Ahead of The Threat Curve

Cyber Security

2018 Cyber Events Summary Report "Year of the Dragon"

Preface

2018 – "Year of the Dragon" – Hundreds of Companies and Organizations Globally Targeted by Chinese APTs

2018 is the third year in which nation-state attackers are the most significant cyber actors. However, unlike 2017, in which we assessed Russian APTs as the most influential cyber threat due to their prolific activity, in 2018 China has become the most significant nation-state attacker.

The campaigns revealed this year indicate a substantial effort by China to obtain by any means necessary bleeding-edge proprietary technology and research, as well as political and military intelligence. It appears that China expanded its cyber operation in order to promote and secure its nations interests; with little care of international, economic or regulatory agreements. Notably in December, the US exposed a large-scale and aggressive attack campaign targeting numerous companies and organizations around the world.

In our assessment, over the last few years, China has systematically amassed a massive and unprecedented wealth of knowledge; unlawfully obtained from thousands of companies, organizations, academic, governmental and military bodies around the world. China's end goals with these operations is surpass the US, economically and technologically, and position itself as the leading super-power.

It should be noted that this method of operation is not new. Many of the attacks that were exposed this year operated undetected over long periods of time. With that in mind, over the last year in particular we have seen bold attacks and campaigns. It appears that Chinese cyber actors are returning to their modus operandi from 2016; characterized by aggressive attack vectors with less emphasis on being covert. This in conjunction with the growing efforts from various countries around the world to combat cyber threats, have resulted amongst other reasons, with multiple large-scale Chinese cyber operations revealed throughout 2018.

Russian Attacks

In 2018, just like in 2017, Russia continues to be a significant nation-state actor and habitat for cybercrime groups. The latter, stealing in the past year billions of dollars via ransomware and spear phishing targeted attacks. Following recent years, in 2018 the most targeted sectors by the Russian were governmental, healthcare and financial sectors. However, unlike previous years, many Russian attacks were thwarted by US intelligence, defense, and law enforcement bodies.

Most Significant Types of Attack in 2018

Spear and scatter-shot cyber extortions – millions of SMEs (Small to Medium Enterprises; aka SMB - Small to Medium Businesses) including their clients and customers, were affected this year by cyber extortions executed by both cybercriminal organizations and lone hackers operating independently.

BEC (Business Email Compromise) – these scams (aka “Man-in-the-Email” and CEO scams) are phishing attacks (often spear attacks) impersonating various key individuals such as CEO/CFO, representatives of third-party service providers, family members or friends, with the purposes of stealing money. According to recent estimates, in the last five years over $12.5 Billion were stolen by this vector.

Theft of financial records and data – as governments and the financial sector are continually pushing to digitize financial services and use, malicious actors are finding more and more vectors to steal and exploit financial records and details. For example, in the US we are seeing an alarming trend in recent years of malicious actors stealing and leveraging W-2 tax forms for monitory gain.

Attacks on banks' core systems and crypto markets – the magnitude of direct financial loss in 2018 is in our assessment around $1.5 billion dollars.

Multi-dimensional cyber attacks - Sophisticated attacks that concurrently target multiple systems of organizations. Some of the most notable victims of these attacks in 2018 were banks in India, Pakistan, Mexico and Chile. For example, in such attacks the attackers may target the ATM system, credit and debit card payment system, and the SWIFT system, as well as various IT systems; taking control of them and/or corrupting them in order to disrupt operation and following investigation.

Espionage attacks – Theft of sensitive data and technology. This is conducted for a wide range of reasons from criminal activity for financial gain, to nation-state operation for national interest.

Destructive attacks – Aka wiper attacks, are spear or scatter-shot attacks, often executed by APTs groups (Advanced Persistent Threat). For example, following the financial sanctions of Iran, the Iranian government re-implementedthe destructive malware Shamoon against multiple energy providers and governmental organizations in the Gulf region.

Exploitation of the supply chain to execute cyber attacks – one of the most notable attack vectors in 2018 has been - targeting third party IT service and product providers in order to breach highly secure companies and organizations. For example, the Chinese attack on HP and IBM.

Destructive attacks – one of the most significant actors executing such attacks are Iranian APTs targeting Gulf Countries. This activity has escalated following the enactment of financial sanctions on Iran.

Notable Events and Trends in 2018

2018 was a pivotal year for cyber regulation – throughout 2018, several high profile cyber regulations and initiatives were approved or implemented within numerous countries around the world. Many of these also included new measures and guidelines that governments and private organizations must follow in order to better protect information. Perhaps the most notable of these was the European Union's act - the GDPR (General Data Protection Regulation), which was implemented in late May.

Attacks on prominent sectors and industries – in 2018 the most targeted industries included, public (e.g. local and national governments), defense and military, healthcare, IT, aviation and financial. Regarding the latter, this past year we witnessed dozens of attacks on banks' core systems as well as crypto-markets; culminating in direct financial losses of about $1.5 billion, in our assessment.

Rapid exploitation of 1-day vulnerabilities, in conjunction with growing proliferation of attack tools - 1-day vulnerabilities are newly exposed vulnerabilities that have not yet received security patches. Attackers monitor reports for them and exploit the window of time between their reveal, and the time official fix are issued. One of the most interesting incidents this year was the 1-day-based malware that was propagated by the Iranians against Gulf states; just hours within the reveal of the vulnerability.

What Didn't Happen in 2018

Infection event affecting hundreds of companies - in the past year there were no destructive attacks with potential of affecting hundreds of companies around the world were executed or mitigated. This is in stark comparison to 2017, during which we witnessed several of these; with NotPetya being the most destructive, hitting hundreds of companies within hours, and causing billions worth of damages.

Critical national cyber event – in the past year no cyber attacks that can be classified as "category 1 - National cyber emergency" were executed (or at least exposed). The UK NCSC (National Cyber Security Centre) defines this category as a "cyber attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life".[1] In comparison, the 2017 WannaCry event was classified as a Category 2.

In our assessment, the reason no category 1 took place this year was due to the significant improvement and strengthening of the global cyber community in detecting, alerting and mitigating cyber threats. In particular, in our assessment, the US government and cyber community uncovered and prevented this year several Russian/North Korean attacks that had the potential of causing considerable damages to hundreds or even perhaps thousands of companies.

Significant shutdown of industrial complexes - in 2018, no significant attack on ICSs (industrial control system) with dedicated wiper malware (such as Triton or CrashOverdrive), resulting in disruption of operation for over a week, were executed or exposed.

Cyber Attacks Targeting Israeli Entities

Iranian APTs - the most significant actor operating against companies and organizations in Israel in 2018.

Hammas threat groups – in 2018 were highly active against defence and military bodies in israel; notably IDF soldiers.

Russian ATPs – in late 2018 we identified initial indicators of first Russian ATP attacks in Israel.

Phishing attacks – a number of cybercriminal (hackers, some of which are Israeli) compromised financial records and successfully leveraged them to steal several million NIS.

Disinformation operations – throughout 2018 we have detected and exposed attempts (notably Russian and Iranian) activities aimed to alter the Israeli status quo, whether to instigated disrest in the public public sphere, or to influence the results of the coming allections.

The Israeli companies that were hit the worst in terms of **financial damage** are cypro firms that suffered losses of tens of millions of dollars.

Also, as in previous years, in April 7th, the annual hacktavist campaign OpIsrael took place. 2018's OpIsrael was characterized by a low-level of activity and did not produce any major results; as opposed to those seen in previous years. In recent years the campaign has significantly lost momentum since it was launched in 2013.

Predictions for 2019

Continuation/escalation of cyber hostility between China, Russia and the US - the growing hostility between the above nations, in conjunction with multiple reveals throughout 2018 of highly successful Chinese espionage campaigns against western countries, may result in 2019 with cyber retaliations operations. This eventuality could culminate in mutual acts of cyber hostility such as, leaking highly sensitive information and large databases, and possibly even destructive cyber attacks.

Continuation/escalation of attacks on the financial sector by North Korea and Russian APTs - we expect North Korean nation-state and Russian criminal APTs to continue and expand their activity against the financial sector, and in particular, banks, inter-bank payment systems, ATM systems and cryptocurrency platforms.

[1] https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

Continuation/escalation Iranian spear attacks on the US, Israel and the Persian Gulf countries - the consistent improvements of tools and vectors used by Iranian threat agents, will continue to test the cyber defenses of the above countries. The Iranians have systematically been improving and modifying their method of operation, with the end goal of obtaining a persistent foothold within academic, defense/military, governmental and critical infrastructure organizations. Further, due to the financial sanctions imposed on Iran in 2018 by the US, it is possible that Iran may attempt to execute a "payback" destructive attack in 2019 against Israel, the US and/or the Gulf states.

Increase of number of attacks executed by breaching third-party providers and exploiting internal organizational systems' flaws - the number of attacks executed this past year, have illustrated to all active cyber attack groups the effectiveness of these vectors. Accordingly, we believe that this method of operation will considerably expand and be improved upon in the coming years. Notably, in our assessment, we will see more attacks targeting cloud base systems, such as email and CRMs; either to steal money and/or information, or as an entry point to the targeted organization.

Raised awareness to the necessity of infosec procedures – protection of databases, embedded system and meeting new regulations – with the new cyber legislations, including GDPR and CCPA (California Consumer Privacy Act), companies are mandated to report cyber incidents within a short period of time (72 hours in the case of GDPR), or face heavy fines and other repercussions. As a result, we expect to see a significant investment in better infosec behavior within organizations, implementation of new cyber security technologies, and increased transparency with regards to companies reporting database and systems security incidents.

Attack resulting in disruption of critical services and possibly even loss of human lives (category 1 - National cyber emergency) - we are unable to accurately predict that such attack will take place in 2019; however, if a category 1 attack happen, it will likely be executed due to military and/or geopolitical activity. Further, we believe that such attacks will likely target Russia's direct political opposition such as Ukraine.

Table of Contents

Overview of Cyber Events and Trends 2018

Event	Date	The attacker	The scope of damage	Attack vector
Chinese espionage campaign against dozens of companies around the world	The campaign was exposed on December, but began almost a decade ago	Chinese attack group APT10	The full scope is yet unknown. Note however, dozens of leading companies were hacked and sensitive information was stolen over long periods of time (between days and years)	They attackers targeted the supply chain – hacking IBM and HP, obtaining information leveraged to gain access to dozens of companies
VPNFilter	June	Unknown as of the issuing of this report. Also, their goal is unknown.	This malware attacks routers of the most of the world's largest producers, such as: TP, Huawei, Netgear, ZTE, D-Link, Link and more	A sophisticated malware with destruction and persistence capabilities. Also, it enables the attacker to perform MitM attacks (Man-in-the-Middle)
Theft of sensitive military documents from a British government security contractor.	The event was first identified in May 2017, and was publicly revealed in March 2018.	Chinese attack group APT15	Systems of a British government contractor compromised, providing access sensitive information and documents, including classified military technology	A targeted attack using Backdoor malwares
Chinese state-attack group stole a 614GB database from a US navy contractor.	The attack was publicly revealed in early June 2018	Chinese nation-state attack group - TEMP.Periscope	The group hacked a US navy contractor and stole a sensitive 614GB database. It included development plans of new submarines and marine weapons planned to be operational from 2020	Sophisticated espionage campaign. As of the end of December, no research findings or technical information about the attack were published
A Chinese-state espionage campaign against telecommunication and satellite companies in the US and southeast Asia.	The campaign was publicly revealed in June 2018	Chinese nation-state APT - Thrip	A sophisticated espionage and destruction campaign, targeting security, satellite, communications and geographical mapping companies in the US and southeast Asia	Destruction and espionage attacks. Various tools were used, both open source and independently developed. High level capability of locating and exploiting vulnerabilities in computer and IT systems for carrying out attacks
Attacks against the financial sector banks (SPEI/SWIFT systems)	Ongoing – a series of attacks against financial institutions around the world	Various attackers. The prominent actors are North Korean and Russian APTs	Tens of millions of dollars. To illustrate the scope of attacks, between January 2018 and the end of May, 67 attacks were reported against	Various sophisticated vectors. For example, hybrid attack vectors combining destruction attacks alongside money theft like the attacks

			financial institutions in the US alone [2]	against the Mexican bank Bankcomext
Ransomware attacks against hospitals and hospitals and public/government organizations.	Ongoing	Criminal actors around the world	Theft of millions of dollars by blackmailing and shutting down critical and life-supporting systems	Infecting hospital systems, mainly with a malware attached to an email.
Attack into the hotel chain Marriot.	Marriot found out about the attack in September and publicly announced it in November. The attack likely occurred in 2014	Unknown as of December 2018. Chinese state actors are suspected.	500 million clients' identification information from 2014 around the world were stolen. Of them, 327 million clients' financial information were exposed	Unknown as of December 2018
Hack into UIDAI, India's Biometric database. **(The largest database in the world – over a billion people)**	The event was revealed in January 2018	Unknown as of December 2018.	1.19 billion Indian citizens' sensitive identification information was stolen – including confidential ID numbers, fingerprints, retina scans, face photos, names, addresses, telephone numbers, bank accounts and accounts in government services. The database is now selling for about $10 dollars.	The attackers exploited a vulnerability in the database's software in order to make 26 changes to the system's code, including security mechanisms[3].
Attacks against the aviation sector including: **Boeing** **Air Canada** **British Airways** **Cathay Pacific**	Boeing March Air Canada August British Airways September Cathay Pacific October	Unknown Unknown Unknown Unknown	Conflicting reports about the scope of damage. Sensitive information might have been exposed, but Boeing denies it. 20 thousand client's information was exposed. 585 thousand clients' information 9.4 million clients' identification information.	WannaCry malware The company's cellphone app compromised The company's website was compromised The company's servers were compromised
Spectre & Meltdown	Revealed in early 2018	N/A	A critical vulnerability affecting almost every computer chip manufactured in the last 20 years.	As of December 2018, no in-the-wild attacks exploiting the vulnerabilities were reported.
Google +	Revealed in October	N/A	A flaw in the social media platform exposed 500 thousand users' information, from 2015	Exploitation of the information for an attack was not reported. Following the reveal Google closed down the platform

[2] https://www.idtheftcenter.org/images/breach/2018/DataBreachReport_2018.pdf
[3] https://www.huffingtonpost.in/2018/09/14/uidai-aadhaar-hack-new-analysis-shows-hackers-changed-enrolment-software-code-in-26-places_a_23525828/

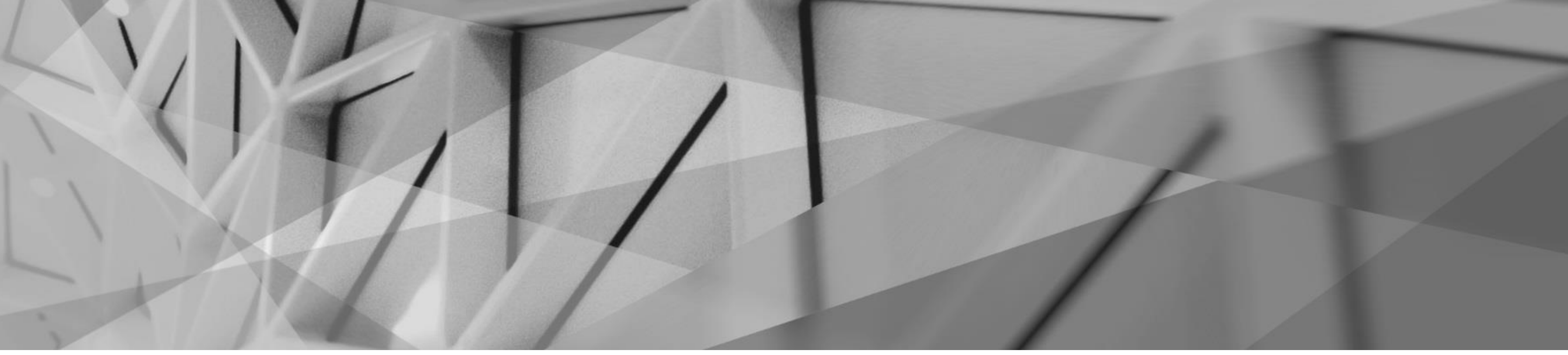
Most Significant Attack Vectors in 2018

Vector	Notes
Exploitation of the supply chain	Breaching a third-party service provider to execute an attack on a company that uses its services or products. In 2018 we have seen numerous events executed with this vector. Chief amongst them is the destructive malware attack on the 2018 Winter Olympics, which was conducted by compromising the event's main IT service provider Atos. These attacks are often executed in conjunction with the exploitation of OS and communication protocols vulnerabilities.
BEC scams (Business Email Compromise)	This type of scam is relatively easy to execute with one of the most common scenarios being that the attacker impersonates a director in the company and requests from the target (often someone in a financial department) to immediately and covertly wire transfer money for reasons such as an urgent and secretive, yet highly important business deal. According to an FBI report, companies around the world have lost over US$12.5 billion to such attacks in the last five years.
Ransomware/wiper malware	Over the last year we saw a dramatic increase in both proliferation and sophistication of ransomware attacks. Further, this year several major events happened in which attackers distributed wiper malware that masqueraded as ransomware with the aim of prolonging the attacks.
Emails containing malicious attachments or redirect users to malicious sites	Spear phishing emails or widespread "scattershot" emails sent via botnets were used in a variety of phishing attacks such as BEC, malicious spam, or as a means of penetrating organizational systems. In order to bypass security and email filtration systems, malicious actors began incorporating in their attacks social engineering techniques[4], For example, the Russian cybercrime group Carbanak contact business by phone and convince the representatives under various pretenses to open malicious attachments, thus insuring that they are compromised.
Leveraging compromised accounts and cloud based systems (e.g. Dropbox, 365 and Gmail) to gain access to sensitive systems	leveraging cloud services to gain access to companies and organizations. Many companies and organizations do not implement 2FA security features, thus enabling a relatively easy penetration vector to organizational cloud based email systems.
Exploitation of native OS and communication protocols vulnerabilities	Hacking companies and organizations by exploiting native OS and IT vulnerabilities, in order to compromised and gain control of targeted networks. Additionally, criminal cyber actors continue to exploit e-commerce website flaws in order to exfiltrate valuable data, including credit card records.

[4] https://www.malwarebytes.com/pdf/labs/Cybercrime-Tactics-and-Techniques-Q1-2017.pdf

Waterhole attacks	The attacker creates a fraudulent site or abuse a legitimate site that is usually often visited by the target. In many cases the attacker lures the target to the site by using different methods such as phishing emails, spear phishing, etc. Once accessed the site usually serves malicious payload such as exploit code or malware. In cases of spear targeted attack, the attacker creates custom content to his target and his interests. Malicious actors have even started creating websites that imitate web browsers' warning of malicious sites. These types of sites most often download a malware or redirect the users to various fraudulent services that tricks them into providing sensitive information such as login credentials or credit cards details. Another common technique is creating a website with a minor almost invisible change in their URL. For example, malicious actors registered the domain google[.]com that impersonates Google.com (the little G is in fact a Latin character). This method is growing and nowadays entire domains are registered with various languages that have similar character to English, thus increasing the difficulty of identifying a fake URL. Earlier this year we identified Iranian campaigns that used the same method to compromise computers of Israeli users.
Attacks on mobile devices via malicious apps	Multiple infection vectors, including - infecting users who reach waterhole attacks by exploiting a vulnerability to download and install an App (commonly with older android versions), or propagation of malicious apps via unofficial and fake app stores. Victims are lured to download and install external APK files. For example, malicious versions of games, dating apps, chat apps etc., not released worldwide; tempting many to install versions disseminated across various channels such as social networks. Once infected, the malicious apps can execute any number of activities such as keylogging, downloading additional malware, exfiltrate data such as GPS location, place an "overly" image or interface over the existing system, and much more. Because of them, many of the malicious apps impersonate banking or other financial service apps. Throughout 2018 there have been countless dissemination and infection campaigns. For example. In November, ESET revealed a sophisticated android malware used to steal money from PayPal users while bypassing the two-factor authentication technology.[5] The malware disguised itself as a cellphone battery optimization tool, and propagated through unofficial app stores. After activation, the app collapses and its icon disappears.
Physical attack of ATM machines and card skimmers	As technology constantly becomes smaller and cheaper, we see more advances and concealed skimmer devices, with designs that enable easier installation. This year, there is was a notable rise of such attacks in Israel. Also, this year a first wave of Jackpotting attacks took place in the US.
Amplified DDoS Attacks	During 2018, two DDoS attacks took place of an unprecedented scope of 1.3 and 1.7 Tbps. The two attacks were neutralized successfully without any significant damage, but they are worth mentioning because they were carried out by exploiting vulnerable memcached servers, rather than via botnets such as Mirai.

[5] https://www.welivesecurity. com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/



Most Significant Attacks and Events – Review and Analysis

Most Significant Cyber Actor in 2018 – China

Chinese Attacks and Espionage Campaigns Against Western States and Companies

Throughout 2018 we saw significant Chinese cyber activity against both the public and sector private. For example, in July it was revealed that a former Apple employee who stole over 40GB of proprietary autonomous cars, and allegedly attempted to sell to a Chinese car manufacture by the name Xpeng Motors.[6] This incident however is just one of many espionage operations against western companies and countries.

As of late December, many of these incidents are still developing. Furthermore, it is currently unknown whether they have shared overarching agendas. In our assessment, with the political shift taking place between the US and China, we are likely to witness in the coming years an expansion of both nation-state and industrial espionage activity. With this regard, several factors and notable events should be noted:

- China's economic plan "Made in China 2025" – a large-scale and aggressive governmental developed plan aiming to push China to a global leader in development, manufacturing and exporting cutting-edge technology.[7]
- The US sanctions on Chinese technology giants such as Huawei and ZTE, placed amongst other reasons, due to fear of espionage. A number of US senators have even referred to Huawei as "effectively an arm of the Chinese government".[8] Moreover, in February, the heads of six major US intelligence agencies warned American citizens against using products and services by Huawei and ZTE.[9]
- The arrest of Huawei's CFO in early December.[10]
- Billions of dollars' worth of import and export tariffs.[11]

One of the biggest fears is the nation-state actors will install malicious components in electronics shipped to the west. Case in point, in October, Bloomberg published a report claiming that China installed spy microchips in computer systems of about 30 major western corporations, including Amazon and Apple. [12]

6 https://www.washingtonpost.com/news/morning-mix/wp/2018/07/11/ex-apple-engineer-arrested-on-his-way-to-china-charged-with-stealing-companys-autonomous-car-secrets/?utm_term=.c4fdbc6dc28a
7 https://www.forbes.com/sites/marcoannunziata/2018/08/10/seven-steps-to-success-or-failure-for-made-in-china-2025/
8 https://www.cio.com.au/article/633134/huawei-effectively-an-arm-chinese-government-us-senator/
9 https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears
10 https://www.rte.ie/news/2018/1206/1015449-huawei-arrest/
11 https://www.bbc.com/news/world-latin-america-46413196
12 https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

As of early January, all parties involved have denied these allegations, and as of yet, no additional evidence to support them has surfaced. Nevertheless, due to the considerable western dependence on China's manufacturing capabilities, this concern is legitimate and highlights a genuine potential espionage vector.

Consequently, in early August the Pentagon banned deployed service members from using wearable technology that relies on geolocation including fitness-tracking devices[13], as they can expose location of bases and other critical facilities[14]. This policy came into effect just three months after the Pentagon also enforced stricter rules regarding the use of mobile devices within the Pentagon and supported buildings. The new policy applies to all DoD personnel, contractors, and visitors[15].

Early this year, due to the same concerns, the Dutch government began providing its officials with highly secure mobile phones, developed in mind to mitigate cyber threats[16]. Notably, these phones have hardware-based encryption that provides restricted-level secure voice and text. Additionally, they lack support for apps. Consequently, certain threats such eavesdropping and compromise of data via malicious applications, are considerably reduced.

Below is a review of the most significant events that took place or were exposed this year

Large-Scale Chinese Espionage Campaign via Supply Chain - APT10 Group Hacked HP and IBM Stealing Sensitive Data of Dozens of Clients

In December, a sophisticated and lengthy espionage campaign against numerous industries and across at least 12 countries was exposed[17]. As it stands, this event is looking to be one of the most significant from the last couple of years. The Chinese nation-state actor APT10 hacked Hewlett Packard Enterprise Co and IBM's network and stole hundreds of GB's critical data regarding dozens of clients, which it leveraged for additional attacks.

The US CERT issued an alert on this matter, however it refrained from naming the clients' name (likely due to pressure from the clients to keep that information confidential). This breach to two of the largest IT firms in the world, and establishing a foothold that lasted for months and years is a critical hit to the world of cyber security. In particular IBM, who is an industry leader for cyber security solutions, experiencing such a comprehensive breach demands a thorough examination of all aspects of the event.

This event became public when the US indicted two Chinese hackers and members of the nation-state group APT10, who were involved in the attacks against IBM and HP, as well as the subsequent attack on the clients. These supply-chain attacks were part of a larger campaign dubbed CloudHopper targeting managed service providers (MSPs).

Note that info-sec firms have reported on CloudHopper in 2017, and according to the indictments it has been operating since at least 2014. As part of the campaign the group breached IBM and HPE several times over the course of the last few years, maintaining a foothold for weeks and even months at a time. IBM and HPE are not the only major companies compromised by CloudHopper, however as of late December the investigation has not revealed their identities. Further, both IBM and HPE have refused to share any information regarding the attacks, and are claiming that no sensitive data was compromised.

This Chinese nation-state group (aka Menupass, Stone Panda, CVNX, Red Apollo and POTASSIUM) first appeared in 2006. Amongst the group's target are construction and engineering, aerospace, and telecom firms, and

13 https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/
14 https://www.militarytimes.com/news/your-military/2018/01/29/dod-reviewing-stravas-global-heat-map/
15 https://abcnews.go.com/US/pentagon-allowing-cell-phones-strict-rules/story?id=55362258
16 https://www.securitynewspaper.com/2018/01/23/dutch-government-switches-super-secure-dumb-phone-prevent-hacks/
17 https://www.reuters.com/article/us-china-cyber-hpe-ibm-exclusive/exclusive-china-hacked-hpe-ibm-and-then-attacked-clients-sources-idUSKCN1OJ2OY

governments in the United States, Europe, and Japan. Their primary attack vectors are spear-phishing and exploiting supply chain such as MSP.[18]

Further stated in the indictment[19] is that since 2006 until recently the defendants worked for a Chinese company called Huaying Haitai Science and Technology Development Company (Huaying Haitai), and operated in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.[20]

It appears from the investigation that other major companies, other that HPE and IBM, were attacked and had their supply chain compromised; however, the US-CERT has so far refrained from stated their names (in our assessment this is due to pressure from these companies not to divulge this information at this point).

The fact that one of the largest IT infrastructure companies in the world has been breached for such a long time is a hard blow to the world of cyber security. IBM is a market leader in cyber security solutions, and such a comprehensive breach demands an in-depth examination of the event in order to prevent recurrences.

Chinese Hackers Target National Datacenter in a Sophisticated Espionage Campaign

On June 13, Kaspersky lab reported[21] an ongoing country-level waterholing campaign against an un-named country in Central Asia. The campaign, executed by APT27 (aka LuckyMouse and EmissaryPanda), compromised a key national datacenter, providing the attackers with "access to a wide range of government resources at one fell swoop.". The campaign is believed to be active since at least autumn 2017.

According to the report, the attackers leveraged this access to execute waterhole attacks via an unspecified number of the country's official websites, which were injected with malicious scripts. The weaponized sites would then direct redirect visitors to instances of both ScanBox and BeEF. The former is a reconnaissance framework gathers data regarding the victim's machine. The latter, BeEF (short for The Browser Exploitation Framework), is a "penetration testing tool that focuses on the web browser".[22]

It should be noted that as of writing this report, the initial infection vector is unclear. However, one of the tools found in this campaign is a variant of the HyperBro Trojan, which is regularly used by various Chinese-speaking actors.

APT15 Steals Military Documents from UK Government Contractor

Chinese affiliated threat agent APT15 has reportedly penetrated the systems of UK government contractor, affectively gaining access to highly sensitive military technology information, according to a report by NCC Group, published on March 10, 2018**[23]**.

The incident in question was discovered in May 2017, when a contractor providing a range of services to Britain's government suffered a network breach by the threat actor. NCC Group's analysis of the incident yielded that two new backdoors, dubbed RoyalCli and RoyalDNS, were used by the actor, as well as BS2005, a tool previously affiliated with APT15.

APT15 operated on the compromised network between May 2016 until late 2017 and affected over 30 hosts during that time. The initial point of entry into the network remains unclear; however, the attackers gained

18 https://www.fireeye.com/current-threats/apt-groups.html
19 https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
20 https://www.reuters.com/article/us-china-cyber-hpe-ibm-exclusive/exclusive-china-hacked-hpe-ibm-and-then-attacked-clients-sources-idUSKCN1OJ2OY
21 https://securelist.com/luckymouse-hits-national-data-center/86083/
22 http://beefproject.com/
23 https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

domain administrator credentials by using the open-source tool Mimikatz, which later facilitated the seizure of a VPN certificate which was then used to access the victim's network remotely.

Chinese Hackers Stole 614GB of Data from a U.S. Navy Contractor

In early June, it was reported that between January and February of this year, hackers linked to the Chinese government stole 614GB of highly sensitive data from an unnamed contractor, such as plans for a supersonic anti-ship missile intended to be operational by 2020.

According to the Washington Post, the hackers also stole material related to a "project known as Sea Dragon, as well as signals and sensor data, submarine radio room information relating to cryptographic systems, and the Navy submarine development unit's electronic warfare library." [24]

The post claims that further data was compromised, however at the request of the Navy it is withholding reporting any details about it to avoid harming national security. It should be noted that the data was hosted on an unclassified network. Furthermore, while the compromised data is described by the Post as "highly sensitive", official sources have stated that when aggregated, it could be considered classified.

The breach is being investigated jointly by the Navy and the FBI. As of writing this report no technical information regarding the attack vector or tools has been revealed. China on her part is denying any involvement, telling Reuters[25] that the Chinese government "staunchly upholds cyber security, firmly opposes and combats all forms of cyber attacks in accordance with law."

This attack however comes after it was exposed[26] in March, that the Chinese affiliated threat agent APT15 stole military documents from UK government contractor. The incident in question was discovered in May 2017, when a contractor providing a range of services to Britain's government suffered a network breach by the threat actor. NCC Group's analysis of the incident yielded that two new backdoors, dubbed RoyalCli and RoyalDNS, were used by the actor, as well as BS2005, a tool previously affiliated with APT15.

APT15 operated on the compromised network between May 2016 until late 2017 and affected over 30 hosts during that time. The initial point of entry into the network remains unclear; however, the attackers gained domain administrator credentials by using the open-source tool Mimikatz, which later facilitated the seizure of a VPN certificate which was then used to access the victim's network remotely.

Chinese APT Targets US Satellite and Defense Companies

A Chinese threat group has been targeting satellite, communications, geospatial imaging, and defense organizations in the United States and South-East Asia, and is doing so for espionage and/or destructive purposes, according to a Symantec report from June 19, 2018.[27]

In the latest wave of attack beginning in 2017, the threat actor, dubbed by Symantec as Thrip, has been launching attacks using a wide-range of tools, a mixture of custom made malware, open-source tools and "living off the land" tactics - the use of legitimate operating system features or network tools to compromise targets. Among the targets in this campaign were a satellite communications operator and an organization involved in geospatial imaging and mapping.

24 https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.a64f5945b9d9
25 https://www.reuters.com/article/us-usa-china-cyber/china-hacked-sensitive-us-navy-undersea-warfare-plans-washington-post-idUSKCN1J42MM
26 https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-anaysis-of-royalcli-and-royaldns/
27 https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

Notably, the actor seemed to focus on the operational side of these companies, and deliberately sought to infect systems running software that monitor and control satellites and geospatial imaging applications. This focus suggests the threat actor likely had a destructive motive. In addition to these targets, the threat actor also targeted three different telecom operators based in Southeast Asia and a defense contractor.

As mentioned above, Thrip uses a wide range of tools and custom-made malware on its targets. However, the group is increasingly relying on living off the land tactics and open-source tools. This renders the malicious activity more difficult to detect and attribute, as it blends in within a large number of legitimate processes.

In this campaign, the actor employed a previously unknown custom Trojan called Catchamas, an information stealer that contains additional features designed to avoid detection.[28] Catchamas is built to obtain various information from infected computers, including keystrokes, clipboard data, screenshots based on specified keywords in the window title and network adapter information. Moreover, the threat actor used an updated variant of Rikamanu, a Trojan attributed to Thrip that logs keystrokes made on a compromised computer.[29]

The threat actor leveraged PsExec, a legitimate Microsoft Sysinternals tool for executing processes on other systems, in order to install the malware and to move laterally on the compromised networks. In addition, the threat actor utilized the following legitimate/open-source tools:

- **PowerShell:** Microsoft scripting tool that was used to run commands to download payloads, traverse compromised networks, and carry out reconnaissance.
- **Mimikatz:** Freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext.
- **WinSCP:** Open source FTP client used to exfiltrate data from targeted organizations.
- **LogMeIn:** Cloud-based remote access software.

Chinese APT 'Tick' Weaponizes USB Drives to Access Air-Gapped Systems

According to a report by Palo Alto's Unit 42 published in June, the Tick cyberespionage group, sometimes referred to as Bronze Butler, leveraged a unique attack vector to target air-gapped systems, that is, systems isolated from unsecured networks nor connected to any other system that is connected to the public internet. The threat actor, which is likely based in China, primarily targets organizations in South Korea and Japan.

In this attack, the group attempted to spread to isolated systems by compromising a specific type of USB drive created by a South Korean defense company and certified as secure by the South Korean IT Security Certification Center (ITSCC). The USB drives were likely compromised during the manufacturing stage (supply-chain attack), or by various social engineering tactics post-manufacturing.

Attack Vector

At the time of writing, the complete sequence of attack, specifically the initial vector of infection of the USB drive, remains unclear. Nevertheless, Unit 42 provided some of its findings on malware used in this incident, a custom-made tool dubbed SymonLoader, which is designed to compromise Windows XP and Windows Server 2003 systems.

28 https://www.symantec.com/security-center/writeup/2018-040209-1742-99
29 https://www.symantec.com/en/sg/security-center/writeup/2015-072710-4212-99

This is despite the fact that it was created when newer versions of Windows software were available, suggesting the intentional targeting of older and out-of-support versions of Microsoft Windows that are often used in air-gapped systems.

Attack Sequence

- Initially, Tick likely tricked users with a Trojanized version of legitimate software to install SymonLoader. The malware then checks the operating system version of the target host, so as to ensure it is in fact Windows XP or Windows Server 2003.
- After verifying the OS version, SymonLoader creates a hidden window named "device monitor," which continually monitors storage device changes on the compromised system:
- When a removable drive is connected, SymonLoader checks the drive letter and drive type, verifying that the drive letter is not A or B, and the drive type is not a CDROM. If it finds that a newly attached device is a USB drive made by this particular company, it will extract an unknown executable file from the compromised USB.

As mentioned above, Unit 42 did not obtain a compromised USB drive nor the unknown malicious file. Therefore, it was unable to determine how the USB drives were infected nor analyze the unknown malware.

Chinese Espionage Campaign Targeting Aerospace Companies

On October 30, The United States Department of Justice (DoJ) announced[30] that it has indicted ten individuals for allegedly stealing intellectual property, confidential business information and proprietary aerospace technology including designs for a turbofan engine. The targeted companies are a number of U.S. aerospace companies including a gas turbine manufacturer by the name Capstone Turbine, as well as an un-named French aerospace company.

The indicted individuals, two Chinese intelligence officers who recruited six Chinese hackers and two aerospace insiders, reportedly operated for over five years between January 2010 and May 2015. The intelligence officers worked for Ministry of State Security (JSSD), a section of the Ministry of State Security (MSS). Two of the defendants are also charged in a separate private hacking conspiracy that targeted amongst other entities a San Diego-based technology company.

Below are notable known points of time and activities

January 8, 2010 - The hacker team breached Capstone Turbine with a duel propose – stealing proprietary data and use the company's website as a "watering hole."

August 7, 2012 to Jan. 15, 2014 - Two members of the hacker team attempts to hack into the San Diego-based technology company.

January 25, 2014 - One of the insiders (Tian Xi), a Chines national working for the French aerospace company, infects their systems with Remote Access Trojan (RAT) by the name Sakula.

Feb. 26, 2014 - The second insider (Gu Gen) alerts JSSD that foreign law enforcement agencies detected the malware. Subsequently JSSD tries to obfuscate its connection with the malware.

May 2015 - One of the US companies identifies and removes the JSSD's malware from its computer systems.

Attack Vector and Malware

[30] https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

According to the DoJ the hackers used a range of techniques, including:

- Spear- phishing attacks.
- Injecting multiple different strains of malware into the companies' computer systems. Amongst the malware are reportedly:
- Remote Access Trojan (RAT) Sakula, which previously was used by Chines nation-state APT Deep Panda, who is attributed[31] to the 2015 U.S. government's Office of Personnel Management (OPM) breach[32].
- A trojan known as IsSpace, which was previously used by in attacks against tech companies in Japan and Taiwan. The attacks have been attributed to the Chinese espionage APT DragonOK[33].
- Watering holes attacks – the hackers took control of the companies' websites and leveraged them to compromise visitors' computers.
- Domain hijacking through the compromise of domain registrars. The indictment states an Australian domain registrar only referred as "Company L". According to several sources this may be Melbourne IT, who has since changed their name to Arq group[34]. However, the company denies any relation to the event[35].

[31] https://threatconnect.com/blog/opm-breach-analysis/
[32] https://www.ibtimes.com/every-federal-employee-hacked-cyberattackers-stole-more-personal-data-obama-1963492
[33] https://securityaffairs.co/wordpress/62615/apt/dragonok-apt-changes-ttps.html
[34] https://www.zdnet.com/article/melbourne-it-now-arq-group-surprised-by-chinese-aerospace-hack-claims/
[35] https://www.asx.com.au/asxpdf/20181101/pdf/43zy2qmwz4f1z2.pdf

Attacks on Prominent Sectors and Industries

Cyber Attacks on the Financial Sector

Below is a review of the most significant events that took place or were exposed this year

In continuation to the last few years, 2018 is characterized by numerous and successful attacks on the financial sector. For example, over the past year we continued seeing attacks on core banking systems (such as SWIFT and comparable systems), alongside attacks on cryptocurrency platforms and companies.

In regard to banks, this year the SWIFT organization attempted to implement a number of measures. However, despite many promises from the SWIFT organization, little has changed in regard to fixing the underlining issues that enable attackers to exploit its system.

It does seem that there is more awareness amongst the banks and their employees on the matter, which helps detect and terminate fraudulent wire-transfers. Yet, despite the financial sector claiming otherwise, unless wide-scale (and likely costly) measures are taken, we expect that these types of attack will continue.

Attacks on Banking Systems in Latin America

In January 2018, a number of cyber attacks were carried out on banks across Mexico, among them Bancomext, during which threat actors attempted to siphon off funds by targeting SWIFT systems. In May 2018, another cyber attack was conducted against a financial institution in Latin American, this time targeting Banco de Chile (Bank of Chile), a large commercial bank with headquarters in the capital Santiago. Below we review the Chilean bank attack and provide new details on attack against the Mexican bank.

Attack on Banco de Chile

In late May 2018, Banco de Chile was targeted with an unprecedented attack vector, a combined cyber attack that was both destructive and financial in nature. The attack caused major disruptions to the bank's operations in its various branches and services.[36] The damage included the shutdown and/or wiping of 9000 workstations and 500 servers, as well as the theft of $10 million. The latter was carried out via fraudulent financial transactions on the bank’s SWIFT network. The attackers attempted to wire a large number of transactions through SWIFT; however, only four of these were ultimately approved and siphoned to accounts in Honk Kong.

Note that after Banco de Chile failed in its attempts to retrieve the money, the bank filed an official complaint about the matter to Honk Kong’s government. Concurrently, the bank employed the services of Microsoft and

[36] https://www.reuters.com/article/us-chile-banks-cyberattack/bank-of-chile-trading-down-after-hackers-rob-millions-in-cyberattack-idUSKBN1J72FC

Dreamlab teams for assistance in the forensic analysis of the event. A preliminary investigation of the incident determined that the attack was highly sophisticated and likely originated from either Eastern Europe or Asia.[37]

The unique attack included the use of a wiper malware on the bank's IT infrastructure. This was most likely done to remove any remaining incriminating traces from the system and distract the IT and security teams while the financial transactions were being carried out on the SWIFT system. On June 7, 2018, Trend Micro published a report[38] reviewing the spread of a new variant of the wiper malware "KillDisk", also known as MBR Killer and KillMB", in a bank in Latin America in May 2018. Although the company did not publish the name of the targeted bank, we believe the report refers to this same event.

According to a Flashpoint blogpost[39] published on June 12, 2018, the wiper malware that spread through the Chilean bank's infrastructure shares several similarities with an existing component of a malware variant called Buhtrap. This component is also known as MBR Killer and according to Flashpoint, it was leaked on deep web and darknet forums in February 2016. Further, it was also reported that the malware involved in the attack in Chile is a customized version of MBR Killer's "Kill OS" module. Note that Trend Micro's analysis suggests that the new KillDisk variant was named MBR Killer by its authors.

Buhtrap was used in the past in attacks against a number of Russian financial institutions that resulted in the theft $1.23 million. Although no direct link was found between the attacks on the Chilean and Mexican banks, identical malware components were used in these incidents. Please note that the attack in Mexico targeted the country's interbanking electronic payment system (SPEI) and not the SWIFT network. We reviewed these events in our Cyber Intelligence report from May 6, 2018.

Attack Timeline

- On May 24, 2018, Banco de Chile announced[40] that an error in its systems caused disruptions across the its branches and impacted various banking services, including the bank's call center; however, Banco de Chile clarified that no customer transactions were affected.
- On that same day, a screenshot from an instant messaging app that was posted in a Chilean web forum revealed that a wiper malware shut down 9000 of the bank's endpoints and 500 servers.[41]
- The initial efforts to curb the attack spanned four days, during which the bank contacted Microsoft and Dreamlab in for forensic analysis assistance. During the event itself, the bank's security teams focused on preventing the spread of the malware and protecting clients' personal information, accounts and finances.[42]
- At the same time, the attackers began silently conducting a series of fraudulent bank transactions on the SWIFT network. As mentioned above, most of these were declined, apart from four transactions that totaled to about $10 million.
- Four days later, the bank announced that disruption it had experienced stemmed from an infection that impacted the workstations of bank clerks.[43] The forensic analysis revealed the attack originated from either Eastern Europe or Asia.

[37] http://www.latercera.com/pulso/noticia/gerente-general-banco-chile-eduardo-ebensperger-ciberataque-evento-fue-destinado-danar-al-banco-no-los-clientes/198912/
[38] https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-latin-american-financial-organizations-again/
[39] https://www.flashpoint-intel.com/blog/banco-de-chile-mbr-killler-reveals-hidden-nexus-buhtrap/
[40] https://ww3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/declaracion-publica
[41] https://www.antronio.cl/threads/esta-pasando-posible-hackeo-a-banco-chile-a-nivel-nacional.1287865/#post-24410653
[42] http://www.latercera.com/pulso/noticia/gerente-general-banco-chile-eduardo-ebensperger-ciberataque-evento-fue-destinado-danar-al-banco-no-los-clientes/198912/
[43] https://ww3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/declaracion-publica2

Phishing Campaign Launched During the Attack - within an hour of the attack on the bank's systems, its customers began receiving a wave of phishing emails. At this stage, it is unclear whether the attackers themselves were behind this campaign. However, phishing campaigns often accompany attacks of these nature.

ClearSky's Preliminary Insights

- The attackers in question, whether based in North Korea or Russia, are becoming increasingly aggressive and are incorporating destructive methods in their attacks on financial institutions. This is done in order to paralyze a bank's daily operation and security controls, as well as to distract employees from the actual heist. This is new kind of combined attack vector that we have not previously seen used in past bank heists. It is possible that the threat actor involved (that is possibly state-sponsored) is incorporating nation-state attack methods in heist attacks.
- The attackers may have intended to wipe their tracks from a small number of systems, but ultimately lost control of the malware. It is possible that the bank's infrastructure lead to more serious damage than the threat actor intended.
- Defense infrastructure - as soon as an attack on one bank system is detected, we highly recommend considering promptly carrying out a fast inspection/blocking/shutdown of other critical infrastructure that can potentially be attacked.
- We suggest considering the establishment of an emergency protocol to deal with destructive malware spreading across a financial institution. For example, we recommend creating the ability to execute a quick power shutdown of a bank's computer systems, including its IT centers. This is a kind of "reverse" protocol to the bank's redundancy systems. That is, if until now banking systems were designed to continue functioning during a power shutdown through the use of alternative conducting lines, generators and batteries, **we suggest creating the ability to quickly take down the entire system, in order to prevent an attack from spreading.**
- The wiper malware involved in this case functioned in a completely automatic manner and did not communication with the C2 server for commands. Its initial activation was likely carried with an automatic timer, or possibly using remote activation (more likely).
- Current control systems successfully prevent a significant number of attempted bank heists that rely on the SWIFT system.
- The preliminary attack vector is a malicious email attachment that is sent to bank employees. We believe proper network segmentation could have successfully foiled these attacks.

Threat actors today have complete access to a wide range of attack tools that are available in darknet malware markets.

Attacks on SPEI - Mexico's Interbanking Payment System

On January 9th, 2018, the Mexican state-owned bank " Bancomext" reported that it is temporarily suspending its operations due to computer system diagnosis[44]. A day later the bank admitted that it fell victim to a cyber-attack, impacting its international payment platform; presumably its SWIFT system[45]. As of yet, no information regards the threat actor nor the malware that was used, has been reported. According to various sources, $100 million

44 https://www.gob.mx/bancomext/prensa/comunicado-bancomext-suspende-operaciones-para-diagnostico-de-sus-sistemas-informaticos?idiom=es
45 https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion?idiom=es

was stolen in the attack. Further, they stated that this attack has many similarities to additional attacks that took place across Latin America.

On January 15th, 2018, TrendMicro published a report regarding a new variant of the wiper malware KillDisk that is used against financial organizations in Latin America[46]. This malware has been previously seen in other events such as the 2016 BlackEnergy campaign[47] that targeted the Ukrainian energy and financial sector, the 2017 WannaCry attack, etc. In our assessment, this report exposes a covert part of the attack against Bancomext.

In relation to this event, in April 2018, cyber security firm Group-IB published a research regarding the Russian threat actor MoneyTaker. The report reviewed several of the group's attacks against financial organizations across the world, and have deducted that MoneyTaker is currently developing a banking malware, indented against Latin American banks[48].

Additional attacks - This event was followed by a series of spear-phishing attacks against banks in Mexico; however more notably, in late April, Mexico's Interbanking Electronic Payment System – SPEI, was targeted in a sophisticated attack. In our assessment, all these incidents were executed by the same threat actor, which has been leveraging the relatively weak security system of Mexico's financial institutions.

The SPEI system was established in 2004 and allows banks to electronically transfer money between deposit accounts through a private, encrypted network operated by Mexico's central bank, Banco de Mexico. According to recent reports in Bloomberg[49] and Finextra,[50] three Mexican banks were forced to activate contingency measures on Friday, April 27, 2018, in order to foil attempts by attackers trying to infiltrate the payments network.

The central bank clarified that the incident did not result in any client financial loss and that the system's infrastructure was not compromised. Impacted institutions said they had resorted to using an alternate transfer system, which significantly slowed down transaction time from mere seconds to several hours; this likely signifies the payments were conducted manually.

According to another Bloomberg report,[51] Mexico's monetary authority requested that about one dozen additional Mexican banks implement contingency measures and connect to the SPEI network via a less risky backup method, after some transfers were disrupted one week earlier.

Malfunctions in SPEI network connections - according to a tweet[52] by Mexico's Grupo Financiero Banorte on Friday April 27, 2018, the bank experienced a communications error upon connecting to the SPEI service, which resulted in a system reboot. The system was later restored. The bank did not indicate whether the error was a result of an attack. Later, Financiero Banorte said that it had experienced additional communication problems with the SPEI network, which started Thursday, April 16, 2018, and lasted for about 24 hours.

Moreover, Mexico's central bank asked Banco del Bajio SA to connect to the SPEI network via an alternate network. The latter had experienced temporary network communication issues between April 26 and 27, 2018. Another two banks, Corp. Actinver and JPMorgan Chase & Co, were not direct victims of the attack, but also experienced network communication difficulties.

New insights - According to a Bloomberg report from May, reviewing the attack on Bancomext,[53] the event was a foiled $110 million attempted bank heist by a North Korean threat actor. On the day of the attack, transaction

46 https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/
47 https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/
48 https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2017/2017.12.11.MoneyTaker/Group-IB_MoneyTaker_report.pdf (Page 25)
49 https://www.bloomberg.com/news/articles/2018-04-28/mexican-banks-are-said-to-have-been-targeted-in-cyber-attack
50 https://www.finextra.com/newsarticle/32040/mexican-banks-moved-to-alternative-network-as-hackers-target-real-time-payments-system
51 https://www.bloomberg.com/news/articles/2018-04-30/banorte-is-said-to-be-among-mexican-banks-targeted-by-hackers
52 https://twitter.com/GFBanorte_mx/status/990004589486333957
53 https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret

volume was several times higher than normal and unusual activity was detected on the account Bancomext used for international wires. It appears these bank transactions had been disguised as a donation from the Mexican bank to a Korean church. However, since the threat actor's destination banks in Seoul, South Korea, were not yet open for the day (it was 3 AM), the transaction luckily had not gone through.

Additional information uncovered in the article was that the penetration vector consisted of a malicious email attachment sent to a bank employee. Upon being accessed, the attachment dropped espionage malware that likely sat undetected in system while assembling data for the attackers.

Cobalt Recon Campaign Targeting Russian and CIS Banks

On May 23, 2018, cyber security firm Group-IB published a report reviewing the activity of the Cobalt threat group against banks in Russia and the Russian Commonwealth.[54] The report provides an in-depth analysis of the actor's activities and development in recent years, including its new TTPs and chosen targets, which consist of financial institutions in Europe, Asia and the US. The threat campaign reviewed in Group-IB's report took place in late May 2018.

Background - On May 23, 2018, bank employees across Russia received phishing messages impersonating Kaspersky Lab. The emails claimed that a complaint of a violation of "current legislation" was made against the user's PC. The users were prompted to provide a detailed explanation about this so-called incident within 48 hours of receiving the message, under the threat of sanctions on the user's web resources. To view this complaint message, the employees were prompted to access the provided link - a malicious link that downloads the malware to their computer.

The email was drafted in English, which suggests that the actor did not only target organizations within Russian speaking countries. In fact, Group-IB researches found in samples of previous emails sent by the actor the addresses of over 80 organizations, including banks, insurance companies and IT companies across the globe. Below is a screenshot of the email:

The emails were attributed to Cobalt due to the involvement of the unique Trojan **CobInt** in the attack, a tool used by this actor since December 2017. Moreover, the messages were sent from **kaspersky-corporate[.]com,** a domain that was registered by an individual with the same name as one who registered domains previously involved in Cobalt attacks. Nevertheless, the high-quality nature of this phishing campaign is not characteristic of Cobalt, a fact that suggests the possibility of a joint operation with other criminal groups, such as the Russian cybercriminal group Carbanak.

First Jackpotting ATM Attacks in the US

In late January, a sophisticated attack dubbed "Jackpotting", which cause ATM machines to eject all of their cash[55], has hit the US. Jackpotting originated in Russia several years ago, spread to additional countries in Europe and Asia, and recently the US. ATM vendor NCR Corp. and Diebold Nixdorf issued alerts not the matter to banks[56].

In these attacks, the attackers used Ploutus.D. This is a variant of Ploutus, which was first detected back in 2013, when it was used in Mexico. The malware was developed with .net, and can run either as a Windows Service or as a separate program.

Ploutus interacts with Kalignite multivendor ATM platform, developed by the ATM software vendor KAL[57]. These attack's samples indicate that Ploutus targets Opteva 500 and 700 series ATM machines, manufactures by Diebold

[54] https://www.group-ib.com/blog/renaissance
55 https://krebsonsecurity.com/2018/01/first-jackpotting-attacks-hit-u-s-atms/
56 https://www.bleepingcomputer.com/news/security/atm-jackpotting-attacks-hit-the-us-for-the-first-time/
57 http://www.kal.com/en/

Nixdorf. However, with minor changes to the code, it could easily be modified to be compatible with ATM machines from other vendors, as about 40 manufactures use the Kalignite multivendor platform.

To deploy the malware, attackers require physical access to the ATM's internal computer. Consequently, Attackers often impersonate an ATM maintenance team, approached stand-alone machines (often located in places such as pharmacies, large retailer shops, and drive-thru ATMs), and either picked the machine locks, used a stolen master key, or destroyed parts of the machines to gain access to its internal computer.

After gaining access, the attackers connect a laptop and upload a mirror image of the ATM's OS that contains the malware. Once completed the compromised machine will appear out of service to any potential customer.

At this point, the attackers can remotely control the machine and issue a command to dispense cash, which is picked up by money mules. Once the command is issued, the machine will empty all of its cash within several minutes unless the attacker presses cancel on the keypad.

According to a 2017 analysis of Ploutus.D by FireEye, this malware is one of the most advanced ATM malware identified in recent years. The Secret Service has stated in an alert that Windows XP based ATM machines are notably vulnerable, and advised to promptly update them to Windows 7 or later versions of the OS.

Hackers stole $2.4M in two attacks on National Bank of Blacksburg, Va.

Following a lawsuit filed against the bank's insurance firm, a financial heist on National Bank of Blacksburg was exposed. It was revealed that the bank was fell victim twice to phishing attacks over the course of 8 months, between late May 2016 and January 2017, losing $2.4 million dollars[58]. The lawsuit was filed after the insurance firm refused to fully cover the loss[59].

The attackers, presumed Russian, sent spear-phishing emails to the National Bank of Blacksburg in Virginia, infecting a workstation with access to the debit card transaction system used by the bank, the STAR Network[60]. Concurrently the malware continued to spread, eventually infecting another workstation that was authorized to manage National Bank customer accounts and their use of ATMs and bank cards. This was exploited to disable and alter anti-theft and anti-fraud protections, such as 4-digit PINs, withdrawal limits, daily debit card usage limits, and fraud score protections.

Timeline

First attack: May 28, 2016 – leveraging the weekend and holiday. the first attack took place between Saturday and Monday. The bank usually opens for business on Mondays, however at this point of time is was closed due to the federal holiday of Memorial Day. In this attack, the hackers withdrew over $569,000 from hundreds of ATMs across North America.

When the breach was detected, the bank hired cybersecurity forensics firm Foregenix to investigate, which determined that the tools and activity likely originated from Russia. Following this discovery, the bank National Bank implemented additional security protocols, by the recommendation of FirstData, who operates the Star Network. These protocols, which are known as "velocity rules", help the bank monitor and flag suspicious patterns of transactions executed within a short period of time[61].

Second attack: January 7 and 9, 2017 - the attackers presumably maintained an access to the bank's systems, which was not detected in the investigation. Note that the second breach was more substantial as the attacker

58 https://krebsonsecurity.com/2018/07/hackers-breached-virginia-bank-twice-in-eight-months-stole-2-4m/
59 https://krebsonsecurity. com/wp-content/uploads/2018/07/1-main. pdf
60 https://www. firstdata. com/en_us/products/financial-institutions/debit-processing-atm-and-network/star-network. html
61 https://chargeback. com/velocity-checks-fraud-prevention/

not only regained control of Star Network systems, but also compromised a workstation that had access to **Navigator**, a credit and debit management software used by the Bank.

This enabled them to disable clients' withdrawal limits for over $2 Million dollars, of which they successfully stole $1,833,984 million.

In 2017, the bank hired Verizon to investigate the attacks and reached to three main conclusions and findings:

- First that the origin of both the tools and servers used by the attackers was indeed from Russia.
- Second, that both attacks appear with highly likelihood to have been executed by the same actor.
- Lastly, Verizon found that the malware used to obtain the initial breach to the bank's systems was embedded in a malicious Doc file[62].

Lawsuit against the insurance company - To cover the losses, the bank activated its cyber insurance policy with its insurer, Everest National Insurance Company[63]. The policy covered two cyberattack scenarios. The first was for "computer and electronic crime" (C&E) with a single loss limit liability of $8 million, with a $125,000 deductible. The second covered losses that resulted directly from the use of lost, stolen or altered debit cards or counterfeit cards. This had a single loss limit of liability of $50,000, with a $25,000 deductible and an aggregate limit of $250,000.

However, the insurance company determined that both attacks exclusively fell under the second scenario (credit and debit), rather than the C&E scenario due to two exclusions, and thus is eligible for only $50,000 in total. Consequently, the bank filed a lawsuit, on June of 2018, claiming that it does not yet know for certain how the hackers in the 2017 heist extracted the funds.

In previous such heists, often referred to as "unlimited cash-outs"[64], attackers used numerous "money mules". These are usually street criminals who are given cloned debit cards and stolen or fabricated PINs along with instructions on where and when to withdraw funds. In response, the Everest issued a statement[65] regarding bank's claims, claiming that National Bank did not accurately characterized the terms of its coverage, nor did it fully explain the basis for Everest's decision.

Conclusions - there is no foolproof method to fully prevent cyberattacks; according, when organizations insure their assets, it is advised to closely examine various insurance policies and firms together with an expert that specializes with cyberattack claims. Further, if possible, we recommend to custom create a policy that is tailored made as much as possible to your organization.

Russian Hacking Group "MoneyTaker" Stole $1 Million Dollars Russian Bank via AWS CBR System

On July 3, 2018, Russian cybercriminal group MoneyTaker stole, about $1 million from Russia's PIR bank. The actor gained access to the Russian Central Bank's Automated Workstation Client (AWS CBR) system, which is equivalent to the inter-banking communications and transactions system swift. The group then transferred the stolen money to 17 different accounts, at major Russian banks and cashed out without leaving traces.[66]

MoneyTaker primarily targets interbank payment systems such as SWIFT or AWS CBR.[67] According to the investigation executed by Group IB, MoneyTaker has conducted 21 known attacks against banks so far. 16 were executed against banks in the U.S, while five attacks were aimed on banks in Russia. Average damage per incident

62 https://blog. barkly. com/what-is-macro-malware-2017
63 https://www. everestre. com/
64 https://krebsonsecurity.com/2011/08/coordinated-atm-heist-nets-thieves-13m/
65 https://krebsonsecurity.com/wp-content/uploads/2018/07/everest-response.pdf
66 https://www.group-ib.com/media/new-attack-MoneyTaker/
67 https://thehackernews.com/2017/12/bank-hackers.html

amounted to $500,000 in the U.S. and $1.2M in Russia. Further, the group also stole documents about interbank payment systems needed for subsequent attacks, and executed an attack against a banking software company in the UK.[68]

The group is highly sophisticated, often using self-developed hacking methods and tools, including file-less malwares. Other tools used by MoneyTaker are widely used such as Metasploit, NirCmd, psexec, Mimikatz, and Powershell Empire, which further make it hard to establish attribution. The group is known for their covert operation, obfuscating their activity by using 'one-time' infrastructure and meticulously deleting evidence following their attacks.[69]Nevertheless, cyber researchers have identified this modus operandi since late 2017[70].

The attack - The attack on PIR bank begun in late May 2018, after the group maned to obtain access to the bank's systems via a compromised router. As mentioned in Group IB's report, this technique is a characteristic of MoneyTaker, and was previously used at least three times against banks with regional branch networks[71].

On July 3, after establishing a persistent foothold for over two months, the group hacked the bank's main network, accessing AWS CBR system. Once in, they transferred funds to mule accounts prepared in advance across 17 major banks around the world, which were cashed out immediately via ATMs.

The attack was detected the following night, on July 4, when the bank's IT staff identified unauthorized transactions with large sums. They promptly contacted the regulator and requested to block the AWS CBR digital signature keys, however by that point it was not possible to stop the financial transfers. MoneyTaker successfully withdraw $920,000 dollars.

The group then deleted OS logs on many of the bank's computers in order to hinder the response to the incident and its following investigation. As stated, this technique was observed in previous attacks executed by the MoneyTaker. Moreover, they left PowerShell scripts that potentially could enable them to reestablish access to the in the bank's network and thus execute new attacks. This however was discovered by Group-IB and removed by the bank's sysadmins[72].

$13.5M Stolen in Attack on Indian Cosmos Cooperative Bank

On August 15, the Indian bank Cosmos Cooperative Bank[73] reported that it fell victim to cyberattacks targeting two core banking systems, the ATM/Debit card and SWIFT systems. As a result of these two attacks, which took place over two days, the bank lost $13.5 million dollars.

Once the bank detected the breach it immediately reported the attack and shut its VISA and Rupay Debit card payment system. Further, the bank hired a cyber-security company to conduct a forensic investigation of the event. According to the bank, the perpetuates are highly sophisticated and likely obfuscated their tracks by various means. A full investigation report is expected to be published in the coming days.

As of now, the identity of the attackers is unknown, however various assessments are attributing the attack to the North Korean nation-state threat group Lazarus, which executed numerous attacks on financial institutes around the world in recent years.

68 https://arstechnica.com/information-technology/2018/07/prolific-hacking-group-steals-almost-1-million-from-russian-bank/
69 https://www.group-ib.com/media/new-attack-MoneyTaker/
70 https://securityaffairs.co/wordpress/74586/cyber-crime/moneytaker-cyber-heist.html
71 https://www.securityweek.com/MoneyTaker-hackers-stole-1-million-russian-bank
72 https://arstechnica.com/information-technology/2018/07/prolific-hacking-group-steals-almost-1-million-from-russian-bank /
73 https://timesofindia.indiatimes.com/business/india-business/hackers-siphon-over-rs-94-crore-off-a-co-operative-bank-in-pune/articleshow/65411078.cms?from=mdr

$6.5M Dollar Theft Attempt from BankIslami in Pakistan

On October 27, the Pakistani bank BankIslami fell victim to a "cash-out" cyber attack[74]. The attackers used clients' debit cards to withdraw money from ATMs in various countries, most notable of which was Russia. The bank claims that only $20,000 dollars were stolen, despite the large amount of withdrawal attempts. The rest of the transactions were halted.

However, in contrast to other attacks against banks in Asia over in 2018, the attack vector appears to be different. According to reports it seems that the attackers stole the debit card database and sold on a designated credit card Darknet market. Russian hackers purchased the information and then duplicated the cards and tried to withdraw money with them. It is unclear if the attackers had access to the bank's balance management systems. Following the attack, BankIslami halted all withdrawals outside of Pakistan.

We believe that that this attack was not executed by any of the groups we are currently monitoring, which conducted the attacks on banks in Asia and Latin America during this year (i.e. Russian and North Korean actors). The attack vector indicates it was a lone hacker that took advantage of a compromised database.

Mumbai Branch of State Bank Hacked; $4 Million Stolen

In early October, it was reported by Indian news outlets that a Mumbai branch of State Bank of Mauritius (SBM) was breached, and $4 million were successfully taken, out of an attempt to steal $20 million[75]. Currently it is believed that behind this attack is the same North Korean group that also hacked Cosmos Bank.

The heist was identified by the London bank[76], after its officers got suspected due to the unusable number of remittances carried out within just a few hours. The bank then sent an email for verification SBM.

The attackers had control of SMB's email server, however due to a mistake on their behalf, one of the banks officers successfully sent a response to the London bank stating that the transaction is not authorized. Concurrently the attackers sent a fraudulent response of their own claiming that transaction is legitimate.

The double response alerted the banks and prompted them to look into the matter, and later block most of the remittances. Consequentlythey were able to retrieve most of the money, with the exception of four million dollars.

Attack on HSBC Compromises Sensitive Personal and Financial Customers' Data

HSCB discovered that an unknown attacker accessed several clients' accounts between the October 4th and October 11th, 2018. The bank notified affected clients, stating that their[77] account is impacted and that they suspended online access to prevent further unauthorized entry.[78]

The information that was likely exposed includes full names, email addresses, phone numbers, birth dates, account numbers and account types, account balance, transaction history, payee account information, and statement history. The letter did not include information about how the attack occurred, but that HSBC is improving its authentication process for personal accounts, and that a layer of information security was added to the login system.

The bank's spokesperson stated that during October, that the bank's monitoring team detected that an authorized user accessed a few accounts. Subsequently, the bank suspended use of these accounts immediately, and asked

74 https://propakistani. pk/2018/10/31/heres-how-and-why-bank-islami-accounts-were-hacked/
75 http://pushpmagazine.com/hackers-hacked-server/
76 https://indianexpress.com/article/cities/mumbai/cyber-fraud-state-bank-of-mauritius-case-lodged-5400004/
77 https://securityaffairs.co/wordpress/77761/data-breach/hsbc.html
78 https://oag.ca.gov/system/files/Res%20102923%20PIB%20MAIN%20v3_1.pdf

the impacted account owners to contact the bank. He also added that because of the recent attack, the bank safeguarded its authorization and login processes, and added more layers of protection for mobile device login. This is done by adding information details required to log in to the account. From this we can conclude that HSCB is implementing the two-step authentication method to its systems.

The spokesperson stated that he believes that the attack was of the "credential stuffing" type. The clients used their bank passwords for other interfaces. The attackers hacked into those interfaces and used their login details on their bank accounts. He states that it is nearly impossible that the login details were stolen from the bank's systems.

FASTCash – Lazarus campaign targeting ATMs

On October 2, the US-CERT issued an alert[79] (TA18-275A) regarding a new cash-out scheme campaign by the North Korean APT Lazarus (aka Hidden Cobra), in which tens of millions of dollars were stolen. According to the FBI, the DHS and the U.S. Treasury, the campaign primarily targets banks in Africa and Asia.

Each attack affects multiple banks around the world. For example, in one attack executing during 2017, Lazarus simultaneously cashed-out ATMs located in over 30 different countries. In another attack executed in 2018, the group withdraw cash from ATMs in 23 different countries. At the time of the alert's publication, the U.S. Government has not confirmed any FASTCash incidents affecting institutions within the United States. However, it was also stated that the investigation is still undergoing to determine whether it targets any banks in other regions.

Other than the direct loss of money, such an attack can cause to a targeted organization: temporary or permanent loss of sensitive or proprietary information; disruption to regular operations; financial costs to restore systems and files and potential harm to an organization’s reputation.

The attackers first target the bank's employees via spear phishing; however currently, the exact infection vector is unclear. Nevertheless, it is known that they use Windows-malwares as well as legitimate credentials to laterally move through a bank’s network in order to execute transactions and interacting with various financial systems, including the switch application server. Lazarus uses their knowledge of the international standard for financial transaction card - ISO8583 - to intercept and manipulate cash withdrawals request.

- The investigators believe that Lazarus blocked transaction messages to stop denial messages from leaving the switch and used a GenerateResponse* function to approve the transactions. These response messages were likely sent for specific PANs matched using CheckPan verification
- If the requestdoes not contain the attackers' account number then the server will transfer the withdrawal requestas regular transaction requestvia the bank systems.
- If the requestdoes contain the attackers' account number then via the GenerateResponse function (1 or 2) the malware creates a fake response before the withdrawal approval arrives to the legitimate bank's systems.
- One more function the malware has is intercepting and even blocking denial of withdrawal notices.

DarkVishnya – Attacks on Banks via Dedicated Hardware Devices

Throughout 2017 and 2018, a series of cyber attacks with the same attack method was discovered – connecting a dedicated hardware device directly to the local network of the attacked bank. In this attack series at least **eight**

79 https://www.us-cert.gov/ncas/alerts/TA18-275A

eastern European banks were attacked. The damage caused is estimated at tens of millions of dollars. All the [80] attacks in this series have a few similar stages, detailed below:

First stage of attack - The attacker enters the bank branch or office disguised as a courier, or someone looking for work. He then looks for an opportunity to connect the hardware device to the local network. For example, an exposed connection in the waiting room, in the self-service area, or nearby the bathroom. The attackers choose devices according to their professional preferences and capabilities. When they were investigated, the following devices were exposed:

- A laptop or netbook.
- A Raspberry Pi computer – a computer the size of a credit card that connects to a computer or monitor.
- Bash Bunny – A special tool for carrying out a USB attack. After inserting the device, it appears in the network as an unknown computer, hard drive or keyboard. Remote access to the planted device was via a built-in or USB-connected GPRS/3G/LTE modem.
- Note that during simulation drills, we inserted a hardware device disguised as a computer keyboard. It was connected to a satellite phone, making detection difficult.

Second stage of attack - the attackers remotely connect to the device and scan the local network seeking to gain access to public shared folders, web servers, and any other open resources. The aim is to harvest information about the network, servers and workstations used for making payments. At the same time, the attackers try to brute-force or sniff login data for such machines. To overcome the firewall restrictions, they plant shellcodes with local TCP servers. If the firewall blocks access from one segment of the network to another, but allows a reverse connection, the attackers use a different payload to build tunnels.

The attackers searched for privileged connection details for devices and computers in order to bypass the network's security restrictions. The attackers planted shellcodes, which direct to the local TCP server. In case the firewall blocks entrance of one code segment from one network to the other, but enables the path the other way them, the attackers used a different payload to create tunnels.

Third stage of attack - the attackers connect to the attacked system while using remote access software to retain access. The attackers used the tool msfvenom, which is a combination of Msfencode and Msfpayload.

The attackers used fileless and Powershell attacks, and in doing so evaded detection by security systems and whitelisting. It appears that they used winexesvc.exe and psexec.exe files in order to remotely run files.

Three US Payment Processing Companies Fell Victim to BGP/DNS Hijacking Attacks

On August 8, Oracle exposed a sophisticated BGP[81] hijack campaign targeting DNS servers of three US payment processing companies Datawire, Vantiv and Mercury Payment Systems. The first attack took place on July 6, followed by additional attacks throughout July.

Attack vector - BGP (Border Gateway Protocol) is a standardized routing protocol used to makes routing decisions based on various factors such as paths, network policies, and/or rule-sets configured by network administrators.

BGP/DNS hijacking enables the attackers to redirect users from legitimate websites to fraudulent ones under their control in order to steal their account credentials. Accordingly, this is often used to target users of financial services. For example, in April this vector was used against users of a cryptocurrency wallet service. In this attack attackers

[80] https://securelist.com/darkvishnya/89169/
[81] https://en.wikipedia.org/wiki/Border_Gateway_Protocol

stole $160,000 USD worth of Ethereum coins from MyEtherWallet users by redirecting them to a fake version of the site hosted in Russia.

Timeline – on July 6, the Indonesian ISP Digital Wireless Indonesia, announced that they detected a short-lived attack that attempted to reroute network prefixes or blocks of IP addresses. These attacks targeted Vantiv and Datawire payment processing. Several days later on July 10 the Malaysian ISP Extreme Broadband reported a similar attack on the exact same prefixes targeted in the previous attack; however, this time the attack lasted for 30- minutes. The attackers executed additional attacks throughout July, including one against Mercury Payment Systems. One of the attacks on Vantiv and Datawire lasted 3 hours.

Re-routing - according to Oracle, passive DNS observations between the 10th and 13th of July showed that datawire[.]net domains resolve to IP 45.227.252.17. This address is registered to the Dutch Caribbean island of Curaçao, however it routed out to the region of Luhansk in eastern Ukraine. This indicated a possible link to the April attack, in which domains that resolve to an IP in Germany (46.161.42.42) also routed out of Luhansk.

It appears that the July attacks were executed with great attention to detail. For example, the attackers set the TTL (Time to Live) of the forged response to about 5 days, as opposed to the normal TTL of the targeted domains which was only 10 minutes (600 seconds). By configuring a lengthy TTL, the attackers can achieve persistency in the DNS caching layer for extended period of time, even after the BGP hijack stops.

Conclusion - it appears that malicious actors are getting more proficient in executing these types of attack. As a result, it is likely that we will continue seeing these types of attacks against high-value targets in the near future. It is unclear how to prevent this vector; however, security expert and IP development engineer at NTT Communications, Job Snijders, believes that consolidation of the internet industry might help mitigating such attacks[82].

More specifically he suggested that major DNS service providers sign their routes using RPKI, and validate routes received via EBGP. Snijders claims that doing so might reduce the impact of attacks because protected paths are formed back and forth.

North Korean Actor Lazarus Targets Turkey's Financial Sector

On March 8, 2018, a report by McAfee's security blog[83] reviewed the recent campaign attributed to the North Korean Lazarus threat agent. The campaign targets financial institutions in Turkey for espionage-related purposes, most likely in order to carry out a future heist. As part of the campaign, there was a repeated use of previous Lazarus tactics, including the use of the group's unique Trojan, Bankshot, as well as the use of similar code sections.

According to McAfee's analysis, targeted emails were sent to Turkish victims starting February 28, 2018. The emails contained malicious word documents leveraging the recent Adobe Flash vulnerability (CVE-2018-4787), which was first exploited by North Korean threat agent APT 37 (Reaper) in November 2017[84]. (APT 37, as well as groups such as Scarcruft and Group123[85], primarily focuses on social engineering and individual targeted attacks).

The infection in Turkey occurred between March 2 and 3. The targets of this campaign included a state-run financial institution, immediately followed by a Turkish government organization involved in finance and trade. Later, three other large financial institutions in Turkey were infected. Bankshot was not detected in attacks on other sectors or countries.

[82] https://www.v3.co.uk/v3-uk/news/3037173/three-us-payment-processing-companies-dns-servers-hit-by-bgp-hijacking-attacks-claims-oracle
[83] https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-.implant
[84] https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
[85] https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html

Connection with Lazarus - The structure of the commands sent to the C2 server are similar to those detected in the Bluenoroff sub-group's attack on one of the five largest banks in South Korea. In addition, samples from the latest Bankshot campaign are highly similar to previous versions of Bankshot seen in other campaigns. In 2017, Bankshot payloads were spread through Word documents containing contents concerning the financial and cryptocurrency sector, similar to the tactic used in the current campaign.

Infection vector - The infection was carried out by spreading a Remote Access Trojan (RAT) uniquely used by Bankshot, using a domain similar to one used by a cryptocurrency stock exchange called Falcon Coin, but which does not belong to it. The domain, falcancoin[.]io, was registered on December 27, 2017 and was updated on February 19, 2018 – several days before the implants began to appear.

Dutch Banks and Tax Office Hit by a Series of DDoS Attacks

Between January 27 and 29, 2018, several Dutch banks and the Netherlands' tax office, were hit by a series of DDoS attacks[86]. Each attack was between several minutes to several hours long, denying users access to the banks' websites and apps. However, it should be noted that no money was stolen and no sensitive data was compromised. According to reports it appears that some of the attacks used Zbot, a Windows based Trojan. Dutch security researcher Ricky Gevers[87] reported that the attacks were up to 40Gbps.

According to ESET, most of the traffic originated from Russia[88]. However, the researchers pointed out that this does not necessarily indicate that the attackers were also in Russia. Nevertheless, these attacks did take place several days after Dutch media published a report claiming that Dutch Secrete Service (AIVD), are monitoring and investigating the Russian threat agent APT29 (aka Cozy Bear) – a nation-state group attributed to the Russian government. This group has been link to numerous cyber-attacks, including the attack on the Democratic Party during the 2016 US elections.

TCM Bank Data Breach - Credit Card Applicant's Info Leaked for 16 Months

On August 3, 2018, TCM Bank, a company that provides credit cards services to over 750 small and community U.S. has leaked sensitive information of applicants for close to a year and a half, due to a Website misconfiguration[89]. The compromised data includes, names, addresses, dates of birth and Social Security numbers of about 10,000 individuals who applied for cards between early March 2017 and mid-July 2018.

About 25% of all applications that were processed during the relevant time period. TCM Bank, who is a limited-purpose credit card bank and fully owned subsidiary of ICBA Bancard, discovered the breach on 16 July 2018, and allegedly resolved the issue the following day.

86 https://koddos.net/blog/dutch-banks-tax-office-hit-ddos-attacks/
87 https://twitter.com/UID_?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor
88 https://nltimes.nl/2018/01/29/russian-servers-linked-ddos-attack-netherlands-financial-network-report
89 https://krebsonsecurity.com/2018/08/credit-card-issuer-tcm-bank-leaked-applicant-data-for-16-months/

Cryptocoin Heists in 2018

Below is a review of the most significant events that took place or were exposed this year

Largest Recorded Cryptocurrency Heist Hits Japan's Coincheck

On January 26, 2018, cybercriminals stole $523 million worth of NEM coins from the Tokyo-based **Coincheck** crypto-exchange in a matter of minutes.[90] The tokens were stored in a low-security "Hot Wallet," which exposed them to attackers and facilitated the heist, already labeled as "the biggest" crypto heist on record.[91] The biggest sums stolen from the crypto-market, according to extent of financial damage, are as follows:

Market	Financial lose	Year
Coincheck	**$530 million**	**2018**
Mt Gox	$480 million	2014
BitGrail	$170-195 million	2018
Parity Wallet	$155 million	2017
Bitfinex	$65 million	2017
NiceHash	$63 million	2017
Zaif	$60 million	2018
DAO	$50 million	2016
Coinrail	$40 million	2018
Bithumb	$40 million	2018
Tether	$31 million	2017
Bancor	$23 million	2018
Trade.io	$7.5 million	2018

[90] https://www.deepdotweb.com/2018/04/09/coincheck-hackers-have-laundered-all-of-their-nem/
[91] https://hacked.com/nem-theft-suggests-hacking-is-more-lucrative-than-mining/

NEM, also known as XEM, is a cryptocurrency that was launched on March 31, 2015 and is particularly popular among investors in Japan. Its market value currently stands at $3.5 billion, which places it among the top 15 cryptocurrencies in the world.

The attacker's initial penetration vector was most likely carried out with Spear Phishing emails. Research of the incident revealed that in the weeks leading up to the heist, there were suspicious communications between Coincheck hosts and unidentified servers. These servers were most likely used as C2 infrastructure of the currently **unidentified attacker**, whom researchers estimate is based in North Korea.

In early February 2018, two weeks after the heist, the attackers began laundering and liquidating the stolen funds. Using a darknet website called "The Exchange Cryptocurrency," the criminals launched an automated makeshift platform set up for trading NEM tokens for Bitcoin and Lightcoin, in rates 15% lower than current market value.

This lured interested buyers to purchase stolen coins in exchange for other legitimate cryptocurrencies.[92] This method effectively made the stolen NEM impossible to trace. The exchange platform also offered onsite technical support for potential buyers via "support tickets," which received replies shortly after being submitted.

Soon after the heist was made public, in an attempt to prevent the attackers from liquidating the stolen funds, the NEM Foundation began tagging all associated wallets containing stolen tokens with a tracking system called Mosaic. The attempt ultimately proved unsuccessful as criminals found numerous methods of circumventing the blacklist, such as creating numerous wallets and repeatedly moving the funds among several accounts, throwing off the tracker.

In March 2018, the NEM Foundation announced that it would no longer track the stolen funds,[93] despite claiming that the effort "was effective at reducing the hacker's ability to liquidate stolen XEM and provided law enforcement with actionable information." This decision most likely stemmed from the practical difficulty of tracking such a massive amount of currency transactions.

Moreover, the Mosaic system functioned in an inefficient manner, taking about 2-3 minutes to tag an individual account; this enabled the criminals to transfer the funds between several accounts after one was tagged. Moreover, the process significantly slowed down such transactions. In April 2018, the makeshift crypto-exchange was removed from the website and was replaced with a photoshopped image of North Korea's smiling and apparently mocking leader, Kim Jong-un, surrounded by piles of cash. This change signifies that the attacker has terminated its laundering operation.

Immediately after the heist, Japan's financial regulator (FSA) issued new compulsory security measures for cryptocurrency market operators in the country. In addition, FSA sent Coincheck a "business improvement order" under threat of license revocation, in an effort to prevent similar heists from happening in the future. In response, Coincheck announced it would partially reimburse impacted customers with a total of $400 million. The company also issued a formal apology and said it has a reinforced its security infrastructure in a multiple-day operation.

$195 Million Dollars in Cryptocoins Stolen From BitGrail

In February, $195 million dollars' worth of Nano (formerly known as Raiblocks XRB) cryptocoins were stolen from the exchange market BitGrail[94]. The developers of Nano and BitGrail have blamed each other for the breach, and the exchange even issued a law sued against the former. Following these events Nano's market value crashed. BitGrail has promised to refund customers 20% of their funds, with an additional 80% if they sign a contract agreeing not to sue them.[95]

92 https://btcmanager.com/coincheck-hackers-may-have-successfully-laundered-all-their-stolen-nem-coins/
93 http://www.livebitcoinnews.com/nem-foundation-removes-tracking-mosaic-stolen-coincheck-funds/
94 https://www.ccn.com/17-million-nano-xrb-lost-on-bitgrail-exchange/
95 https://thenextweb.com/hardfork/2018/03/15/bitgrail-nano-hack-cryptocurrency

Two Major South Korean Crypto Exchanges Fall Victim to Cyber Attacks

On June 20, 2018, major South Korean cryptocurrency exchange Bithumb announced it was suspending all deposit and withdrawal services after $30-$35 million worth of cryptocurrency was stolen from the exchange in an attack. Bithumb clarified it would reimburse clients affected by the incident that it is transferring all assets to a cold wallet while systems are secured. [96]

It is worth noting that Bithumb's announcement came just a few days after the company carried out a security upgrade in its systems, due to experiencing an increase in the number of unauthorized access attempts by attackers.[97] The announcement about the heist was made in a post on Twitter, which has since been deleted[98] and replaced with request that clients avoid making deposits until further updates are provided:

The exact extent and nature of this incident is unclear, as Bithumb refrained from providing additional details. The attack vector is likewise unknown, although the South Korean news agency Yonhap has cited sources that claims hackers leveraged malicious emails sent to Bithumb's users in early June.[99] In a statement on its website, Bithumb said it would provide further information about the incident in due course. Meanwhile. the cybersecurity division of South Korea's National Police Agency has been sent to Bithumb's offices in Seoul to investigate the incident.

The Bithumb attack is the second logscale crypto-heist South Korea has experienced within two weeks. On June 10, 2018, a top cryptocurrency exchange named Coinrail was hit by an attack that resulted in the theft of about $40 million worth of cryptocurrency. Coinrail notified the public about the theft in a blog post one on June 11. In its announcement, the exchange confirmed it had suspended its services after a "cyber intrusion" was detected in its systems during the early morning of June 10, 2018.[100]

Coinrail clarified that 70 percent of its reserves remain safe, as they have been moved to a cold wallet. As for the 30 percent that were compromised, two-thirds of these are currently frozen, while the fate of the final third is currently being investigated with the help of law enforcement authorities.

Bancor Crypto-currency market hacked, $23 million stolen

On July 9, the crypto-currency exchange platform Bancor announced that it is disabling its operation and services following a breach. The attackers stole Ethereum coins worth $12 million dollars, as well as $10 million worth of the company's in-house crypto-coin BNT. Their in-house coin BNT (Bancor Network Token) publicly became tradable on June 2017. It is also used by Bancor as a platform to quickly and cheaply exchange various crypto-coins. This is done automatically, and with no third-party intervention, by changing the coins to BNT and then to the requested crypto-coin.

As Bancor controls the operation of their coin, they were able to freeze its transactions and thus minimized the loss. While they were only able to do so with their coin token and not with other crypto-currencies, Bancor is claiming that it's working with other crypto-exchange markets to try and located the stolen funds. According to the company, their clients are not affected, and no funds were directly stolen from them, however the value of BNT has dropped significantly due to these events.

96 https://www.theguardian.com/business/2018/jun/20/south-korea-bithumb-loses-315m-in-cryptocurrency-heist
97 https://www.coindesk.com/bithumb-exchanges-31-million-hack-know-dont-know/
98 https://bitcoinexchangeguide.com/developing-bithumb-hack-story-fake-news-insider-job-or-back-tax-bill-ploy/
99 http://www.yonhapnews.co.kr/bulletin/2018/06/20/0200000000AKR20180620126300017.HTML?from=search (Note: Korean language)
100 https://www.ccn.com/korean-cryptocurrency-exchange-coinrail-suffers-40-million-theft/

Hackers stole $7.5 Million From Trade.io Cold Crypto Wallet

On October 22, it was reported[101] that hackers stole 50 million TIO (Trade Tokens) worth 7.5 million dollars from the Swedish crypto company Trade.io (located in Israel). The money was stolen from the company's cold wallet that was used for keeping its tokens, and not from clients' personal accounts.

Trade.io posted on their official website[102] that on the 20th of October, at 08:40 EST, their security team received an alert about a large transaction from their wallet valued at 50 million TIO. They immediately stopped withdrawals and deposits from and to the wallet, and also stopped trade with the company's tokens.

The breach was performed on a cold wallet based on a USB device containing login details to accounts. The device was stored in a safe in a bank. Trade.io confirmed that the safes and devices were not taken, and does not know how their wallet was hacked.

Trade.io added that the tokens were stolen from their liquidity pool, and were also transferred via companies working with them – Kucoin and Bancor. These companies are now assisting with the investigation and have also temporarily blocked withdrawal, deposit and trade with the TIO tokens. The theft does not affect the company's day-to-day trade activities, and the platform will continue to operate normally.

The CEO noted that although they do not know who stole the money, hacking into cold wallets can happen even when there are special security measures guarding the money. Trade.io uses cold storage services such as safes in banks that were not stolen. Therefore, the group responsible for the theft did not have access to the company's storage services, but was able to obtain the wallet address necessary to perform the transactions.

Note that a cold wallet is comparable to an encrypted wallet file disconnected from the internet on an HSM/computer. Stealing from a cold wallet can be done by the following methods:

1. Inside job – an employee who had information, stole or utilized the information.
2. The wallet was not really "cold" and was exposed because it was connected to the internet. Alternatively, the information protection procedures of the wallet's details might not have been adequately protected.
3. The company did not adequately protect the wallet's passwords and details.
4. The wallet seller (unclear how the wallet was purchased) kept the identification details of the wallet.
5. The attackers were able to bypass the Air Gap through sophisticated methods.

$150,000 dollars in Ethereum coins stolen via DNS Hijacking

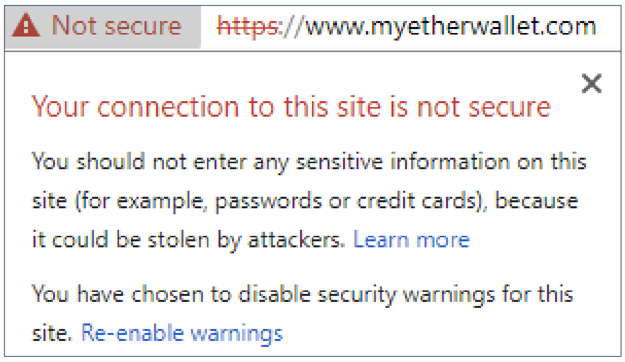
On April 23, 2018, hackers conducted an attack against users of the online Ethereum wallet service - Myetherwallet. An estimated 216 Ethereum coins valued at $150,000[103] were stolen in this incident.[104] The attack was carried out with DNS hijacking, which redirected victims to a phishing website spoofing the popular service. The attackers then stole wallet details and credentials from the redirected users.

This tactic was executed by publishing a more specific IP prefix in the network hosting the Amazon DNS service (Route 53). As a result, several internet networks began routing the traffic of 1,300 Amazon IP addresses to a network in Russia, where the threat actor's C2 server is located. During the hijacking, DNS queries for myetherwallet.com (whose authoritative server belong to Amazon's Route 53 service) received an IP address of a

[101] https://www.zdnet.com/article/trade-io-loses-7-5mil-worth-of-cryptocurrency-in-mysterious-cold-wallet-hack/
[102] https://trade.io/en/news/contains-breach-protects-tio-holders
103 https://www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum
104 https://wccftech.com/hackers-domain-service-to-empty-ethereum-wallets/

server controlled by the attackers, which consisted of a phishing page spoofing the legitimate website. The attack was exposed shortly after it began and the company warned its users on Twitter[105] some 15 minutes later.

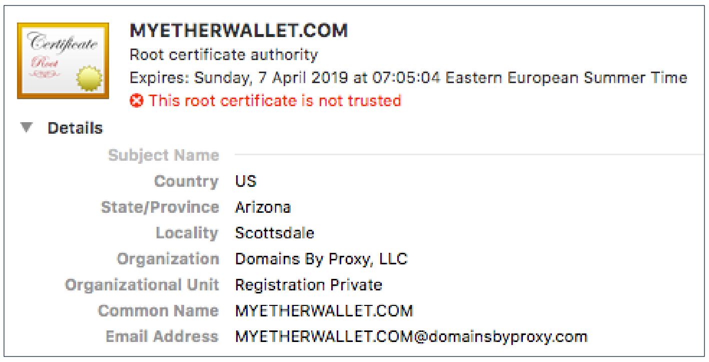
Please note that the fictitious website had an unofficial SSL certificate. Most users, depending on their choice of web browser, received a warning upon entering the website; nevertheless, many users opted either to ignore the warning or avoid reading it.


Not secure ~~https~~://www.myetherwallet.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings


MYETHERWALLET.COM
Root certificate authority
Expires: Sunday, 7 April 2019 at 07:05:04 Eastern European Summer Time
This root certificate is not trusted

Details

Subject Name
Country US
State/Province Arizona
Locality Scottsdale
Organization Domains By Proxy, LLC
Organizational Unit Registration Private
Common Name MYETHERWALLET.COM
Email Address MYETHERWALLET.COM@domainsbyproxy.com

For about two hours, numerous users fell victim to the scam and the criminals began shifting the stolen coins between various wallets, distributing them into smaller sums so as to cover their footprints. The original wallet to which the stolen coins were transferred had contained over $17 million in Ethereum. The identity of the attackers is currently unknown; however, we believe a Russian cybercriminal group is behind the attack, possibly even Carbanak.[106]

This incident is just one of in a series of DNS hijacking attacks against cryptocurrency platforms and users. For example, in January 2018, criminals used this method to steal $400,000 in Lumens.[107] Moreover, in December 2017, 267,000 Ethereum coins were stolen from the EtherDelta website.[108]

"HaoBao" – North Korean Bitcoin-Stealing Phishing Campaign

On February 12th, the McAfee research team published an article exposing an aggressive Bitcoin-stealing phishing campaign executed by the North Korean threat agent Lazarus[109]. The campaign, known as HaoBao (Vietnamese for "wallet") uses tactics and methods that were previously utilized in early 2017 during a spear phishing targeting well-known key financial organizations, crypto currency exchanges, as well as private Bitcoin wallet holders.

The penetration vector of the malicious .doc files that were utilized is implanted in Dropbox addresses. The report did not mention how those arrived at their target destination. The dropped malicious files masqueraded as various job recruitment offers, for example:

- Business Development Executive post located in Hong Kong for a large **multi-national bank**
- Relationship Director specializing in **corporate banking**
- Engineering Manager specializing in cryptocurrency

The documents are embedded with a malicious macro that contains a data gathering malware. Note that the malware achieves persistency by creating a shortcut in the user's Startup folder. The implant receives a unique string through the command line, which constitutes a confirmation for the malware processes to begin.

105 https://twitter.com/myetherwallet
106 https://www.kaspersky.com/resource-center/threats/carbanak-apt
107 https://bitcoinmagazine.com/articles/blackwallet-hacked-warns-stellar-community-not-log-site/
108 https://mashable.com/2017/12/21/etherdelta-hacked/#sAVWX0dMtqql
109 https://securingtomorrow.mcafee.com/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/

Attacks on the Healthcare Sector

Below is a review of several of the most significant events that took place or were exposed this year

Over the last few years, due to its sensitive nature amongst other reasons, the healthcare sector systematically has been one of the most targeted sectors, with the number of attacks growing from one year to the next. One of the most notable increases are of ransomware attacks. Due to the critical nature of hospitals and healthcare providers, and the extensive and possibly immediate damage that can take place if systems are shut down, these organizations are invariably forced to pay the ransom.

Moreover, it should be stated that the actual scale of attacks would appear to be considerably larger than official numbers indicate, as many events are under-reported or even unreported. It seems that many healthcare companies and organizations choose not to report ransom attacks, regardless whether the ransom was paid, believing that the data was only deleted without considering whether the attackers may have copied it with an intent to sell.

Another concerning issue is that many healthcare organizations fail to adopt DMARC standard that help prevent phishing attack. Despite the prevalence of email-based cyber attacks in healthcare and across other industries, a study by mail authentication vendor Valimail, published in May, found that the majority of healthcare organizations are not sufficiently protected against impersonation and phishing attacks and do not employ DMARC, an open standard designed to detect and prevent email spoofing and domain abuse.[110]

The Domain-based Message Authentication, Reporting and Conformance (DMARC) standard, an email-validation system that is designed to detect and prevent email spoofing was found to be rarely used in any capacity across the health sector, according to the report. Valimail discovered that 98.3 percent of the healthcare companies analyzed were susceptible to being impersonated by phishing attacks directed at employees, partners, patients or others. DMARC is designed to fit into an organization’s existing inbound email authentication process. When a DMARC record is created for a domain, the receiving server checks to determine whether the sender of the message is authorized to use the domain.

For the study, the vendor analyzed the domains of 928 healthcare companies around the world (with annual revenues of over $300 million). These include hospitals, medical equipment suppliers, pharmacies, physicians and health practitioners. Just 121 of those companies (13%) have adopted DMARC to secure their domains and prevent email spoofing.

[110] http://www.healthcareitnews.com/news/despite-email-attacks-healthcare-still-not-using-dmarc-protect-against-spoofing

These findings are concerning, as a new report on data breach found that Healthcare is the only sector in which internal actors are behind most cyber incidents. After error and misuse of data, ransomware was found to be the most common ailment plaguing the healthcare industry (85 percent of all malware propagated in the sector).[111]

Verizon's 2018 Data Breach Investigations Report (DBIR), released on April 10, 2018, found that the majority of cyber security incidents in healthcare, while not all malicious in nature, resulted from the actions of internal actors (57 percent), more so than any other sector studied. For the most part, this stems from the fact that healthcare workers have a direct and daily access to the personal information of patients.

The leading motive behind data breaches in the health sector was found to be financial gain (75 percent), after which are curiosity and fun (13 percent). Other incidents were simply actions taken for the personal convenience of the perpetrator who wishes to avoid certain red-tape procedures and security standards (5 percent). At the bottom of the list of motives are grudges, espionage and other/unknown reasons (< 5 percent). The most common type of compromised data in the healthcare industry is medical information (79 percent), followed by personal information (37 percent) and lastly, payment data (4 percent).

However, in early August, new standards named OWASP Secure Medical Device Deployment Standard V2., were announced. These were developed by Cloud Security Alliance[112] (CSA), in conjunction with the Open Web Application Security Project[113] (OWASP). These new standards, follow a significant increase of attacks targeting IoT devices in recent years, and the growing need of adequate security protocols in deploying medical devices.

Version 2.0, was developed in conjunction with the CSA IoT working group and with assistance by the Federal Drug Administration, and has numerous improvements and comprehensive updates, especially in regard to purchasing controls. According to Info-Security Magazine[114], "the changes to support evaluation controls are intended to better guide the secure deployment of medical devices within a healthcare facility."

Multiple Vulnerabilities Discovered in Popular Healthcare Software Potentially Putting at Risk 90M Patients

Researchers at Project Insecurity[115] published on August 8, a report with their findings of over 20 serious issues with open source electronic health record (EHR) and practice management tools developed by OpenEMR[116]. Amongst the issues are nine separate SQL injection vulnerabilities, four remote code execution flaws and several arbitrary files read, write and delete bugs. Other problems include a portal authentication bypass, unauthenticated information disclosure, and cross-site request forgery.

The security firm informed the company on July 7, and gave it a month to resolve the flaws before publicly reporting on the matter. OpenEMR issued a statement [117]on August 8, saying that "The OpenEMR community takes security seriously and considered this vulnerability report high priority since one of the reported vulnerabilities did not require authentication."

Orangeworm – Large-scale Attack Campaign on the Healthcare Sector

In April, Symantec exposed an attack campaign targeting the healthcare sector and its supply-chain in the United States, Europe and Asia, according to a report by Symantec from April 23, 2018.[118] Behind the campaign is a group dubbed Orangeworm, a previously unknown threat actor. It was observed installing a custom-made backdoor called Kwampirs on international targets within and related to the healthcare sector, including **pharmaceutical companies, IT solution providers for the healthcare industry, and medical equipment manufacturer**s, as part of

111 http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf
112 https://cloudsecurityalliance.org/
113 https://www.owasp.org/index.php/Main_Page
114 https://www.infosecurity-magazine.com/news/improved-standards-for-securing/
115 https://insecurity.sh/assets/reports/openemr.pdf
116 https://www.open-emr.org/
117 https://www.bbc.co.uk/news/technology-45083778
118 https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

a supply-chain attack designed to reach **deliberately and meticulously chosen targets** within the health sector, likely for espionage purposes.

The origin of Orangeworm is currently unknown, as there are currently no technical or operational indicators. The group likely consists of an individual or a small number of individuals, as opposed to being a nation-state actor. appears to conduct well-planned strikes on its targets. According to Symantec, almost 40 percent of Orangeworm's confirmed victims operate within the healthcare industry, while attacks on other industries such as Manufacturing, Information Technology, Agriculture, and Logistics were also intended to reach targets in healthcare. Notably, the group has deployed the backdoor on medical imaging devices such as X-Ray and MRI machines, as well as machines used to assist patients in completing consent forms.

Once deployed, Trojan.Kwampirs allows the attackers to remotely access the compromised host. After ensuring its persistence, the malware collects initial information on its victim to determine whether the target is of high-value. If the victim proves to be of interest to the threat actor, Kwampirs then collects additional network information to facilitate its propagation, which the malware carries out by copying itself over network shares.

This method is suitable for older operating systems such as Windows XP, which are in prevalent use across the healthcare industry. Despite slightly modifying itself while moving across a network to evade detection, Orangeworm does not appear too concerned about being discovered and uses "aggressive" and "loud" methods to propagate the malware and communicate with C2 servers.

Attack Campaign by Tropic Trooper Hacking Group Targeting Healthcare Providers

On March 14, cyber security company Trend Micro reported[119] an on Tropic Trooper hacking group campaign against Taiwanese, Philippine, and Hong Kong healthcare providers. Unlike many other threat actors, Tropic Trooper (aka KeyBoy) develop their own tools, which they also continuously maintain and upgrade.

As TrendMicro stated, "many of the tools they use now feature new behaviors, including a change in the way they maintain a foothold in the targeted network." Moreover, the group appears to be highly organized and capable. Other than healthcare providers they also focus their efforts on the aforementioned governments, transportation, and high-tech industries.

The group exploit flaws in Microsoft Office document to deliver malware to their targets. The documents are job vacancies applications with content that TrendMicro claim is presumed to be "socio-politically sensitive to recipients". Note the document does not require to download anything as the backdoor's dropper is already embedded in it. This does not however affect the end result for the victim.

Once executed, the backdoor loads the encrypted configuration file and decrypts it. After that it uses SSL protocol to connect to C2 servers. The malware executes commands through exploits for CVE-2017-11882[120] or CVE-2018-0802[121].

Healthcare Data Compromise Incidents Due to Misconfiguration of Servers and Databases

Improper configuration of servers and/or databases can result in sensitive data being exposed and potentially exploited by malicious actors. This problem affects all industries, however due to the critical nature of the sector this issue can cause considerable harm, including possibly even loss of lives. Below are several examples from 2018 the illustrate the problem.

119 https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/?utm_source=trendlabs-social&utm_medium=smk&utm_campaign=03-2018-tropic-trooper-new-strategy
120 https://nvd.nist.gov/vuln/detail/CVE-2017-11882
121 https://nvd.nist.gov/vuln/detail/CVE-2018-0802

Confidential Data of 33,400 BJC HealthCare Patients Compromised due to Misconfigured Server

Missouri-based non-profit BJC HealthCare has notified[122] 33,420 patients that a misconfigured server has compromised their confidential information, which was easily accessible through the internet for over eight months. Between May 9, 2017 and January 23, 2018, a data server configuration error made it possible for stored images of identifying documents to be accessible through the internet without the appropriate security controls.

Among the documents stored on the compromised server were copies of patient driver's licenses, insurance cards, and treatment-related documents that were collected during hospital visits spanning 2003 to 2009. Patient information that was potentially accessible included name, address, telephone number, date of birth, Social Security number, driver's license number, insurance information and treatment-related information. According to BJC's statement, no personal data has been accessed.

Third-Party Vendor Exposes Data of 19K Patients For 2 Months Due to Misconfigured Database

On August 2, 2018, Orlando Orthopedics' transcriptionist vendor reported that due to a misconfigured access to a database during a software upgrade, data of 19 thousand patients was exposed for two months. The vendor conducted the upgrade throughout December 2017, however during the time it neglected to take necessary measures, resulting in the server being publicly exposed and accusable with no authentication.

According to the investigation, the breach exposed patient names, dates of birth, insurance details, employers and medical treatment. Further, the vendor stated that a "limited number of patients" had their Social Security numbers were possibly compromised[123].

Moreover, the report did not provide an explanation to the reason the vendor waited close to a half a year before issuing a notification on this matter. This far exceeded the HIPAA's (Health Insurance Portability and Accountability Act) "grace-period", during which organizations must report to the U.S. Department of Health and Human Services within 60 days from the discovery of a breach.

It is expected that Orlando Orthopedic will receive a substantial fine for delaying the report. In a similar example, healthcare provider "Presence Health" was fined in January 2017, $475,000 for waiting 100 days before reporting, only 40 over the mandatory time.

Telemedicine company Hova Health Exposed Data of over 2M patients

On August 8, 2018 it was reported[124] that Healthcare Firm exposed data on two million Mexican citizens, due to a misconfigured MongoDB installation. This breach was detected by Bob Diachenko, formerly of the Kromtech Security Center via a simple Shodan search. According to Diachenko the data was publicly viewable and editable with no password required. The exposed data included full name and gender, unique identity code, insurance policy number, DOB, home address and disability and migrant flags; as well as hashed and salted admin account passwords and email addresses.

Diachenko has stated that It is unclear how long the data was publicly exposed, nor who else except for himself had access. Hova Health responded by saying that they are investigating the matter to determine exactly what happened and, and checking their entire infrastructure to prevent such events happening in the future.

122 https://www.bjc.org/About-Us/Newsroom/BJC-News/ArtMID/897/ArticleID/3868/BJC-HealthCare-Notifies-Patients-of-Data-Storage-Server-Access
[123] https://www.healthcareitnews.com/news/third-party-vendor-error-exposes-data-19k-patients-2-months
[124] https://www.infosecurity-magazine.com/news/healthcare-firm-exposes-data-on-2m/

Misconfigured Amazon S3 Bucket Exposes Sensitive Medical Records of 20,000 iCliniq Patients

In yet another data breach involving a misconfigured Amazon S3 Bucket, the sensitive records of around 20,000 patients of a medical consultation service owned by Telemedicine were publicly exposed online. In addition, the company's web app enabled users to easily view medical questions sent by other members.[125]

The India-based online medical consultation service iCliniq has inadvertently exposed thousands of sensitive medical documents of about 20,000 patients that were stored on a misconfigured Amazon S3 bucket database. The documents, which included sensitive medical records such as blood test results and HIV tests, were left publicly available on the online cloud storage until Matthias Gliwka a security researcher in Germany alerted the company several times about the security breach in early August 2018.

The researcher said iCliniq had also failed to check for permissions in its web app, which led to an IDOR (Insecure Direct Object Reference) vulnerability. This means every user was being able to see every medical question asked by other members simply by guessing ID numbers of the questions.

Ransomware Attacks on the Healthcare Sector

Below are several notable examples from 2018 the illustrate the pandemic matter of ransomware attack affecting the sector.

Ransomware Infects Hong Kong Department of Health

The Department of Health (DOH) in Hong Kong was hit in late July by ransomware that encrypted three of its computers. The unidentified attacker left behind an email address to contact for a decryption key.[126] In a statement on August 3, 2018, a spokesperson for Hong Kong's Department of Health announced that three of the department's computers were infected with ransomware that rendered data inaccessible. The infection occurred sometime in the two weeks since July 15, 2018.

The impacted computers belonged to the DOH's Infection Control Branch, Clinical Genetic Service and Drug Office. Investigators believe the initial infection vector was a malicious attachment within an email sent to an employee. Interestingly, the unidentified attacker left an email address to contact for a decryption key; however, no ransom was demanded. Despite this fact, investigators believe that profit was the motive behind this incident.

According to the DOH's statement, the computers did not contain any confidential personal information and no data had been leaked. Moreover, the department had an offline backup of all the data stored on the infected computers. The DOH reported the incidents to the relevant local authorities and is currently investigating the circumstances that led to the event.

Hancock Health Hospital Hit with SamSam Ransomware Forcing Doctors to Use Pen and Paper, pays $55K to Recover Data

On January 11th, 2018, Hancock Health Hospital fell victim to a ransomware attack[127]. The hospital chose to pay the ransom of 4 Bitcoins, valued at $55K as of the time of the attack, after assessing that recovering their systems would be too long of a process, taking days or perhaps even weeks.

The ransomware was SamSam, a variant of SAMAS which was first seen in late 2015 when it was used against numerous healthcare organizations and hospitals. In 2018 alone, the ransomware was used against several large companies and organizations in the US, including Adams Memorial Hospital, the municipality of Farmington New

125https://www.theregister.co.uk/2018/08/03/icliniq_cloud_breach/
126 https://latesthackingnews.com/2018/08/05/hong-kong-health-department-computers-hit-by-cyber-attack/
127 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/samsam-ransomware-hits-us-hospital-management-pays-55k-ransom
http://www.securityweek.com/samsam-ransomware-attacks-hit-healthcare-firms

Mexico, cloud-based HER (electronic health records) provider Allscripts, and according to Bleeping Computer[128], an unnamed ICS (Industrial Control Systems).

First appearing in 2016, SamSam is a ransomware strain that exploits vulnerable systems to gain access to a victim's network, or uses brute-force tactics against weak passwords of the Remote Desktop Protocol (RDP). Upon gaining access to a system, the malware holds the victim's data hostage using RSA-2048 encryption. In most SamSam attacks, attackers propagate the malware by scanning the internet for systems with open RDP connections, and deploying it after breaching the targeted system via brute force attacks[129]. However, in this case it appears that the penetration vector was different – the attackers logged in to remote backup server of the hospital, which they pivoted to other more central hospital server, where they encrypted critical files.

Allied Physicians of Michiana Hit by SamSam Ransomware

On May 17, 2018, the Allied Physicians of Michiana in South Bend, Indiana, was hit by a variant of the SamSam ransomware, a prolific strain of malware known to target the healthcare sector. The practice immediately took steps to shut down the network and successfully restored its data in a secure format without causing significant disruption to patients and daily operation.[130] The Allied Physicians practice did not disclose whether a ransom was in fact demanded in this incident, nor if any sum was ultimately paid, but clarified that the incident was contained with the help of internal IT staff, its incident responder, outside assistance and other professionals. The company would not disclose any additional information about the incident.

Ransomware Hits Associates in Psychiatry and Psychology

On March 30, threat actors breached the servers of Minnesota-based Associates in Psychiatry and Psychology (APP) and encrypted all data files and disabled all system functions. The attackers demanded ransom in exchange for system restoration.[131] The attackers, who are believed to be located in Eastern Europe, infected several of APP's computers with a TripleM ransomware variant, which encrypted the files with an RSA-2048 encryption protocol. They also disabled the system restore function on all affected computers and reformatted the network storage device where the practice maintained its local backups.

After the discovery of the attack, APP's servers were taken offline for four days so that the practice could assess the situation. The attackers initially demanded 4 Bitcoin, but APP successfully negotiate the sum down to 0.5 Bitcoin, which was paid to the specified Bitcoin wallets provided by the threat actors. The compromised server stored certain demographic information such as insurance claim processing data and medical details. Credit card information was stored in a separate cloud-based bucket and was not part of the breach. APP said it had found no evidence any patient information was accessed or copied.

Phishing Attacks on the Healthcare Sector

Below are several notable examples from 2018.

UnityPoint Health Phishing Attack Impacts 1.4m Patients

In early August UnityPoint Health, a network of hospitals, clinics and homecare services in Iowa, reported that it had been victim of a phishing attack potentially impacting 1.4 million of its patients.[132] The breach occurred after a series of phishing emails were sent to employees between March 14 to April 3, 2018. The messages, which were

128 https://www.bleepingcomputer.com/news/security/the-week- in-ransomware- january-26th- 2018-samsam-and-hack- attacks/
129 https://www.bleepingcomputer.com/news/security/hospital-pays-55k-ransomware-demand-despite-having-backups/
130 https://www.apom.com/content/uploads/2018/05/FINAL_Allied-Physicians-News-Release_May-21-2018-C2-1-e1526932385481.jpg
131 https://www.appmn.com/faq/
132 https://www.scmagazine.com/phishing-attack-compromised-the-data-of-14-million-unitypoint-health-patients/article/785692/

disguised as emails sent from an executive within the organization, tricked the employees into providing sign-in credentials for UnityPoint's email system.

Among the data stored on the system were patient names, addresses, dates of birth, medical record numbers, medical information, treatment information, surgical information, diagnoses, lab results, medications, providers, dates of service and/or insurance information, Social Security numbers, driver's license numbers and payment card information.

Data of 500K patients exposed in LifeBridge Health Breach

LifeBridge Health, a nonprofit healthcare corporation based in Baltimore, Maryland, experienced in March a security breach potentially impacting the personal information of over 500,000 patients.[133] LifeBridge Health operates four hospitals in the greater Baltimore area. On March 18, 2018, it detected malware on a server that hosts electronic medical records of Potomac Physicians, one of its physician practices, as well as on a shared registration and billing platform that is used by other LifeBridge Health providers.

After the discovery, LifeBridge promptly launched an investigation into the incident and engaged the services of a forensic firm. The probe revealed that an unauthorized third-party gained access to the organization's network on September 27, 2016.

On May 16, 2018, LifeBridge Health issued a press release about the incident and said it was notifying all potentially affected patients. The organization did not disclose the type of malware found on its systems, nor the nature of the 2016 breach. However, it said the incident compromised certain sensitive information, including patient names, addresses, dates of birth, diagnoses, medications, clinical and treatment information, insurance information, and in some instances, Social Security numbers.

Phishing Attack Compromises Medical Data of 42,600 Aultman Hospital Patients

Attackers used credentials gained from a phishing attack to access several email accounts belonging to the Aultman Health Foundation, including its Ohio-based Aultman Hospital, as well as its occupational medicine division AultWorks, and 25 of its physician practices.[134]

The Aultman Health Foundation notified about 42,600 patients of a data breach potentially affecting their medical information after several employee email accounts were accessed by unauthorized individuals. The unknown attackers gained access to the accounts via a phishing attack that occurred earlier this year.

The breach was first detected on March 28, 2018, after which Aultman launched an investigation to determine how the incident had occurred and what information was impacted. The probe revealed that access to the email accounts occurred on several occasions starting mid-February 2018, and continued until the breach was detected in late March 2018.

133 https://www.prnewswire.com/news-releases/lifebridge-health-and-lifebridge-potomac-professionals-notify-patients-of-a-recent-security-incident-300649922.html
134 https://www.healthdatamanagement.com/news/hackers-access-email-of-aultman-hospital-occupational-medicine-branch?brief=00000157-c311-d2b6-af57-cb9929c60000

Attack Campaigns on Critical Companies and Organizations

Below is a review of several of the most significant events that took place or were exposed this year

Critical Water Utility In US Fell Victim to a Sophisticated Ransomware Attack

On October 15, 2018, it was revealed via a media statement[135] issued by Onslow Water and Sewer Authority (ONWASA)[136], that the FBI investigated a sophisticated malware attack on the critical water utility, located in North Carolina. The attack begun on October 4, when the water utility was targeted with a variant of a polymorphic trojan known as EMOTET[137]. Polymorphic malware is an advanced and modular malware that obfuscates is activity by constantly changing its identifiable features.

The initial attack was believed to have resolved, however due to ongoing and persistent problems ONWASA IT staff contacted an external security experts to assist them. Nevertheless, despite the added security measures and personal, on October 13, ONWASA was hit again, this time by a sophisticated ransomware, dubbed RYUK[138]. The IT and the security team detected the attack at 3 AM and immediately took ONWASA's systems offline, however by that point the malware already successfully infected and encrypted databases and files.

Following the second attack ONWASA received an email with a ransom demand for an unspecified sum. Upon consultation with the FBI, ONWASA decided not to pay the ransom, stating "ONWASA will not negotiate with criminals nor bow to their demands." As a result, ONWASA will need to rebuild several of its databases, but according to the statement their operation will continue manually and no significant disruption is expected in the meanwhile.

Currently no additional information regarding the infection vector has been released. Regarding the identity of the attacker, however RYUK, which shares code with the Hermes malware, was previously linked to the North Korean ATP Lazarus.

Critical Industries Including Nuclear Energy Firms Targeted with NSA Attack Tools

Security researchers from Kaspersky Lab claim to have detected a sophisticated attack campaign[139], allegedly using NSA-developed spy toolkits against multiple critical industries related to telecommunications, nuclear energy, IT, aerospace and R&D. As of writing this report, around 50 victims located in Russia, Iran and Egypt were identified.

135 https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A
136 https://www.onwasa.com/
137 https://www.us-cert.gov/ncas/alerts/TA18-201A
138 https://threatpost.com/ryuk-ransomware-emerges-in-highly-targeted-highly-lucrative-campaign/136755/
139 https://securelist.com/darkpulsar/88199/

The tools that are used in this campaign, DanderSpritz, FuzzBunch[140] and DarkPulsar, originally published in March 2017 by the Russian nation-state group Shadow Brokers; however, since they have been used by various actors against multiple targets around the world.

DanderSpritz and FuzzBunch both provide a framework designed to extend functionality and compatibility with other tools, yet each play a different role in an attack. While FuzzBunch plugins are reconnaissance and attack oriented, DanderSpritz framework was developed for administrating compromised assets.

DanderSpritz - DanderSpritz is a java-based framework with a multitude of spy plugins that gather intelligence, use exploits and examine compromised machines. As seen below it has a graphical windows interface, which according to Kaspersky bears a similarity to botnets administrative panels.

Fuzzbunch - Fuzzbunch is a framework that enables various utilities to interact and work together. Unlike DanderSpritz, which is almost exclusively designed to gather information, Fuzzbunch has various plugins that provide it with a number of capabilities such as analyzing compromised devices, exploiting vulnerabilities, setting schedule tasks, etc.

DarkPulsar - DarkPulsar is a backdoor that bridges Fuzzbunch and DanderSpritz frameworks. In the first stage of the attack, Fuzzbunch is used in conjunction with DarkPulsar to enable the attacker with remote access to the targeted machine. This is followed with DanderSpritz which provides the attacker with monitoring and data exfiltration capabilities.

The detection of in-the-wild use of the above three toolkits show how different tools, malware and frameworks can be chained together to execute a formidable attack with relatively little resources. Further, the discovery of DarkPulsar helps to better understanding how backdoors can play a role in bridging different frameworks in order to create a uniform attack platform designed for long-term persistent compromise.

Ukrainian Intelligence Thwarted Russian VPNFilter Malware Attack

In July the Ukrainian Secret Service (SBU) reported to have a cyber attack via the VPNFilter malware on a chlorine distillation plant.[141] As the plant provides drinking water and sewage treatment across the country, a disruption or shut-down of operation and could have caused considerable damages. No technical details regarding the attack have been reported, however it is currently attributed to Russian APT attackers. [142]

Insights and conclusions

As seen in the above incidents, malicious actors are continuing to develop their skills and tools, becoming increasingly proficient in executing attacks on a wide gamut of industries, including critical infrastructure. As technology matures and evolves we are seeing that it is becoming more and more interconnected; bridging the gaps between industries, geographical locations, and worryingly also those who are affected by cyber-attacks.

Each of the above incidents represents poignant examples of different chain of events that could affect any company, organization and sector. Accordingly, understanding the current progression of attack vectors and trends is vital in mitigating complacency, which in turn can result in grievous errors.

[140] https://medium.com/francisck/the-equation-groups-post-exploitation-tools-danderspritz-and-more-part-1-a1a6372435cd
[141] https://ssu.gov.ua/ua/news/1/category/21/view/5037
142 https://www.bleepingcomputer.com/news/security/ukraine-says-it-stopped-a-vpnfilter-attack-on-a-chlorine-distillation-station/

Attacks on the Aviation Sector

Below is a review of the most significant events that took place or were exposed this year

Throughout 2018 we have seen a wave of attacks against the aviation sector, and in particular large airlines. Many of the attacks are likely unrelated, yet it seems that the sector is slowly becoming more targeted, both directly and as a proxy for other entities via supply chain attacks. It is likely that criminal and/or nation-state actors will continue executing attacks on the industry, be it for profit or against human lives. Below are the most notable incidents.

Attacks on Major Airlines

Air Canada

The first attack took place between August 22-24 against Air Canada. The airline detected “unusual login behavior” with its mobile application. According to the notice the breach compromising personal data of up to 20,000 costumers. The airline has yet to confirm the nature of the breach, notably whether hackers breached Air Canada’s systems, or rather malicious actors accessed users’ accounts by using previously compromised data. Nevertheless, the relatively small number of accounts affected suggests the latter.[143]

British Airways

Just several days later in early September British Airways reported[144] that it experienced a website-related breach affecting close to 400,000 customers, exposing sensitive information including billing and email address, as well as payment card information.[145] In late October BA notified another 185,000 individuals. Of the affected customers, about 77,000 also had their cards' CVV number compromised. The attack affected customers who made payments via BA's main website and mobile app between August 21, 2018, and September 5, 2018.

According to security firm RiskIQ the cybercriminal group Magecart is likely responsible for attack[146]. The group often employ in their attacks malicious skimming code, and was previously attributed to a series of extensive digital credit card skimming campaigns, including the Ticketmaster breach on in July[147]. Although they carried out attacks on multiple targets, Magecart set up custom infrastructure to blend in with the British Airways website. It is not clear how much reach the attackers had on the BA servers, but the fact that they were able to modify a resource for the site indicates that it was substantial.

143 https://www.infosecurity-magazine.com/news/air-canada-presses-reset-app/
144 https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information?dr=&dt=British%20Airways&tier=&scheme=&logintype=public&audience=travel&CUSTSEG=&GGLMember=&ban=||P1M||||||HOME|||L4|||anonymous-inspiration|||&KMtag=c&KMver=1.0&clickpage=HOME
145 https://www.infosecurity-magazine.com/news/ba-breach-an-extra-185k-customers/
146 https://www.riskiq.com/blog/labs/magecart-british-airways-breach/
147 https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/

This is the second incident British Airways has been involved with in the last six months. As a reminder, in July the airline had to delay and cancel flights at Heathrow airport after it experienced an un-specified "IT system issue"[148]. As of writing this report it is unclear whether the two events are related.

Cathay Pacific

The third attack was reported on October 24, Cathay Pacific Airlines revealed[149] that it was the latest in major airlines to fall victim to a data breach. This time however the magnitude of the attack, which was executed in March, is reportedly the largest airline data breach, compromising personal information of 9.4 million passengers. But, unlike BA, only a handful of credit card numbers were accessed. Instead, most of the compromised records were personally identifiable information (PPI).

According to the statement the following data was accessed: "passenger name; nationality; date of birth; phone number; email; address; passport number; identity card number; frequent flyer program membership number; customer service remarks and historical travel information. In addition, 403 expired credit card numbers were accessed. 27 credit card numbers with no CVV were accessed." The airline added that "no-one’s travel or loyalty profile was accessed in full, and no passwords were compromised." Like BA, Cathey Pacific is also claiming that the information has not been used, further stating that there was no impact on flight safety as the IT affected systems are fully separate from their flight operations systems.

Additional notable events Affecting the Aviation Sector

The above events do not appear to be related, however the recent increase of attacks against major entities within the aviation sector is concerning. Other than the above-mentioned attacks, below are several additional events from the last six months that affects the sector.

Bristol Airport Falls Victim to Ransomware Attack, Disabling Flight Information Screens - in the middle of September there was an attempted ransomware attack on Bristol airport's administrative systems. To contain the attack, the airport shut down several of its facilities for a few days, including their flight information screens.[150] Airport officials decided to decline paying the ransom demand, choosing instead to manually restore all affected systems.

Ransomware Attack on Bristol Airport Disabled the Flight Notification System - in September, Bristol airport in the UK was hit by a ransomware that infected several administrative systems. [151] In order to mitigate the infection, the airport disconnected several facilities for several days, including its flight notification screens. Further, the airport decided to not pay the ransom, and instead restore its systems from backups.

Drones Disable London's Gatwick Airport for a Day and a Half - between December 19-20, unknown individuals disrupted the airport's flight operation by flying drones over the runways. It seems that this incident was intentional and well planned as it requires considerable amount of batteries for such a long operation.[152]

Travel Management Firm Breached, Compromising Records of 30K Pentagon Employees - on October 12, the Pentagon issued a statement in which it revealed that it fell victim to a cyber attack compromising sensitive travel records of U.S. military and civilian personnel[153]. According to the statement an unnamed contractor providing travel management services to the Department of Defense was hacked. The breach potentially compromised personal information and credit card data of up to 30,000 individuals. The breach was discovered on October 4th, yet not much is known about the attacker. According to the Pentagon, the breach affected a

148 https://www.welivesecurity.com/2018/07/19/british-airways-cancelled-flights-heathrow-system-issue/
149 https://infosecurity.cathaypacific.com/en_HK.html
150 https://www.zdnet.com/article/ransomware-attack-blacks-out-screens-at-bristol-airport/
151 https://www.zdnet.com/article/ransomware-attack-blacks-out-screens-at-bristol-airport/
152 https://www.theverge.com/2018/12/20/18149819/london-gatwick-airport-drone-shutdown-reports
153 https://www.bleepingcomputer.com/news/security/pentagon-data-breach-exposes-up-to-30-000-travel-records/

single vendor that provided services to a small portion of the total population. The event is currently being investigated and no additional information was provided.

Flightradar24 - in June, the real-time flight-tracking website was hacked affecting an unspecified number of users[154].

Domodedovo Airport - in July, Moscow International airport received threatening e-mails from unknown actors claiming that they will disrupt the Airport's navigation equipment unless they are payed a ransom in Bitcoin[155].

Aviation ID Australia - in July, the Australian airport identity card issuer's website was accessed by an unauthorized entity compromising personal information of applicants and cardholders[156].

Un-named major international airport - In July, it was revealed[157] that remote desktop protocol (RDP) access to the security and building automation systems of an un-named major international airport was sold on a Russian market for as litter as US$10.

Ransomware Attacks on Municipalities

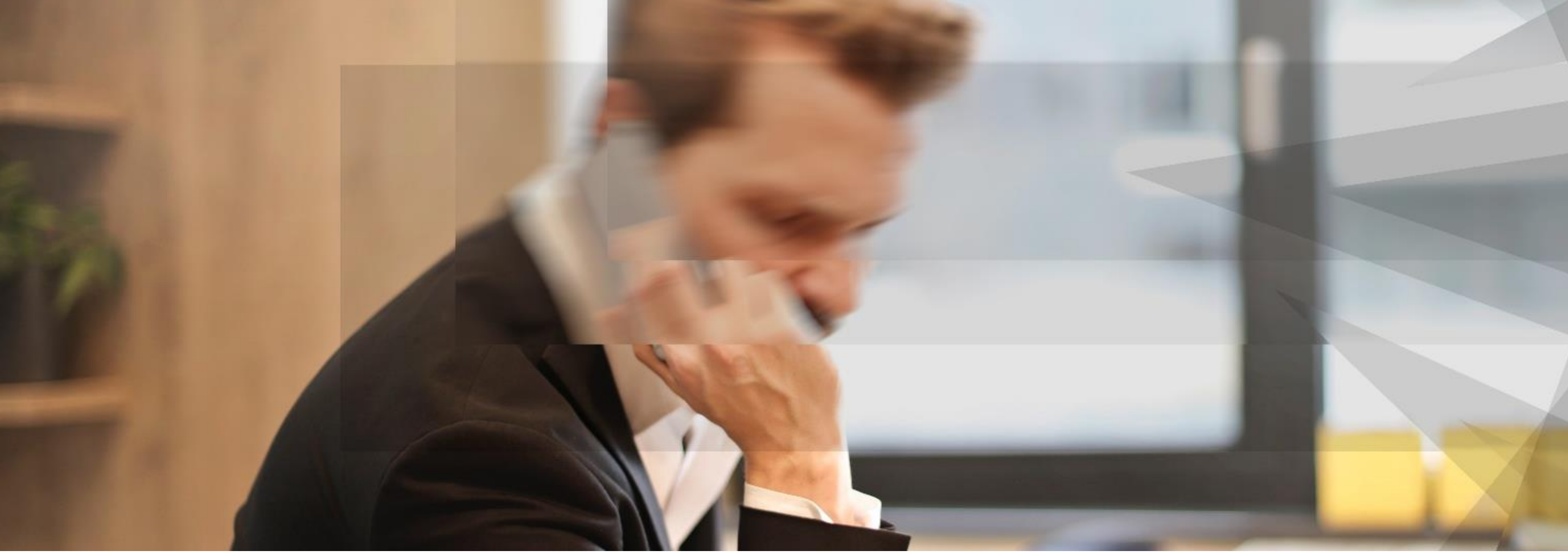
Below is a review of several of the most significant events that took place or were exposed this year

In 2018, we have seen numerous ransomware attacks on municipalities around the world. However, the most notable incidents were the attacks on Atlanta and Baltimore in March that disrupted vital services, and the attack on the port of San Diego in late September.

The city of Atlanta was hit by SamSam ransomware which exploits a deserialization vulnerability in Java-based servers[158]. The attackers compromised a vulnerable server first, and ransomware spread to desktop computers throughout the whole network of Atlanta. Many of the city's online services were crippled for six days, with some workers resorting to using pen and paper. Three months after the attack, a third of the city’s 424 software programs were still offline or partially inoperable.[159] The ransom was set at US$55,000 dollars' worth of bitcoin, but was never paid. Following recovery efforts have since been estimated at US$17 million. In contrast, prior to the attack, the Atlanta government was criticized for a lack of spending on upgrading its IT infrastructure. SamSam differs from other Ransomware in that it does not rely on phishing, but rather utilizes a brute-force attack to guess weak passwords until one breaks open. It is known to target weaker IT infrastructures and servers.[160]

This ransomware has prominently been behind attacks on the healthcare sector, as well as governmental organizations since its discovery in 2016, with previous attacks on targets ranging from small towns such as Farmington, New Mexico to the Colorado Department of Transportation and the Erie County Medical Center. In November 2018, the US federal prosecutors indicted two Iranian nationals for creating and deploying the malware.[161] The attack raises the question if paying ransom is the right choice. The official US government guidelines are against paying ransoms, as to not encourage attackers to execute them. Hackers often demand relatively small amounts of money, to make the option of paying the ransom more favorable. This makes the choice of whether to pay ransom or not even more difficult, as the cost in paying the ransom is much lower than combatting it.

154 https://thehackernews.com/2018/06/flightradar24-data-breach.html
155 http://www.ehackingnews.com/2018/07/hackers-threaten-to-disrupt-moscow.html
156 https://www.bankinfosecurity.com/australian-airport-id-card-issuer-breached-a-11205
157 https://www.darkreading.com/threat-intelligence/major-international-airport-system-access-sold-for-$10-on-dark-web/d/d-id/1332270
158 https://www.zdnet.com/article/atlanta-spent-at-least-two-million-on-ransomware-attack-recovery/
159 https://www.infosecurity-magazine.com/news-features/top-ten-atlantas-ransomware/
160 https://statescoop.com/atlanta-was-not-prepared-to-respond-to-a-ransomware-attack/
161 https://techcrunch.com/2018/11/28/justice-department-indicts-two-iranians-over-samsam-ransomware-attacks/



BEC Scams - Financial Losses of $12.5B Over Last 5 Years; Review of Recent Trends

BEC (Business Email Compromise) scams is one of the most profitable and common type of cyber attacks in recent years. BECs (aka "Man-in-the-Email" or CEO scams) are carried out using a variety of social engineering methods and tools.

According to the latest data from the FBI's Internet Crime Complaint Center (IC3)[162], over 78,000 incidents were reported, adding up to a total sum of over $12.5 Billion dollars stolen between October 2013 and May 2018. Moreover, this trend only appears to be growing, with global losses have going up by 136% since December 2016. BEC however, is only one aspect of a larger problem plaguing the global financial sector.

For example, a recent report[163] by the IMF (International Monitory Fund), has assessed the average annual potential losses from cyber-attacks as close to 9 percent of banks' net income globally, or approximately $100 billion, with severe scenarios potentially going as high as $350 billion.

Nigerian cybercriminal operation

When reviewing the global online scam operation, it appears that Nigerian actors play a prominent role. Further, according to data from PaloAlto, the number of BEC incidents are scientifically higher than the IC3 report suggest. PaloAlto have found that in 2017 alone, about 17,600 Nigerian BEC attacks were executed per month; a 45 percent increase compared to the year prior.

In Total, over a period of three years PlaoAlto have attributed more than 300 actors or groups to nearly half a million attacks. Moreover, their method of operation has significantly evolved and become complex over the last couple of years, namely adopting the use malware and RATs, (Remote Administration Tools).

One of the striking aspects of Nigerian BEC actors is that unlike other cybercriminals around the world, make little to no effort to obfuscate their real-world identity. Many even create attack infrastructures associated with public social media accounts such as Google, Facebook, MySpace, Instagram, and various dating and blogging sites. The age range of Nigerian BEC actors appear to mostly be between 20s and 40s, with the vast majority in their 30's. Many are married with children, with alleged higher education, and seemingly hold or have held legitimate jobs in various fields.

[162] https://www.ic3.gov/media/2018/180712.aspx
[163] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/

BEC actors targeting companies with global operations

The most prominent sector targeted by BEC/EAC actors in recent year has been real-estate, with an increase of 1100% in reported incidents, and almost 2200% in report losses between 2015 and 2017. However, attackers are also increasingly targeting companies with global operations, exploiting the nature of time differences to their advantage. Below is an example of a notable campaign against the maritime shipping industry; note however that the methods described below could easily be used against the banking sector.

In April, it was report that between June 2017 and January 2018, a hacking group dubbed "Gold Galleon" stole at least $3.9 million from maritime shipping organizations via sophisticated BEC attacks. The group targets a wide range of companies, including companies that provide ship management services, port services and cash to master services.

Due to their global and complex operations, the shipping industry, not unlike the financial sector, often coordinates their activity across multiple time-zones. Subsequently, financial organizations are highly reliant on email for communication between numerous actors such as, various departments and offices, third-party service provides, governmental offices, customers, etc. This in turn makes them vulnerable to BEC scams, as it may be difficult to verify if someone is being impersonated.

Gold Galleon is likely based in Nigeria, and is comprised by at least 20 members who work together to executes various parts of BEC campaigns, from the initial compromise to gathering and extracting data. The group employs various spear phishing techniques to compromise their targets; notably emails with malicious attachments such as a remote access tool with keylogging and password stealing functionalities. Stolen email account credentials are then leveraged for additional phishing attempts.

Recommendations for protection

BEC/EAC scams are considered "low-tech", however as they can involve sophisticated social engineering tactics across multiple channels of communication, including emails, SMS messages and even phone calls. Accordingly it is advised to verify all requests for a change in payment type and/or location, and any unusual request for information, via a secondary means of communication. It is also advised to establish code phrases unique to each client/department/vendor, etc. that would only be known to the two legitimate parties.

Moreover, it is recommended to examine the option of creating dedicated email accounts, with two-factor-authentication enabled, for the sole purpose of communicating or verifying such requests; whether internally, or between employees and clients/third-party suppliers.

As is often in cases of financial scams, basic info-sec awareness and quick response are vital to mitigate such attacks. Accordingly, it is recommended to routinely inform employees about new social engineering techniques and significant phishing campaigns.

Additional Events of Note

Olympic Destroyer – Destructive Malware Attack on the 2018 Winter Olympics

The Pyeongchang Winter Olympics began February 9th, in South Korea and will be held until February 25th. Prior to the opening ceremony, there have been numerous concerns regarding potential cyber-attacks amid tensions between South Korea and its neighbor to the north. In addition, there were concerns regarding a possible retaliatory attack by Russian entities after the Russian delegation has been suspended due to doping allegations.

At the eve of the opening ceremony, a series of destructive cyber-attacks led to disruptions in the computer infrastructure of the Pyeongchang games that compromised and temporarily paralyzed various systems (several of those were not reported), such as the stadiums' WiFi networks and broadcasting stations. Furthermore, shortly before the ceremony began, the official Winter Olympics website went down for several hours, disrupting ticket sales, downloads and online visitor services.

On Sunday February 11th, Olympic officials announced that these malfunctions were a result of a cyber attack; however, no further information concerning the attack vector or identity of the attacker was revealed. Nevertheless, Cisco Systems' Talos research team identified malware it called the Olympic Destroyer, which was likely used in the attack. Several characteristics of the malware were previously seen in the NotPetya and Bad Rabbit attacks, which were conducted by Russians.

Attack vector and malware workflow

According to Talos, the identified malware appears to operate in a solely destructive manner and does not communicate with a C2 server. The attack and infection vectors were most likely carried out by using the supply chain – penetrating Atos, the key IT vendor of the Olympics that was previously attacked several months ago[164].

Below is the Olympic Destroyer workflow:

- After initial infection, two malwares are dropped onto the victim host, that steal usernames and password credentials from the victim's infected browsers and computer systems. Talos researchers have identified 44 account credentials within the binary code of Olympic Destroyer.
- The malware uses a legitimate Microsoft tool called PsExec, as well as the Windows Management Instrumentation (WMI) interface, in order to perform lateral movement within the network. The malware does this while using stolen credentials and infecting other systems with Olympic Destroyer.
- The malware deletes shadow copy files and backup system logs in order to prevent future information recovery.

164 https://www.cyberscoop.com/atos-olympics-hack-olympic-destroyer-malware-peyongchang/

- The attacker covers its tracks by deleting System & Security windows event log, including the recovery console of the infected host.
- The malware maps shared network folders and deletes every file it can access and finally shuts down the compromised system, leaving the victim unable boot it.

The attacker

As of writing this report, the identity of the attacker remains unknown. However, as previously mentioned, Russia is suspected to be behind the operation after it was suspended by the Olympic Committee following athlete doping allegations. Russian entities have previously carried various retributory attacks. For example, in September 2016, the Russian cyber espionage group APT28 (also known as Fancy Bear) attacked the World Anti-Doping Agency (WADA) and leaked sensitive information it collected about Olympic athletes. In late 2017, the Crowdstrike cyber security company detected espionage activity targeting various international sporting organizations[165]. These operations were attributed, with moderate certainty, to APT28.

In addition, there are numerous similarities between the Olympic Destroyer and previous Russian attacks. However, these indications are not conclusive. Accordingly, Talos and the Olympic Committee have refrained from attributing the attack to any specific entity.

New Olympic Destroyer Attacks on Biochem Labs and Financial Institutions

Kaspersky researchers who continued to monitor the threat actors behind the Olympics attack have identified in May and June a new spear-phishing campaign that utilizes malicious documents containing malware that shares numerous similarities with the Olympic Destroyer malware. According to Kaspersky's report, the threat actor involved in the Olympics attack is now focusing on financial organizations in Russia, as well biological and chemical threat prevention laboratories in the Netherlands, Germany, France, Switzerland, and Ukraine.[166]

Note that although Kaspersky does not yet know the identity of the victims; however, a forensic analysis of the campaign's samples, infection vector, and attack infrastructure enabled the security firm to create a general profile for these victims, which includes such details as location and sector.

Meltdown & Spectre – Critical Vulnerabilities Affecting Major Manufacturers' Microchips

In early January, it was reported that AMD, Intel and Arm are exposed to potential cyber-attacks due to an underlying CPU architecture design vulnerability, dubbed – Meltdown and Spectre. The ramification of this discovery was wide-reaching as they affected almost every computer chip manufactured over the last 20 years; and potentially impacting billions of computers systems globally, be them private, industrial, commercial or governmental. Since the vulnerabilities were detected the manufactures released security patches, however up until recently, security researchers have discovered new exploitation vectors.[167]

As of late December 2018, there have been no reports of in-the-wild attacks that exploited Meltdown or Spectre. Nevertheless, due to the severity and the scale of the problem, it is likely that malicious actors have developed an attack vector or malware

What are the actions that you can take to mitigate this situation - As this is a hardware vulnerability the solution is highly complicated. It requires a massive organization-wide computer system update. We recommend to first

165 https://www.scmagazineuk.com/russian-actors-mentioned-as-possibly-launching-olympics-cyber-attack/article/743932/
166 https://www.kaspersky.com/blog/olympic-destroyer-biochem/22792/
167 https://www.zdnet.com/article/researchers-discover-seven-new-meltdown-and-spectre-attacks/

update the work stations that have internet access (surfing, emails, etc.), followed by network servers that offer online services, and then the remaining computer systems.

Note that the order of the update is of importance. Microsoft OS update will not run unless the AV software is up to date. This is due to the reason that some AV software turn to the Kernal. Consequently, if the Microsoft update is executed prior to the AV update, it is possible the computer will enter an endless loop and will crash. To prevent this, before running the Microsoft update, check a Registry Value to see if was properly updated by the AV. If not, then the update will not run. The full explanation is available on the Microsoft support page (link in footnotes).[168] Below are the necessary update and their required order:

1. Updating end-stations' AV software.
2. Running OS update.
3. Updating the firmware.
4. Updating database systems and vulnerable applications.
5. Updating peripheral security components.

Notes

- This is a significant update that could disrupt/slow down users/work-stations' work.
- The firmware update is issued by the manufactures and not by Intel.
- Updating just one component in the system, such as the AV, without updating the OS or firmware will leave the system vulnerable.
- The update could possibly hurt the work speed of virtual work-stations (e.g. VMware and Hyber-v), as well as the computers themselves.

As of late December 2018, there have been no reports of in-the-wild attack exploiting Meltdown or Spectre. With the in mind, it should be noted that these vulnerabilities still pose a risk. Due to the severity and large scale of the issue, it is likely that malicious cyber actors have developed an attack vector/malware that leverages Meltdown and Spectre, and have refrained from using it for various reasons. Alternatively it is possible this has not yet happed and an exploit is in the developing process and will be used at a later time. Accordingly, it is advised to insure all of your systems are up to date with the latest security patches. In not, please do so promptly. If you will for consultation regarding hardening your systems, we will be happy to assist.

VPNFilter - Destructive Malware Compromises 500K Network Devices Worldwide

On May 23, 2018, Talos (Cisco's threat intelligence team) published initial research findings exposing a sophisticated modular malware dubbed VPNFilter. It should be noted that this malware's code overlaps with versions of the BlackEnergy, which was used in a series of large-scale attacks against Ukraine. Accordingly, VPNFilter may also be destructive.

Talos estimates that at this point, the malware has infected at least 500,000 routers and networking equipment in at least 54 countries. Affected devices are from manufactures Linksys, MikroTik, NETGEAR and TP-Link. Additionally, VPNFilter compromised NAS (Network-attached storage) devices from QNAP.[169]

The malware is likely being used for gaining control of communication infrastructures, gathering intelligence, and establishing an attack infrastructure for widescale destructive or disruptive attacks. As of writing this alert, the identity of the attacker is unknown, however initial attribution is to a Russian threat actor.

168 https://support.microsoft.com/en-us/help/4072699/january-3-2018-windows-security-updates-and-antivirus-software
169 https://www.qnap.com/en/

Attack Vector

Stage 1 - VPNFilter compromises devices that are based on open-source systems such as Linux and Busybox. During this stage, the malware obtains persistency to ensure the completion of the infection process. The main goal of this stage is to locate the IP address of the current stage 2 deployment server. It does so by downloading an image from a free photo sharing service (Photobucket.com), and extracting the IP address from GPS values in the image EXIF information.

The malware also has a backup domain in case for any reason it cannot access or acquire the IP address from the Photobucket image. Having this failed, VPNFilter has an additional contingency to obtain the address. Consequently, VPNFilter is extremely adaptable and capable of dealing with unpredictable C2 infrastructure changes.

Stage 2 - Once the first stage is completed, the malware turns to the C2 server for additional commands such as - file gathering, remote execution of shell command or plugin, data exfiltration, reboot the device.

Note that some of the samples analyses by Talos had a wiper function that reboots the device after overwriting critical firmware data; effectively bricking it.

Stage 3 - During this stage, the malware downloads plugin modules that provide it with additional capabilities. While Talos have so far identified and analyzed only two, they believe there several others that they have not yet detected. The exposed plugin modules are:

Packet sniffer – listens to outgoing traffic from the compromised device. This allows the attack to steal website credentials and monitor Modbus SCADA protocols.

Communications module - allows the malware to communicate over Tor.

FBI PSA - Mitigating Malware Operation

On May 25, 2018, amid the spread of the malware, the FBI issued a Public Service Announcement with recommendations aimed to facilitate VPNFilter mitigation.[170] The PSA urges any owner of small office and home office routers reboot the devices to temporarily disrupt the malware and aid the potential identification of infected devices. Owners are also advised to consider disabling remote management settings on devices and secure with strong passwords and encryption when enabled. Network devices should be upgraded to the latest available versions of firmware.

Insights

Info-sec and IT teams across numerous companies and service providers failed to detect the malware over a long period of time. This is despite the fact that the malicious variant was installed in April and appears to have been used to execute attacks. [171] Yet, the malware was only detected only once the attackers considerably expanded its activity and disrupted companies' operations. This event illustrates how many users are not aware or ignore the importance of routinely and promptly updating routers and other IT components.

There were no indicators that could be used to identify and block the malware's communication traffic. In similar fashion to WannaCry, and APT's modus operandi against supply chains, it currently impossible to detect, monitor and block the malware's traffic via malicious IP and domain addresses. This is due to that C2 control is conducted

[170] https://www.ic3.gov/media/2018/180525.aspx
[171] https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/

via legitimate communication channels to the service providers; or with no C2 server commands, as was the case with WannaCry.

Factory resetting the routers can cause additional problems. As the malware has persistency capabilities, a simple reset is an insufficient measure. Nevertheless, in certain cases (depending on the nature of the infection and model of the device), the malware can be removed by doing a factory reset. However, doing so may also remove updates, which in turn could expose the device to old vulnerabilities.

Personal Information of 500 Million Marriott Clients Compromised

In early December, the hotel chain Marriott announced that information of its guests was exposed and copied. **The firm also announced that 327 million people's credit card information was stolen**. The scale of attack is unprecedented, and it appears that the credit card companies have not yet decided how to deal with such a theft.

On September 8th, an internal security tool alerted that there was an attempt to access the Starwood booking system in the US. Due to this alert, the hotel management began an investigation on November 19th and concluded that the system was hacked from 2014. Information of guests that stayed in the hotel (including the following hotels - W, Sheraton, Le Mereidien, and Four Points by Sheraton) from 2014 until September 10th were exposed to attacks. There was data of 500 million clients in this system.

Marriott stated that for 337 million guests, some of the following information was stolen: name, address, telephone number, email address, passport number, bank account information, birth-date, gender, arrival and departure from the hotel. **Even though the hotel systems had credit card encryption, there is still a possibility that deciphering keys were also stolen during the attack.**

Researchers that investigated the attack claim that the attack vector provides some hints about their identity[172]. It is likely attackers from the intelligence unit of the Chinese government. They found that there were similar tools and attack methods used with previous Chinese attacks. They asses that the purpose of the attack is not financial, but for gathering intelligence. The Chinese government denies any connection to the attack. FBI officials confirmed that there are similar patterns from previous Chinese attacks. Note that most of these attack tools have previously been exposed, and thus can be used to impersonate a Chinese actor.

Marriot's response

Marriott created a website and hotline for assisting victims of the attack, containing information about attack, and a free one year subscription to WebWatcher, a fraud detection service[173]. Marriott recommends their guests to check suspicious transactions in their accounts, and check to verify whether emails they receive from Marriott are indeed legitimate; chiefly if they ask for identification or contain attached files.

Regulators' response

This is one of the largest attacks witnessed. According to the BBC[174], the British regulator confirmed that the attack is under investigation. The firm has hotels and costumers in Europe **and Israel**, and therefore the GDRP might fine them. Despite the response they gave to their customers, international regulators can still decide that Marriott's response in this case was inadequate.

[172] https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive-idUSKBN1O504D
[173] https://answers.kroll.com/
174 https://www.bbc.com/news/technology-46401890

Facebook Data Breach Affecting 30 Million Users

In late September, it was reported that the social media giant Facebook fell victim to a massive breach in which data pertaining to millions of users. Initially it was reported that 50 million users were affected, however this was later corrected to 30 million[175]. About half of those only had their full name compromised; but for the other 15 million the breach compromised included date of birth, education details, religion orientation, last searches, etc. This type and scale of breach is highly concerning as the attackers can easily leverage the data to execute spear-phishing attack and event identity thefts on a wide-scale. [176]

The attackers exploited a vulnerability with the "view as" functions; present since July 2017. This function enabled users to view their privacy settings from other users' accounts. This however was exploited by malicious actors to obtain large amount of data on numerous Facebook users, as well as leveraging it to compromise additional accounts. Facebook began noticing a spike in "view as" use, and on September 25, it first detected the vulnerability, which was fixed two days later.

This is the largest and most egregious breach Facebook has ever experienced, as the attackers stole "access tokens". These are a type of security key that enables user to login to their account without needing to retype their password. Having this token enables malicious actors to obtain control of users' accounts, including logins to third-party apps that also require Facebook login. [177]

Throughout 2018, Facebook faced harsh public critique with regards to users' data security. For example, in March the political consultation and analysis company Cambridge Analytica that inappropriately obtained access to data pertaining 87 million Facebook users.[178] These events, amongst others, reflect how various actors can relatively easily gain access to massive databases via social media platforms.

US ISP Suffers a Massive Data-Leak of Sensitive Information Due to Misconfigured Amazon Cloud Database

Over the last couple of years we have seen increasing amount of reports of data leaks due to misconfigurations of Amazon cloud-based databases. These databases, known as AWS S3 bucket[179], are often used by companies and organizations, including aviation companies, to store a wide range of data. Accordingly, a seemingly small misconfiguring error could result in a detrimental data leak. Below is a recent incident, poignantly illustrating the risks of such an event, as well as the need to address every aspect of the organization's infrastructure and operation when designing and creating its info-security framework.

On October 23, security firm UpGuard reported that it detected a massive database of 73 gigabytes belonging to Washington-based internet service provider Pocket iNet was publicly exposed. As a result, highly sensitive data including lists of plain text passwords and credentials of Pocket iNet employees, internal network diagramming, configuration details, inventory lists, and photographs of the ISP's equipment.

The database, named "pinapp2", was detected on October 11. UpGuard contacted and notified Pocket iNet on the matter the same day, however it took the ISP a full week to confirm and secure the exposure. In the interim, due to the severity of this exposure, UpGuard expended significant effort following-up on the matter, repeatedly contacting Pocket iNet and relevant regulators.

175 https://www.wired.com/story/how-facebook-hackers-compromised-30-million-accounts/
176 https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach
177 https://www.infosecurity-magazine.com/news/facebook-breach-hit-30-million/
178 https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/
179 Amazon Web Services' (AWS) Simple Storage Service (S3)

If malicious would have obtained the databases, they could have executed a large number of targeted-attacks, taking control of its infrastructure and systems, crippling the ISP's services or establishing a persistent foothold spying on the company and its clients for later attacks. Furthermore, the exposed data also included a list of “priority customers,” with their location and contact details. Amongst the clients are major companies such as Lockheed Martin and Toyota. This information could have easily been leveraged to execute various social engineering on the clients, including BEC attacks.

Insights, Recommendations and Additional Misconfiguration Incidents Compromising Sensitive Data

This incident is extremely concerning on several levels. Notably it shows how a "minor" human error (i.e. misconfiguring a database) could result in an egregious flaw within organization's overarching security framework. The latter may be well designed and robust, but without proper organizational info-sec procedures, one such error could negate many security solutions. This type of data exposure can easily be leveraged to execute spear-targeted attacks on the ISP's clients, and possibly even debilitating attacks against the ISP itself. For example, having Pocket iNet's device configuration schematics, malicious actors could easily bypass many of its security measures.

Lastly, despite the risks, this type of negligence is regretfully common. This incident is especially notable not only because the scale and type of exposed data, but also the unaccepted amount of time it took the ISP to resolve the problem despite getting ample information from UpGuard.

Due to the prevalence of data leaks due to misconfigurations of AWS S3 buckets, it is advised to follow Amazon's official guidelines[180] when creating one. Moreover, it is recommended to conduct a comprehensive review of existing S3 buckets to determine they are configured correctly and no information is publicly exposed.

Misconfigured S3 Bucket Exposes Personal and Medical Data - A misconfigured Amazon S3 bucket maintained by a Chicago-based insurance startup AgentRun, has exposed a large amount of client data, including sensitive medical information and personal identification documents.[181], a Compromised information included client data, among then information belonging to such companies as Cigna, Transamerica, SafeCo Insurance, Schneider Insurance, Manhattan Life, and Everest, as well as the medical information of thousands of insurance policyholders. In addition, the breached bucket contained scans of customer identification documents such as Social Security cards and numbers, Medicare cards, driver’s licenses, armed forces and voter identification cards.

According to Andrew Lech, the company's founder, the permissions on the bucket were erroneously flipped during an application upgrade and during migration, leaving the bucket unprotected and accessible to anyone. The bucket was secured one hour after disclosure of the breach. The company said it is notifying all potentially impacted individuals and has contacted the relevant authorities.

Misconfigured FTP Server Compromises Data of 205,000 Patients - A misconfiguration of a public FTP server maintained by the Arkansas-based MedEvolve, a practice management software provider, exposed the protected information of 205,000 patients from two separate healthcare providers. While a number of clients had files on the FTP server, two had stored the medical files without password-protection.[182] One of the clients, Premier Urgent Care in Pennsylvania, had a SQL database with 205,000 patient records that was not secured. Around 11,000 of those records contained Social Security numbers. The second client was Texas-based dermatologist Dr. Beverly Held, who with three .dat files compromised an estimated 12,000 Social Security numbers that were stored in the files. On May 3, 2018 DataBreaches.net notified the two medical practices and MedEvolve, the files were consequently removed that same day.

[180] https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html
[181] https://www.zdnet.com/article/insurance-startup-leaks-sensitive-customer-health-data/
182 https://www.databreaches.net/more-than-200000-patients-records-were-exposed-on-medevolves-public-ftp-server-researcher/

Massive MyHeritage Breach Compromises Account Details of 92 Million Users

On June 4, 2018, the Israeli genealogy and DNA testing company MyHeritage announced that it had experienced a data breach that compromised the account details of 92,283,889 users who had signed up to its website up to and including Oct 26, 2017.[183]

MyHeritage was alerted to the breach when an unidentified security researcher found a file named myheritage on a private server not related to the company. The file contained the email addresses and hashed passwords of 92,283,889 users. After receiving the file from the researcher on June 4, 2018, the company's IT security team launched an investigation to determine what had occurred.

According to the company's statement, the security researcher reported that no other data related to MyHeritage was found on the private server. Furthermore, MyHeritage found no evidence that the data in the file was ever used by the attackers. Since Oct 26, 2017, the company did not detect any activity indicating that additional MyHeritage accounts had been compromised.

No payment details were comprised in this incident, as MyHeritage does not store this information on its servers. Other types of sensitive data such as family trees and DNA data is stored by MyHeritage on systems that are separate from those that store user email addresses. MyHeritage said it has no reason to believe any other MyHeritage system was compromised.

Largest Darknet Hosting Service Hacked, Shutting Down Thousands of Websites

On November 15th, Daniel's Hosting, the largest hosting service in the world was hacked, and all the websites stored on it (over 6500) were erased. The attackers exploited a zero-day vulnerability that was published one day before the attack. Below is the summary of the event:

About the service

The service was established in 2013 as a non-profit personal project by a German developer called Daniel Winzen. He posted the code to many services on GitHub, which might have assisted the attackers to find out that the website was vulnerable. Moreover, Winzen revealed the operation process of the website. The storage system offered various services:

- Website storage – Before the hack, over 6500 websites were stored. They did not go through content filtering and therefore included many malicious websites or websites with forbidden content. On February 2017, a group identified as Anonymous hacked into the Freedom Hosting II service which stored 10,613 websites on the darknet. After that service was hit, Daniel became the most popular service on the darknet. Most of the websites stored on Daniel were in English (over 4900), and few in Russian (54).
- Anonymous chat – one of the most popular services on the website, managed by four anonymous administrators, under Daniel himself. One can sign up to the chat without identification, but Daniel placed some rules – no pornography, violence incitement, and offensive speech. During the attack the chat service was also hit, but was restored immediately. During the investigation we discovered that after the chat was restored, one of the admins, identified as Marauder, took control over the chat and is now the main admin.
- Search Engine – The website offered an advanced search service on over ten thousand websites on the dark net. The search enabled retrieving the contents of the website, filtering by category and more. Moreover, the service provided a statement about the condition of the website – whether it is active or not. It was one of the

[183] https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident#/

main two services available to the public and reviewed the central status of many websites in the darknet in a relatively reliably way.

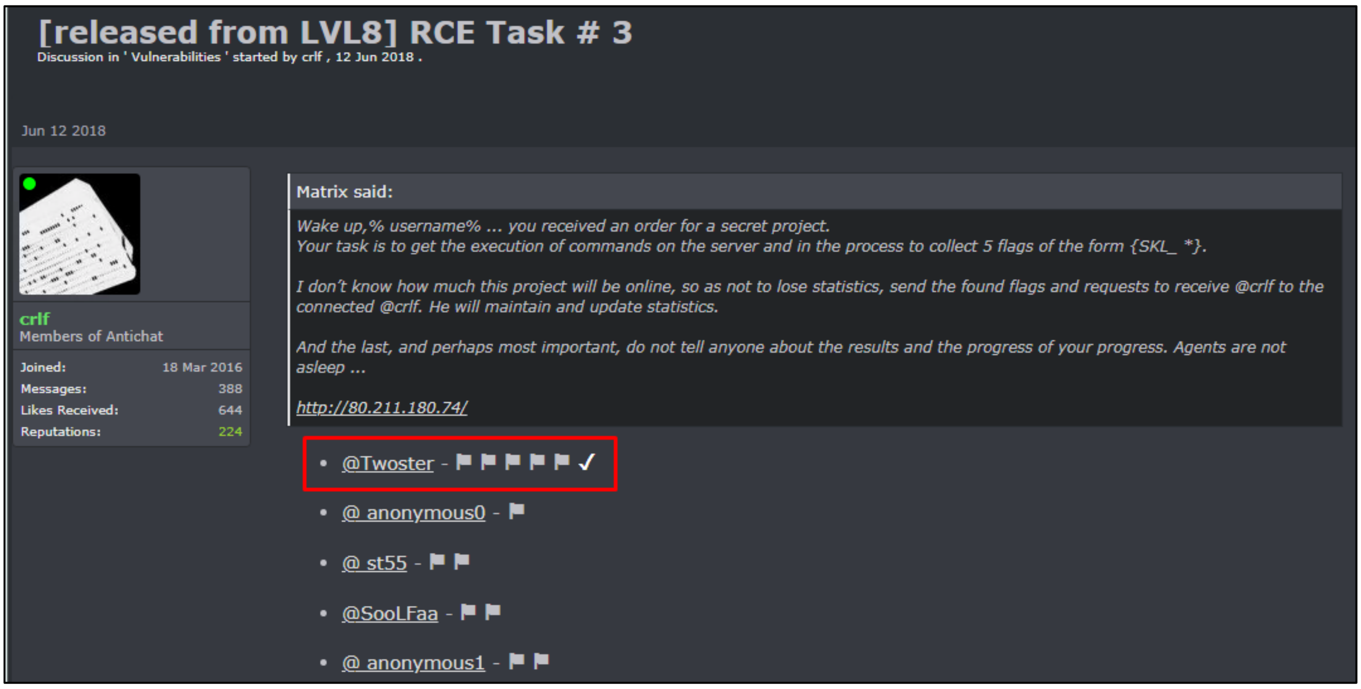
- Email services, address abbreviations and darknet user manuals were not hit during the attack because they were stored separately.

Penetration vector

On November 15th, unknown attackers exploited vulnerabilities on Winzen's storage system and completely erased all the websites stored on the service. A zero-day vulnerability was used during the attack. It was posted one day before, on November 14th on GitHub and Reddit[184]. The vulnerability is executed by parameter injection method with imap_open function (part of imap-2007f library).

This function is not the php kernel function, but an adaptation to this function from imap-2007f library). By exploiting this vulnerability, one can open an RSH connection to an email inbox. The vulnerability enables bypassing exec functions on php pages by using imap_open. We detected a manual for using the vulnerability posted in a hacking forum in Russian.

The discussion on the forum started on June 12th when of the users challenged the other forum members to find RCE vulnerabilities on php servers. The flags symbolize the measure of success of the challenge – each flag represents one discovery. The goal of the challenge is to get 5 flags.



[released from LVL8] RCE Task # 3

Discussion in ' Vulnerabilities ' started by crlf , 12 Jun 2018 .

Jun 12 2018

crlf
Members of Antichat
Joined: 18 Mar 2016
Messages: 388
Likes Received: 644
Reputations: 224

Matrix said:

Wake up,% username% ... you received an order for a secret project.
*Your task is to get the execution of commands on the server and in the process to collect 5 flags of the form {SKL_ *}.*

I don't know how much this project will be online, so as not to lose statistics, send the found flags and requests to receive @crlf to the connected @crlf. He will maintain and update statistics.

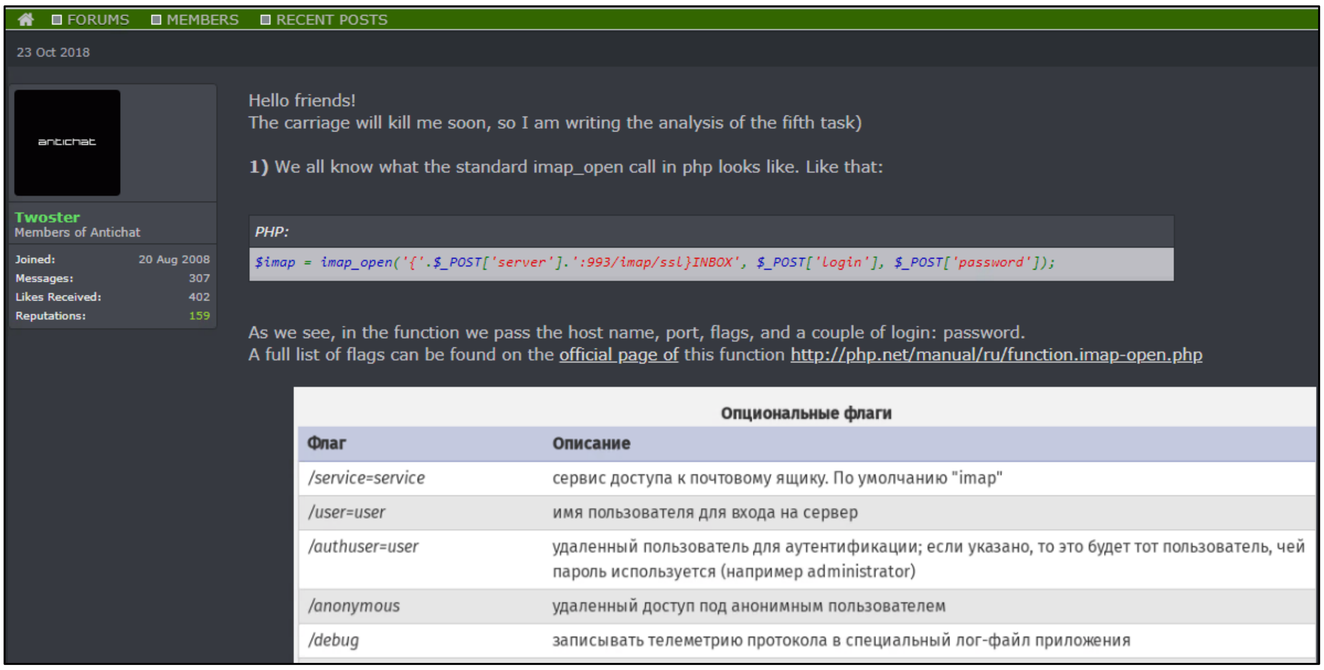
And the last, and perhaps most important, do not tell anyone about the results and the progress of your progress. Agents are not asleep ...

http://80.211.180.74/

- @Twoster - ⚑ ⚑ ⚑ ⚑ ⚑ ✓
- @ anonymous0 - ⚑
- @ st55 - ⚑ ⚑
- @SoolFaa - ⚑ ⚑
- @ anonymous1 - ⚑ ⚑

The response to the fifth challenge is a vulnerability with which the attackers hacked into the storage service. Alexander Twoster, one of the two users who completed the whole challenge, posted the full guide for using the vulnerability which includes nine parts. In the first part, he explains how the imap call is built, and elaborates about its relevant flags:

[184] https://github.com/Bo0oM/PHP_imap_open_exploit/blob/master/exploit.php



Hello friends!
The carriage will kill me soon, so I am writing the analysis of the fifth task)

1) We all know what the standard imap_open call in php looks like. Like that:

PHP:
```
$imap = imap_open('{'.$_POST['server'].':993/imap/ssl}INBOX', $_POST['login'], $_POST['password']);
```

As we see, in the function we pass the host name, port, flags, and a couple of login: password.
A full list of flags can be found on the official page of this function http://php.net/manual/ru/function.imap-open.php

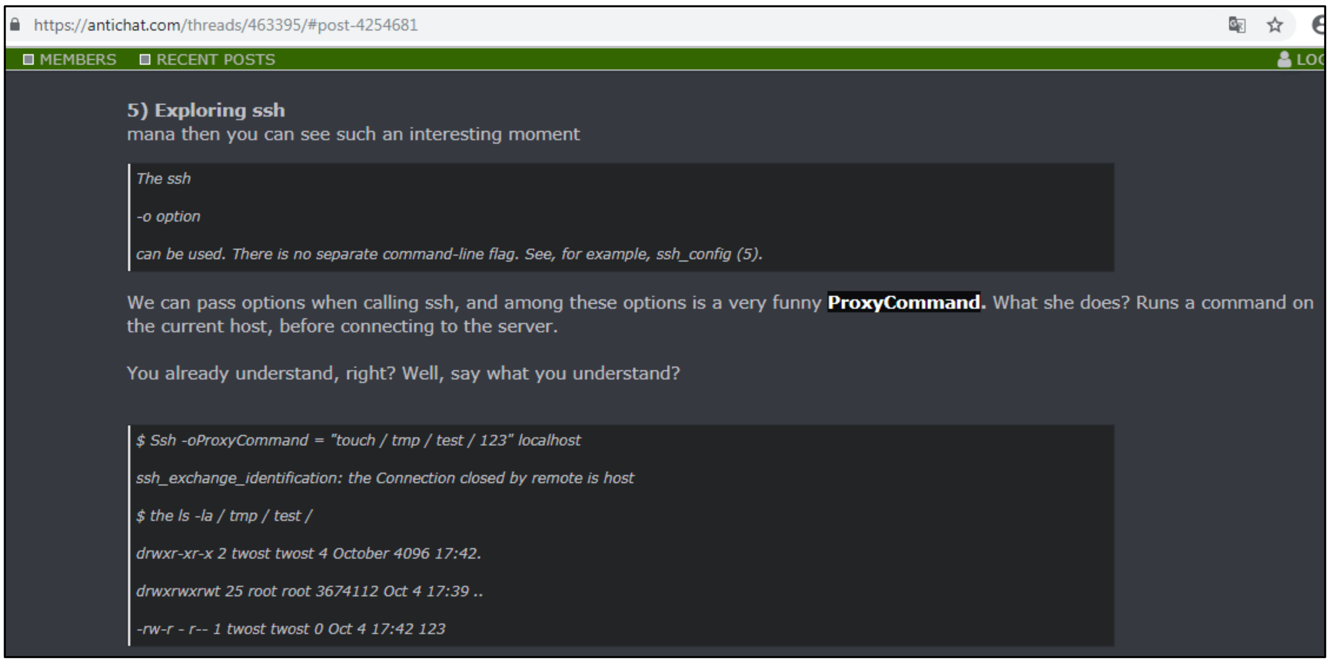
Опциональные флаги

Флаг	Описание
/service=service	сервис доступа к почтовому ящику. По умолчанию "imap"
/user=user	имя пользователя для входа на сервер
/authuser=user	удаленный пользователь для аутентификации; если указано, то это будет тот пользователь, чей пароль используется (например administrator)
/anonymous	удаленный доступ под анонимным пользователем
/debug	записывать телеметрию протокола в специальный лог-файл приложения

In the second part, Twoster explains how to perform the hack with the vulnerability, while using the most relevant flag:

/ norsh do not use rsh or ssh to set up a pre-authorized IMAP session

The fifth phase in the hack is investigating the SSG. Here he reveals the vulnerability itself – using a ProxyCommand command to run commands in the relevant host without connecting to the internet.



5) Exploring ssh
mana then you can see such an interesting moment

The ssh

-o option

can be used. There is no separate command-line flag. See, for example, ssh_config (5).

We can pass options when calling ssh, and among these options is a very funny **ProxyCommand**. What she does? Runs a command on the current host, before connecting to the server.

You already understand, right? Well, say what you understand?

```
$ Ssh -oProxyCommand = "touch / tmp / test / 123" localhost
ssh_exchange_identification: the Connection closed by remote is host
$ the ls -la / tmp / test /
drwxr-xr-x 2 twost twost 4 October 4096 17:42.
drwxrwxrwt 25 root root 3674112 Oct 4 17:39 ..
-rw-r - r-- 1 twost twost 0 Oct 4 17:42 123
```

Two days before the hack (November 13), one of the website admins, BigBear, posted two presentations. The first one is on how to hack Agile Board in Jira, from Atlassian. The second one is about the solution to the challenge presented by Twoster:

KHS2018.pdf 1 / 17

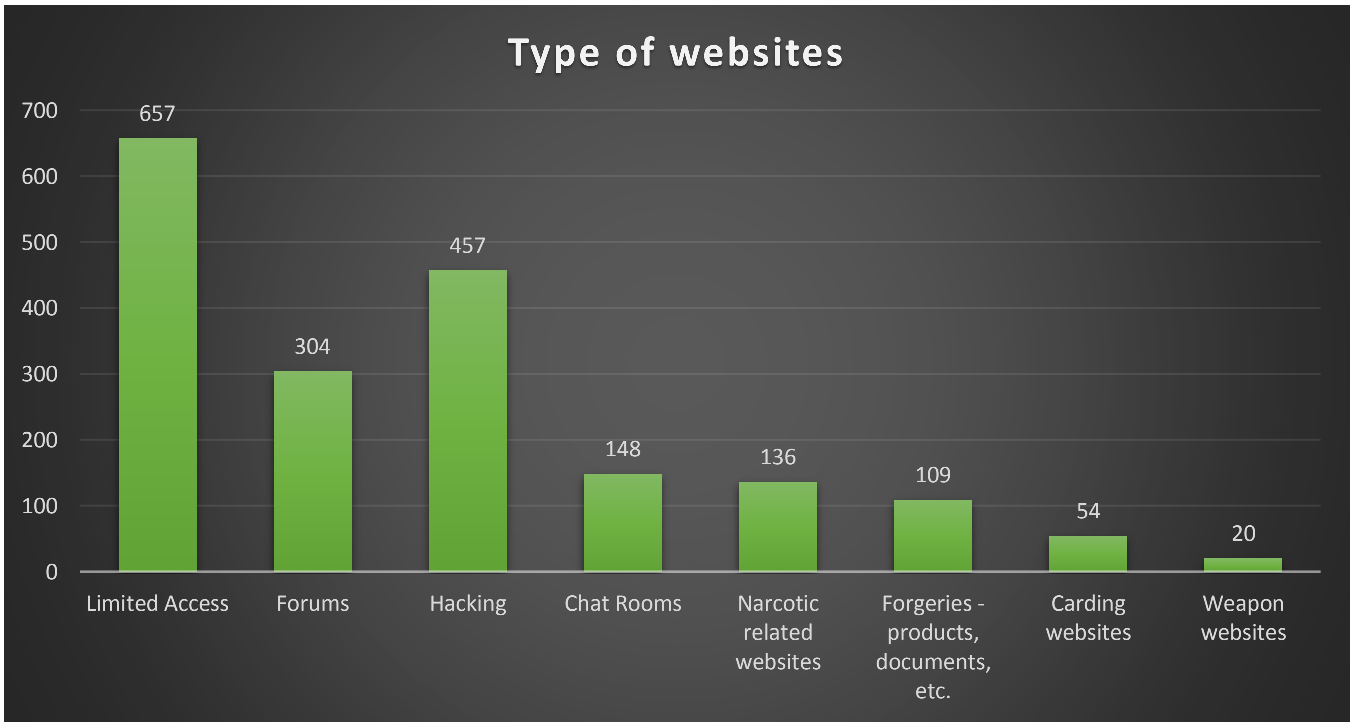
[RCE]
0-day в imap/c-client
на примере PHP

Автор: crlf
Соавтор: Александр Twost

Three days after the hack, Wizmen posted his solution to the vulnerability[185]. In addition to all these note that on November 9th, there was an unknown attempt to login to Wizmen's GitHub account by an unknown actor. He claims that he changed passwords during the hack, but there could be a correlation between the two events.

Consequences

As of early December, the thousands of websites removed from the darknet are not back online. Wizmen claims that he will be able to restore them during December. The blogger Darkowl, an expert on the darknet, stated that erasing the websites from the hosting service lead to erasing 30% of the services on the darknet. He presented statistical data about the types of websites erased[186]:



Moreover, Wizmen listed on his website several other vulnerabilities that could have influenced the hack. As of the time this item was written, it is not clear who is responsible for the attack. It could be the Russian actors who posted the vulnerability on the forum, but there were other theories online:

- In the past, people in the community against child exploitation called for attack groups to perform DDOS attacks on the website, claiming that it does not fight child pornography and does not filter such

[185] https://github.com/DanWin/hosting/commit/db626a54a4f5e3ed4673b88834d6fda3e63f5152
[186] https://www.darkowl.com/blog/2018/daniel-of-the-darknet-goes-dark

- As part of law enforcement's war on various websites on the darknet, in the past years significant markets and forums were closed and their operators were arrested. On some forums, including Reddit, it was suggested that Wizmen himself was arrested and that the website was removed by law enforcement. Note that on July 2017, American law enforcement closed down the two largest markets Hansa and Alphabay, but they posted a picture making the arrest known.
- In the months before the attack, and a bit afterwards, people on the chat were calling for closing the website. According to some actors, the attack could have been executed by an actor with access to the servers.

Wide-scale Propagation of Ransomware in China; Compromising SDK of Popular Programming Software

Info-sec firm Velvet Security discovered[187] that hackers used a "supply chain attack" attack vector to compromise an SDK program version named "EasyLanguage" (widely-used used in many programs in China), in order to propagate ransomware.

The ransomware was first discovered on December 1st; however, by December 4th there were already 100,000 infected computers. The ransom request was 110 Yuan (around 14 euros). The victims needed to pay the sum with WeChat Pay (analogous to PayPal) within three days to get the encryption key to the ransomware. If the ransom would not by paid in time, the encryption key would be erased from the C2 server. Chinese defense companies deciphered the weak encryption, and released the keys. Also, Velvet revealed the hacker's name and the websites he uses to post, and handed all the information it had to Chinese authorities.

Our insights

This is most likely an amateur attack. However, implanting a hostile code in SDK, a programming software used by dozens of Chinese software firms, has resulted in the malicious code being compiled in their applications, and thus significantly challenging and problematic. Software companies around the world use code segments that they add to their code, but their ability to examine the code that they add is inadequate. The result is that we, clients and consumers of "legitimate" programs are completely exposed to attacks of these kind, without the possibility to defense ourselves.

The infection vector and malware capabilities

Hackers used a malicious version of "Easy Language" to inject the code they developed into every Chinese program compiled with it. The malware is also capable of stealing users' information and passwords using Chinese services and platforms such as: Alipay, Taobao, Baidu, AliWangWang, NetEase163 email services and more.

Moreover, the malware gathered information about the infected system including the type of processor, screen resolution, information about the network and a list of installed software. In addition, the malware developer marked it with a reliable digital certificate from Tencent Technologies, so that in some folders the information would not be encrypted, like rtl, tmp, League of Legends and Tencent Games.

In conclusion - It is an interesting action vector. Fortunately for the victims, researchers discovered that the malware uses XOR encryption instead of DES, which keeps a copy of the encryption key in the victims' system in the routing: %user%\AppData\Roaming\unname_1989\dataFile\appCfg.cfg

The researchers posted the decryptor[188] on in the following link: www.huorong.cn/download/tools/HRDecrypter.exe

[187] https://securityaffairs.co/wordpress/78686/malware/china-ransomware-infections.html
188 https://www.huorong.cn/info/1543706624172.html

Attack Campaign Spreads Malware via Vulnerabilities that Neutralize Antivirus Detection

On the 5th of October 2018, the security company Talos exposed a sophisticated attack campaign that uses vulnerabilities in Microsoft Word to spread malware with information theft capability189. These vulnerabilities (CVE-2017-11882190 and CVE-2017-0199191) are known, but the attackers use a unique vector that allows them to disguise the malware from common antivirus engines.

The current campaign spreads at least three prominent malware families - Agent Tesla, Loki and Gamarue. It is possible that this vector will be later used to spread multiple malwares with different capabilities. As of now, we have not found a connection to an attack group or a specific state actor. However, there are several similarities in the initial stage of the attack campaign which occurred several months ago and spread the malware FormBook192. This campaign was also not attributed to a specific actor, and it is unclear whether there is a link between the two.

Attack Vector

The attacker sends a mail with an attachment of a DOCX Word document which secretly downloads a RTF file with a malicious OLE object. The RTF file download is disguised by using vulnerability CVE-2017-0199. Notice that in some of the attacks, the name of the document is disguised as an invoice. Running a test on VirusTotal, only two out of fifty-eight antivirus engines flagged it. However, in these cases it was only reported that the file is wrongly formatted.

In addition, because many RTF parser document opening programs are defined to ignore unknown values or files, the attackers have many more options to disguise the content of the RTF files. For example, in this campaign the attackers also edited the headers of the OLE object so that the malicious code that uses the CVE-2017-11882 vulnerability will appear as a font tag. After the RTF file is downloaded, it delivers the final payload. It is important to note that the attackers used an /objupdate element so that the embedded object will run immediately, without warning or need to interact with the user.

Malware	Comments
Agent Tesla	This malware is in fact off-the-shelf software with a keylogger function[193]. It is marketed as a program for recovering passwords and monitoring children. Many attackers however use it maliciously to steal sensitive information like passwords and usernames from popular programs including common browsers and email-client program outlook. Moreover, Agent Tesla is able to take screenshots, covertly activate the webcam, and download additional files. The version spread in this campaign has exfiltration abilities through SMTP, FTP and HTTP. The exfiltration vector is chosen according to the settings of the infected computer and its environment.
Loki	A malware for information theft which can specifically search and attack crypto-coin wallets. Out of the three, only Loki doesn't have remote control options.
Gamarue	In addition to information theft abilities, this malware can also enable attackers to gain full control on an infected computer.

In conclusion this is a sophisticated campaign that can overcome standard defense systems. As the attacker exploits common vulnerabilities in new vectors in conjunction with multi-layered obfuscation methods, standard security solutions may not detect and/or block such an attack. Nevertheless, the threat can be mitigated to by installing relevant security patches[194][195]

189 https://blog.talosintelligence.com/2018/10/old-dog-new-tricks-analysing-new-rtf_15.html
190 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199
191 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882
192 https://blog.talosintelligence.com/2018/06/my-little-formbook.html
193 https://www.agenttesla.com/about
194 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
195 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

New Cyber Legislations 2018

Throughout 2018 we have seen the results of a long-drawn shift amongst governments and law enforcement agencies to cybercrime and terror. One of the most high-profile events has been the enactment of the GDPR[196]; however, in September we saw several other initiatives and announcements that are expected to further shape future global cyber power-struggles. Below is a review of the recent developments.

U.S. legislation and initiatives

Defense Forward

The most significant of the recent developments is the announcement of two concurrent policies, one by the DoD[197] and the other by the White House[198], outlaying a new and more aggressive national cyber strategy. This new cyber security framework, dubbed by the DoD as "Defense Forward", grants the government and the military greater allowances in executing offensive cyber operations against any entity that poses a threat to the U.S., its interests, or its allies.

These policies represent a major shift in United States' approach on the matter. In previous administrations the overarching framework was a defensive one, rarely taking an overt and public action against national cyber threats. Under President Trumps however, it appears that the U.S. government is now prioritizing cyber-deterrence through strength and aggression. This is a result of several developments from recent years, most notably:

- The continues occurrences of massive data breaches that pose a threat to U.S. national security such as the 2015 OPM breach, and the 2017 Equifax breach.
- The continues and obvert cyber aggression by criminal and nation-state APTs, chiefly Russian, Chinese and North Korean against U.S. private and governmental sectors.
- The growing proliferation and sophistication of attack tools and malware.

The new Strategy has four main pillars of priority, all of which are focus on protecting the availability and integrity of critical services, and are essentially intended to insure the states' position of power in the global economy and cyberspace.

The Financial Services Breach Notification Bill

On September 13, the House Financial Services Committee approved a bill that standardized the data security and breach notification process for the financial sector[199]. Interestingly, the bill was opposed by state regulators

[196] https://www.infosecurity-magazine.com/news/vote-leave-analytics-firm-hit-with/
[197] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
[198] https://assets.documentcloud.org/documents/4916949/National-Cyber-Strategy.pdf
[199] https://www.congress.gov/bill/115th-congress/house-bill/6743/text

claiming that it will undermine the state authority. The Conference of State Bank Supervisors (CSBS) stated[200] on this matter that the bill will limit the states' "ability to protect its residents and oversee state-chartered and state-licensed financial services providers".

The California Consumer Privacy Act (CCPA)

While not as comprehensive, California recently passed a privacy act by the name CCPA[201] that echoes the GDPR. When it will come into effect on 1st January 2020, California residents will be able to:

- Request companies to provide any data that has been collected on them, including when and where it was obtained, as well as where it is being shared.
- Know why the information is being collected.
- Refuse to the sale of that data.
- Be informed what categories of data will be collected prior to its collection.
- And under certain conditions request to delete records.

Other than the direct implications, this act will force any company operating in California to map and gather all the data they have on specific individuals, as well as have the ability to delete it if necessary. This is a massive undertaking, but many companies have already begun the process following GDPR.

Moreover, as California is one of the largest economies in the states, coupled with the public outcry on the back of recent data breach and infringement incidents such as Facebook - Cambridge Analytica[202], this act may have larger ripples the could be seen nation-wide. Accordingly, this will hopefully lead to stricter info-sec policies and better managed databases amongst the affected companies and organizations.

European legislation and Initiatives

The EU

GDPR - As stated, the General Data Protection Regulation (GDPR) came into effect on May 25, 2018, across EU Member States; however with it came a series of directives concerning the processing of personal user data. The new regulation requires organizations and businesses to be fully transparent about how they are using and safeguarding personal data, and be able to demonstrate accountability for their data processing activities. This includes notifying users on the collection and storage of personal data, as well as enabling the data subject to have the data controller erase their personal data, cease any further dissemination of the data and have third parties halt processing of the data.

GDPR is applicable to any company that collects the personal information of EU residents, even if it does not physically operate within Europe. Moreover, the regulation applies to all business involving European subjects or Member States, such as the employment of workers in Europe, operation of subsidiaries within the EU, or conducting marketing campaigns in EU Member States.

In April 2016, the regulation was adopted by the Council of the European Union and the European Parliament to replace the 1995 Data Protection Directive, which was adopted at a time when the internet was still in its infancy and thus outdated. Entities who breach GDPR can face fines of up to 4% of annual global turnover or €20 million (whichever is higher).

European firms must ensure that all business contact with firms within and outside the EU is conducted with companies who comply with the regulations. Organizations based outside the EU must appoint an EU-based person as a representative and point of contact for their GDPR obligations. Therefore, non-European companies

200 https://www.csbs.org/csbs-opposes-hr-6743-consumer-information-notification-requirement-act
201 https://www.caprivacy.org/
202 https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far

conducting business transactions with EU firms must implement measures to adjust to the regulation and comply with its obligations.

Consequently, even before the regulation came into force, numerous companies in EU Member States began notifying their customers about updates to their privacy policies in accordance with GDPR. But, this also laid the ground for various cybercriminals attempting to carry out phishing attacks using social engineering methods.[203] Moreover, we detected a number of additional phishing attempts, such as those impersonating Gmail, MyetherWallet and PayPal.

Other EU initiatives - while the U.S. new cyber policy is the most prominent, other countries and political bodies have also begun taking similar steps. For example, on September 13, the European Parliament's ENISA Commission (European Union Agency for Network and Information Security) adopted a cybersecurity act[204], which promotes new initiatives to further improve EU countries' cyber resilience, deterrence and defense. It should be noted that this policy follows another first EU-wide legislation by the name Network Information Systems (NIS) Directive[205], which came into effect in May of this year. The objectives of the NIS Directive include:

- Improving cybersecurity capabilities at a national level.
- Increasing EU-level cooperation and conducting risk management.
- And implementing incident reporting obligations for operators of essential services, critical infrastructure and digital service providers.

The results of this initiative were seen over in 2018 with several operations such as the Europol led 'Operation Power Off', which seized and shut down the infrastructure of the world's largest DDoS-as-a-service website[206].

The UK

Building on the success of the GDPR, several countries have also passed additional bills and implemented new cyber security measures. Perhaps most notable in this aspect is the UK, who took many steps in this direction over the last year. Most recently, in late September, the Ministry of Defense (MoD) and surveillance service GCHQ announced the launch of a new and dedicated £250m cyber task force designed to strengthen the UK's offensive cyber capabilities.

According to general Richard Barrons, former commander of Joint Forces Command, by adopting offensive cyber techniques the UK will "level the playing field" and gain new means of deterrence and punishment. This task force follows a recent announcement by the British government[207] on the establishment of a specialized court complex in London for cybercrime cases, expected to be completed by 2025.

This task force follows several successful achievements throughout 2018. For example, in April the GCHQ in coalition with the Ministry of Defense has launched a wide-scale offensive campaign against ISIS; the first time the UK conducted a systematic and persistent cyber-attack as part of a wider military campaign according to GCHQ director, Jeremy Fleming. More recently, in August the European Commission begun looking to mandate social networks to take down terror content within one hour. This move follows social media platform's apparent self-regulation failure on this matter.

[203] https://resources.infosecinstitute.com/gdpr-provides-scammers-with-a-new-gold-opportunity/
204 http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf
205 http://europa.eu/rapid/press-release_MEMO-18-3651_en.htm
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505297631636&uri=COM:2017:476:FIN
206 https://www.infosecurity-magazine.com/news/major-take-down-of-site-selling/
207 https://www.gov.uk/government/news/worldclass-fraud-and-cybercrime-court-approved-for-londons-fleetbank-house-site

According to security commissioner, Julian King, the various social media companies such as Facebook, Google and Twitter have not shown enough progress on the issue since voluntary guidelines were tightened March 2018. This issue appears to stem in part due to a lack of consistency across the various platforms in how such material is handed.

Although these are steps in the right direction, it should be noted that the UK still faces several significant issues. For example, early this year it was revealed that every NHS Trust has failed to meet the recommended data security standards. Later in March it revealed[208] that less 20% of the nearly 200,000 employed by the UK police today went through cybersecurity training. Further, recently it was reported[209] that 46% British local authorities' systems are still running outdated such as Windows Server 2000, Windows Server 2003 and Microsoft SQL Server 2005.

It should be stated that both the NHS[210] and police force received funding to address these issues. Further in late May the NHS even launches a national Opt-Out service to improve patient control of Protected health information (PHI)[211]; mandating by 2020 all health and care organizations to enable patients to choose if they wish to only allow their personally identifiable data used for their care and treatment, or if they wish to allow their data to be shared with other healthcare organizations for planning and research purposes.

Nevertheless, it is yet to be seen what changes will actually take place. Even more worrying, is that a recent research[212] found that security professionals in the UK are increasingly engaging in Grey Hat activities. The reasoning to this appear to primarily be the opportunity to earn more money, the challenge, and/or wanting to retaliate against a former employer.

One of the most striking fact highlighted by the report was that UK organizations' security budgets are lower than those in the US, Germany, Australia, and Singapore. As per the report, organisations in the UK with 2,500 or more employees had an average cyber-security budget of just under £200,000 last year, and is expected increase

this year by only £20,000. Moreover, as most of the security budget of organizations in the UK is spent on mitigation and remediation (on average £188,000 per year), the average starting salary for an entry-level security professional in the UK is the lower than for those in the US, Germany, Australia, and Singapore.

This fact, often coupled with demanding requirements and work hours, causes many British security professionals to take part in Grey-Hat activities. One in 13 UK professional has admitted having been involved in such activities compared to 1 in 22 globally. Further, 53.7% said that they would consider doing so again if opportunity to earn more. Accordingly, it is no surprise that the UK was the most cyber breached country in Europe in 2017[213].

Additional European countries

In late August Poland brought in to effect comprehensive cybersecurity legislation by the name ANCS[214] (Act on the National Cybersecurity System). However, on top of the protection of personal data like the GDPR, it aims to also protect essential services such as banking, water, food, electricity, transportation etc.; similar to the new U.S. cyber security strategy. Other European countries who recently passed a cyber security legislation are:

208 http://parliamentstreet.org
209 https://www.comparex-group.com/web/uk/en/comparex.htm
210 https://www.infosecurity-magazine.com/news/nhs-gets-150m-cyberspending-boost/
211https://www.computerweekly.com/news/252441825/NHS-to-launch-national-data-opt-out-tool
212 https://go.malwarebytes.com/OstermanCostofCybercrimeQ3FY19_UK.html
213 http://www.professionalsecurity.co.uk/news/interviews/uk-most-cyber-breached-in-europe/
214 https://www.jdsupra.com/legalnews/poland-implements-comprehensive-47571/

- Poland – August – ANCS (Act on National Cybersecurity System) [215] .
- Ireland (Sep. 18) - Priority Data Protection, Cyber-Security and IP Legislation for Autumn 2018[216].
- Portugal (Aug. 13) – Legal Framework of Cybersecurity (Regime Jurídico da Segurança do Ciberespaço – RJSC)[217].

Conclusions

These developments are significant and likely shape the cyber landscape for the following years. However, with that in mind, we should also take in to consideration how they can also have adverse consequences.

The first is the negative ramifications of GDPR and similar initiatives. Despite the new data protection these new data laws provide consumers, it also gives malicious actors a greater wall of anonymity to operate under. This unfortunately undermine some the initial intentions that caused them to come in to place. As a result, this new environment could possibly be exploited by various cybercriminal actors against sectors that previously remained, for a variety of reasons, relatively unscathed from major cyber attacks (compared to the financial and health sectors for example).

The second relates to the new more aggressive cyber defense initiatives. In recent years we have seen the cybersphere increasingly becoming a new fighting ground between nations and political powers, chiefly Russia, China and North Korea. United States and Western European countries have remained relatively restrained, however with these recent legislation and initiatives we are beginning to see a shift in their approach.

It is unclear at the moment how this will play-out, but with the ever-growing dependency on technology and interconnected eco-systems, resulting in larger stakes and possible financial gains, we are unlikely to see cybercriminals and nation-state APTs restraining their activity.

215 https://www.jdsupra.com/legalnews/poland-implements-comprehensive-47571/
216 https://www.taoiseach.gov.ie/eng/Publications/Publications_2018/Legislative_Programme_Autumn_2018.pdf
217 http://www.mondaq.com/x/738882/Security/Cybersecurity+Legislation

Anti-Criminal & Terror Operations 2018

Concurrently to the cyber legislation and initiatives that took place in 2018, we also saw significant law enforcement operations around the world against criminal and nation-state cyber actors. It appears that this shift began in 2017 with the take down of two of the largest Darknet markets – Alphabay[218] and Hansa[219], by European agencies and the FBI.

Initially, the ramifications of these take downs were unclear. However, in contrast to previous operations such as the take down of Silk-Road market[220], as of late 2018, it seems that these efforts have resulted in lasting changes across the cyber sphere. Further, in our assessment, this change is still in its infancy. As governments are empowering their militaries and law enforcement agencies to act against cybercrimes, in conjunction with the establishment of new and dedicated anti-cybercrime bodies, and the expansion of global cooperation, we expect that in the following years we will continue seeing major campaigns against malicious cyber actors.

Below is a review of the most significant events that took place or were exposed this

Operation WireWire – Global Crackdown Against Business E-mail Compromise

On June 11, 2018, the Federal Bureau of Investigation (FBI) and the US Department of Justice, announced the results of a coordinated six-months long takedown operation to disrupt and end international business e-mail compromise (BEC) frauds, which continuously target businesses and individuals worldwide[221]. The operation, dubbed WireWire, included the involvement of multiple law enforcement and government institutions in the US and abroad.

BEC, sometimes referred to "Man-in-the-Email" or CEO scams, is a sophisticated type of financial fraud carried out using a variety of methods, usually social engineering. For example, an attacker often impersonates a senior figure in an organization and targets employees with access to company finances. The criminal then attempts to trick the targeted employee into making wire transfers to bank accounts that appear to belong to trusted partners, but are controlled by the cybercriminals. These bank accounts most often belong to third-parties that are dubbed Money Mules. They are in charge of receiving the stolen funds directly from the victim organization and transferring it to other accounts, which belong to the threat actor.

Operation WireWire, the largest international effort to tackle the issue of BEC fraud, resulted in 74 arrests, among them 42 were in the US, 29 in Nigeria, and three in Canada, Mauritius, and Poland. Moreover, the FBI and its international partners successfully seized $2.4 million and recovered or disrupted about $14 million in fraudulent wire transfers. The bills of indictment contained charges for both international criminal organizations that

218 https://www.fbi.gov/news/stories/alphabay-takedown
219 https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
220 https://www.wired.com/2013/11/silk-road/
221 https://www.fbi.gov/news/stories/international-bec-takedown-061118

defrauded small- to large-sized businesses as well as those targeting individual victims who transferred large sums or sensitive records in the course of business. The impact of BEC and EAC (e-mail account compromise) scams is far reaching, as they do not only affect individual businesses but also the global economy, as since the Internet Crime Complaint Center (IC3) began formally keeping track of this kind of fraud, there here has been a loss of over $12.5 billion.[222]

FBI Arrests Three High-Ranking Members of Russian Cybercrime Group FIN7

In early August 2018, three East European citizens, members of the cybercrime group FIN7 (aka Carbanak), were indicted by the FBI.[223] The suspects, Dmitry Fodorov (44), Fadir Heldir (33) and Andrei Kolpakob (30) were allegedly high-ranking members of the Russian cybercrime group, which has been active since at least 2013.

The group has successfully attacked over 100 companies and organizations across many sectors, including restaurants, hotels, gaming and gambling, financial institutions, software companies, real estate companies, government institutes, etc. The group often targets organizations that deal with financial information, such as customers' credit cards, which are then put up for sale on the dark net. The group has committed numerous cybercrimes in the US. Accordingly, in recent years the FBI together with other investigators and law informant agencies around the world, have tried to apprehend members of the group and disrupt their activities.

Cyber security firm FireEye published in August a report regarding FIN7's modus operandi.[224] The group appears to have invested considerable resources in developing new tools and capabilities. Moreover, its members often change their attack methods in order to make their activity more difficult to attribute. Nevertheless, it has been identified that the group tends to use phishing emails as their main penetration vector. For example, in 2016 the group used Microsoft Office docs embedded with malicious Macros. These were both attached to the email and were downloadable via a Google drive link.

The first sign pointing to the evolution of FIN7's tactics was detailed in an April 2017 report by FireEye. The report reviewed a spear-phishing campaign that involved emails with hidden shortcut (LNK) files containing malicious VBScript (Visual Basic). FireEye attributed the files' metadata and the infection vector to FIN7. Note that in 2017, researchers were able to view the original path from which the LNK files were created, as well as the hostnames, MAC addresses and even the desktop environment (DE) of the attackers.

The group generally worked within virtual environments that have generic and dynamic hostnames. Another noteworthy development is the group's utilization of digital certificates. Namely, FIN7 digitally signed malicious files in order to increase their credibility when checked by security systems, thus increasing the chance of penetration, infection and evasion.

Operation Power Off – Take-down of World's Largest DDoS-as-a-service website

In an operation dubbed Operation Power Off, law enforcement agencies from around the globe seized and shut down the infrastructure of the world's largest DDoS-as-a-service website, webstresser[.]org.[225] As of April 2018, Webstresser had 136,000 registered users who requested about four million attacks on various financial institutions and governments. Once the domain of skilled and sophisticated attackers, disruptive DDoS attacks are now offered as a service by criminal actors, which effectively allows anyone with a vendetta or other motivation to launch such attacks on any chosen target.

222 https://www.ic3.gov/media/2018/180712.aspx
223 https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
224 https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
225 https://www.infosecurity-magazine.com/news/major-take-down-of-site-selling/

The services provide buyers with user-friendly interfaces that allows them to customize their attack according to such categories as duration, volume and method. In some cases, providers of DDoS-as-a-service demand ransoms from targets in exchange for calling off a planned attack. As opposed to traditional ransomware attacks, victims may be extorted prior to even losing any data.[226] Crimeware-as-a-service is a lucrative business and earns cybercriminals about $1.6bn per year, with DDoS-as-a-service generating about $13m of revenue per year.

Eight Arrested in an International Take-Down of African-Based Cyber-Scam Operation

In late June, the FBI announced that it arrested eight individuals United States and Africa for allegedly operating a wide-spread fraud campaign against U.S companies and citizens since at least 2012, stealing approximately $15 million. The operation led by the FBI, named "Operation Keyboard Warrior", was a joint international effort disrupt online frauds executed from Africa, including various romance scams, fraudulent-check scams, gold-buying scams, advance-fee scams, credit card scams, and BEC scams. The defendants are being charged with conspiracy to commit wire fraud, wire fraud, conspiracy to commit money laundering, conspiracy to commit computer fraud, and aggravated identity fraud.

Multiple Members of Cybercrime Group Rex Mundi Arrested in International Operation

In a joint international operation between various law enforcement agencies, Europol arrested 15 members of the hacker extortion group known as "Rex Mundi" (Latin for "king of the world"); publicly active since 2012. The latest of the arrests took place in early June 2018, when a French national was apprehended in Thailand. Their main modus operandi is hacking organizations, stealing sensitive data and demanding a ransom by threatening to publicly leak the data unless they are paid. The group demands payment almost exclusively in Bitcoins.

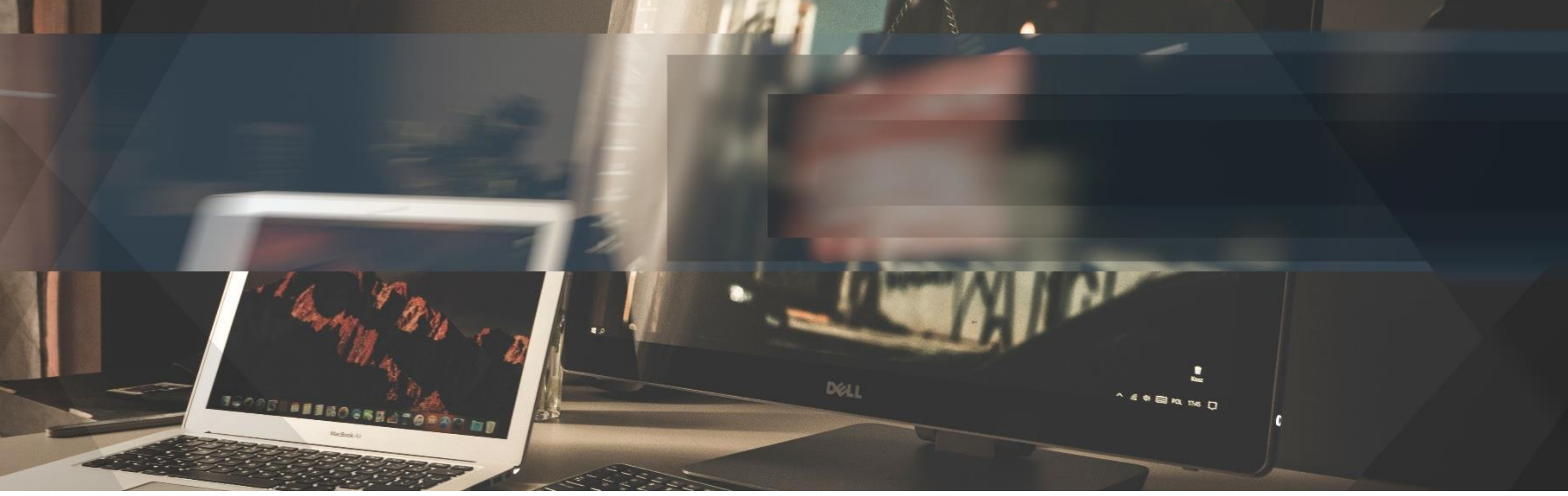
The group has made a name for themselves after successfully targeting large international companies and organizations including, Domino's pizza, Swiss bank Banque Cantonale de Genève, French loan company Credipret, Belgian payroll firm Easypay Group and French diagnostic laboratory Laboratoire de Biologie Médicale[227]. The international operation, which was supported by the Joint Cybercrime Action Taskforce (J-CAT)[228], was launched following a major cyber attack against an unnamed UK company in May 2017.[229] The group demanded $770,000 for not disclosing the stolen data, or $1.1 million for information on how the group compromised the firm's systems.

'Operation Darkness Falls' – Continued Law Enforcement Activity Against Darknet Actors

On August 22, The US Department of Justice, together with several other US agencies announced the result of "Operation Darkness Falls,"; a joint operation targeting people and organizations that sell drugs such as fentanyl over darknet markets.[230] According to the announcement, the operation resulted in the arrest several large vendors, including of one of the most prolific Darknet Fentanyl vendors in the world.

This operation follows another wide-scale 'crackdown' on Darknet criminal activity announced by UK Home Secretary in April.[231] To facilitate this campaign, a £9 million fund was created to fight online illegal activity such as the selling of firearms, drugs, malware and people. The funding is part of £50 million newly allocated money for UK law enforcement agencies to tackle cybercrime at a national, regional and local level in 2018 and 2019.

226 https://www.itgovernance.co.uk/blog/ddos-as-a-service-providers-offer-customer-loyalty-programmes/
227 https://www.bankinfosecurity.com/rex-mundi-hacker-extortion-group-busted-a-11093
228 https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce
229 https://www.infosecurity-magazine.com/news/europol-disrupts-rex-mundi/
230 https://www.justice.gov/opa/pr/operation-darkness-falls-results-arrest-one-most-prolific-dark-net-fentanyl-vendors-world
231 https://www.gov.uk/government/news/home-secretary-announces-law-enforcement-crackdown-on-dark-web

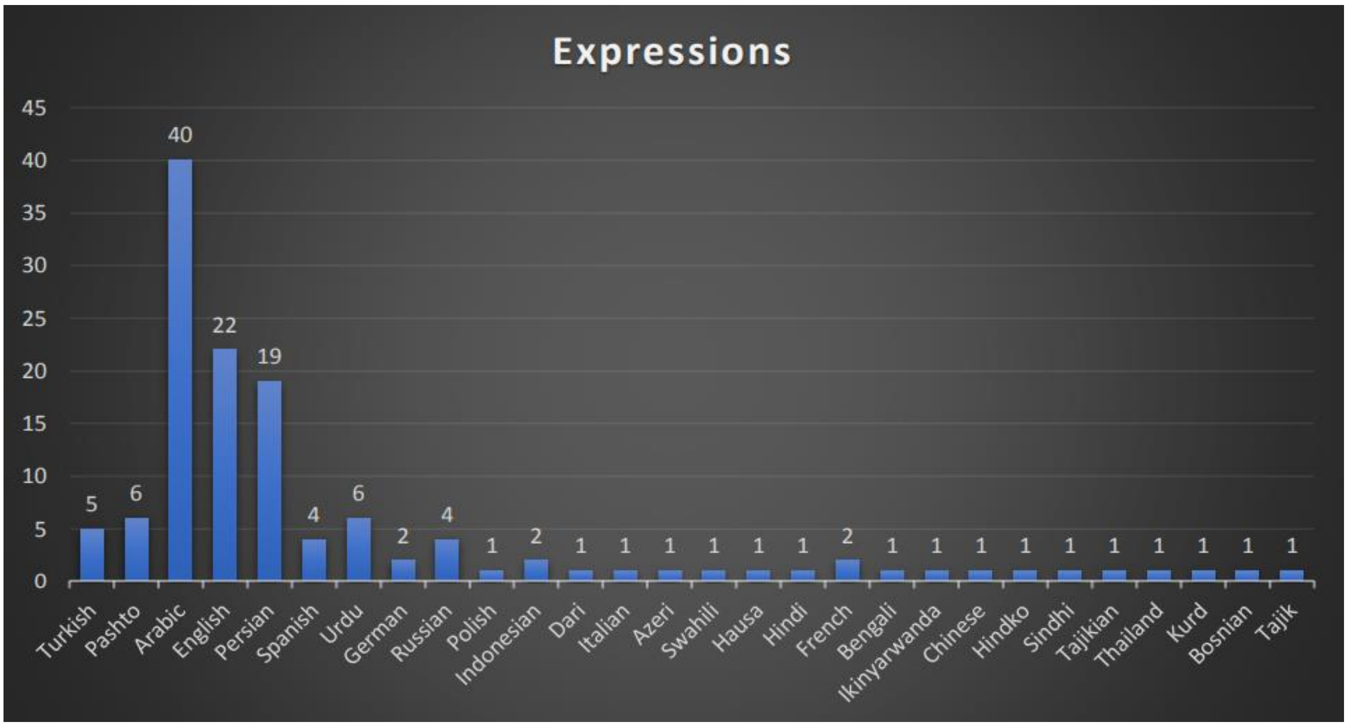


Clearsky Investigations - Cyber Disinformation Operations

Throughout 2018 Clearsky has begun implementing expansive efforts in exposing disinformation and fake-news operations. As part of our investigations, we have exposed 3 large-scale fake-news operations; two of which run uninterruptedly for the last 8 years. Furthermore, we also have been monitoring closely after the cyber activity surrounding several key global events, including the US mid-term elections, the US withdraw from the nuclear treaty, and the France's "yellow vest" protests.

Large-Scale Global Iranian Disinformation Operation

Our research, which was partly based on an initial data by FireEye, mapped, analyzed and exposed the full infrastructure of a wide-scale disinformation operation, comprised of 98 fake news outlets; each with its own websites and array of supporting social media accounts and pages. Moreover, several of the most popular sites had their own mobile apps. This operation, active since at least 2012, targets 28 countries, political bodies and geo-political regions (e.g. North Africa and Eastern Europe). Accordingly, the infrastructure utilizes multiple languages such as Arabic, Persian, English, Urdu and Pashto.



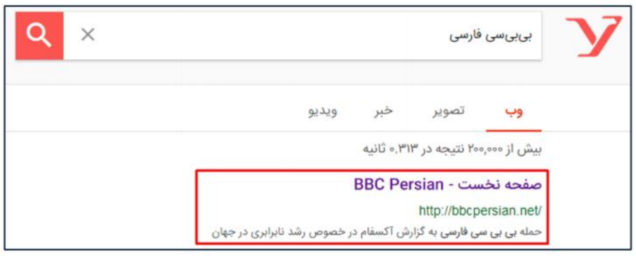
About a week after our research was published concurrently on our website and by Reuters', the Russian propaganda website "Sputnik news" wrote an article countering our findings.[232]

This article blamed us in disseminating false information and Anti-Iranian propaganda, as part of "information war", allegedly lead by the US Secretary of State Mike Pompeo. According to Sputnik News, by publishing this report Clearsky attempted to cause a rift between Russia and Iran, Further, they quote high ranking Iranian officials speaking against Clearsky. However, note that Sputnik claims are unfounded and they provide no hard evidence to support them. Nevertheless, this article does show the level of public exposure our research and publication received.

Ayatollah BBC – Iranian Disinformation Operation Impersonating Western News-Outlets

In late February we publish an extensive research report exposing a large-scale Iranian disinformation operation, active uninterruptedly since 2011. At the center of the operation is the BBC Persian website. We call this operation Ayatollah BBC.

We estimate that the main objective of the operation is to undermine the credibility of western media outlets in the eyes of Persian speakers, presenting them as driven by political agenda and acting against the Iranian regime. Other objectives could be deterring Iranians from trusting websites they visit, and potentially spreading malware. Note that while we do not have proof of malware being propagated by websites covered in this report, in previous campaigns, such as Charming Kitten, fake news websites were used in this capacity.



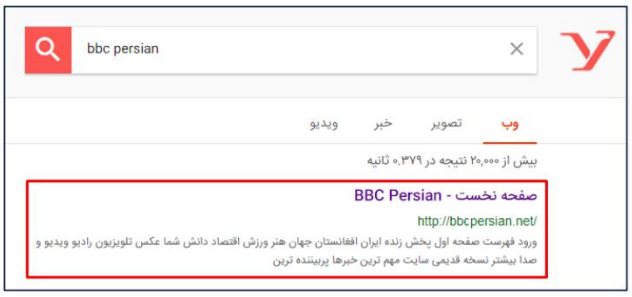
بی‌بی‌سی فارسی

بیش از ۲۰۰,۰۰۰ نتیجه در ۰.۳۱۳ ثانیه

صفحه نخست - BBC Persian

http://bbcpersian.net/

حمله بی بی سی فارسی به گزارش آکسفام در خصوص رشد نابرابری در جهان



bbc persian

بیش از ۲۰,۰۰۰ نتیجه در ۰.۳۷۹ ثانیه

صفحه نخست - BBC Persian

http://bbcpersian.net/

ورود فهرست صفحه اول پخش زنده ایران افغانستان جهان هنر ورزش اقتصاد دانش شما عکس تلویزیون رادیو ویدیو و صدا بیشتر نسخه قدیمی سایت مهم ترین خبرها پربیننده ترین

Some websites were established over seven years ago, and have high rankings in search engines. In Google, Yahoo and Yandex the impostor BBC website is one of the top results in the first result-page. In Yooz and Parsijoo, Iranian search engines designed specifically for Persian speakers, only the impostor website appears in search results, and the legitimate website is not found at all.

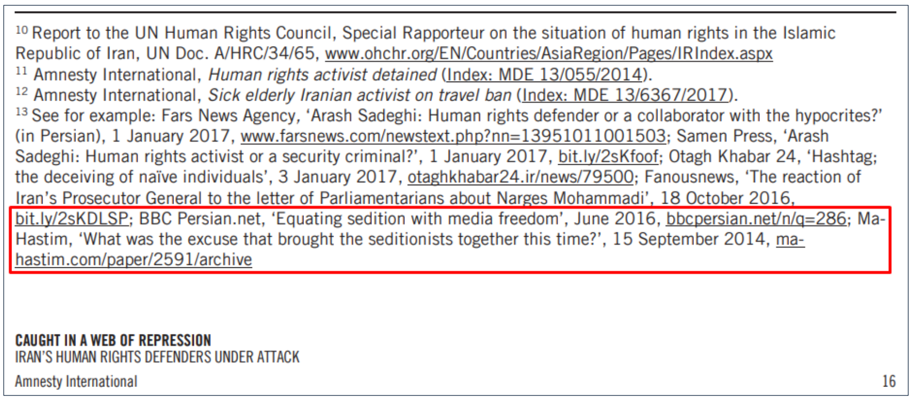
The websites are promoted through social networks, such as Facebook, Twitter and Telegram. In addition to websites impersonating western news outlets, we found websites impersonating Iranian news outlets.

These websites aim to defame foreign media outlets and blacken their name to Iranians. Furthermore, they generate original content including video, podcasts,

[232] https://sputniknews.com/analysis/201812091070537795-iran-whistleblowers-propaganda-fact-checking/

articles and "news" items. The fake websites are meticulously built, and may fool even researchers and legitimate media outlets.

An example of the extent to which this impersonation has been successful: An Amnesty International report, published on the US department of justice website, deals with persecution of human rights activists inside Iran. Two of the sources cited as examples of such persecution, are taken from fake websites - bbcpersian[.]net and ma-hastim[.]com - the citers unaware of the websites being fake[233]. The same footnote also quotes real Iranian news-sites, such as Fars News.



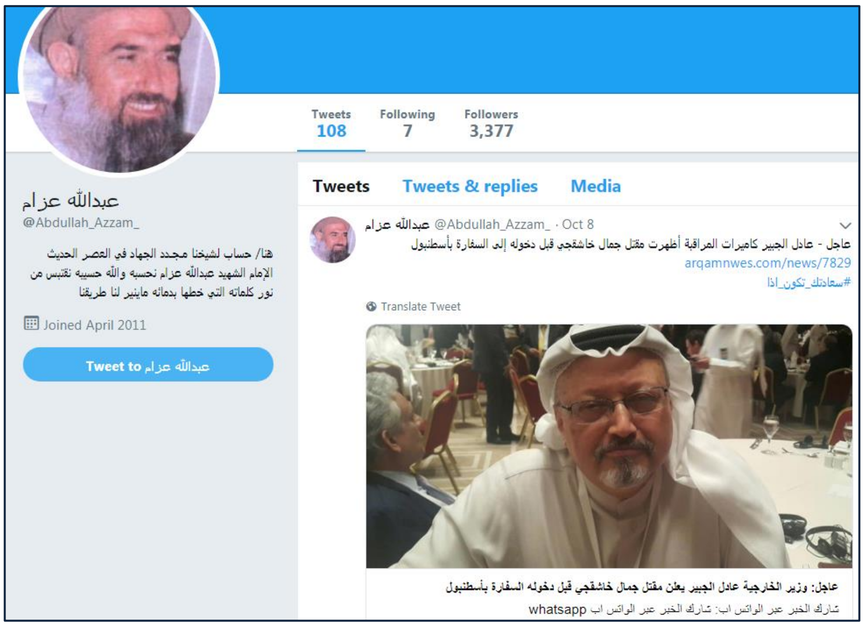
10 Report to the UN Human Rights Council, Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, UN Doc. A/HRC/34/65, www.ohchr.org/EN/Countries/AsiaRegion/Pages/IRIndex.aspx
11 Amnesty International, *Human rights activist detained* (Index: MDE 13/055/2014).
12 Amnesty International, *Sick elderly Iranian activist on travel ban* (Index: MDE 13/6367/2017).
13 See for example: Fars News Agency, 'Arash Sadeghi: Human rights defender or a collaborator with the hypocrites?' (in Persian), 1 January 2017, www.farsnews.com/newstext.php?nn=13951011001503; Samen Press, 'Arash Sadeghi: Human rights activist or a security criminal?', 1 January 2017, bit.ly/2sKfoof; Otagh Khabar 24, 'Hashtag; the deceiving of naïve individuals', 3 January 2017, otaghkhabar24.ir/news/79500; Fanousnews, 'The reaction of Iran's Prosecutor General to the letter of Parliamentarians about Narges Mohammadi', 18 October 2016, bit.ly/2sKDLSP; BBC Persian.net, 'Equating sedition with media freedom', June 2016, bbcpersian.net/n/q=286; Ma-Hastim, 'What was the excuse that brought the seditionists together this time?', 15 September 2014, ma-hastim.com/paper/2591/archive

CAUGHT IN A WEB OF REPRESSION
IRAN'S HUMAN RIGHTS DEFENDERS UNDER ATTACK
Amnesty International 16

Fake News Network Targeting Saudi Arabia

In collaboration with Reuters we published in November a research report exposing a new disinformation infrastructure. It was active for at least the past two years, and targeted Saudi audience[234]. This network contains over sixty news websites, spreading fake news about significant events in Saudi Arabia. The fake news was biased against the Saudi regime and King Salman.

In late 2018, the network focused on propaganda against the Saudi regime regarding the murder of the Saudi journalist Jamal Khashoggi.[235] The fake news was spread via bots on social networks, and also with a fake profile of Abdullah Azam, the founder of Al-Qaida.



عبدالله عزام
@Abdullah_Azzam_
هنا/ حساب لشيخنا مجدد الجهاد في العصر الحديث الإمام الشهيد عبدالله عزام نحسبه والله حسيبه نقتبس من نور كلماته التي خطها بدمائه ماينير لنا طريقنا

عبدالله عزام @Abdullah_Azzam_ · Oct 8
عاجل - عادل الجبير كاميرات المراقبة أظهرت مقتل جمال خاشقجي قبل دخوله إلى السفارة بأسطنبول
arqamnwes.com/news/7829
#سعادتك_تكون_اذا

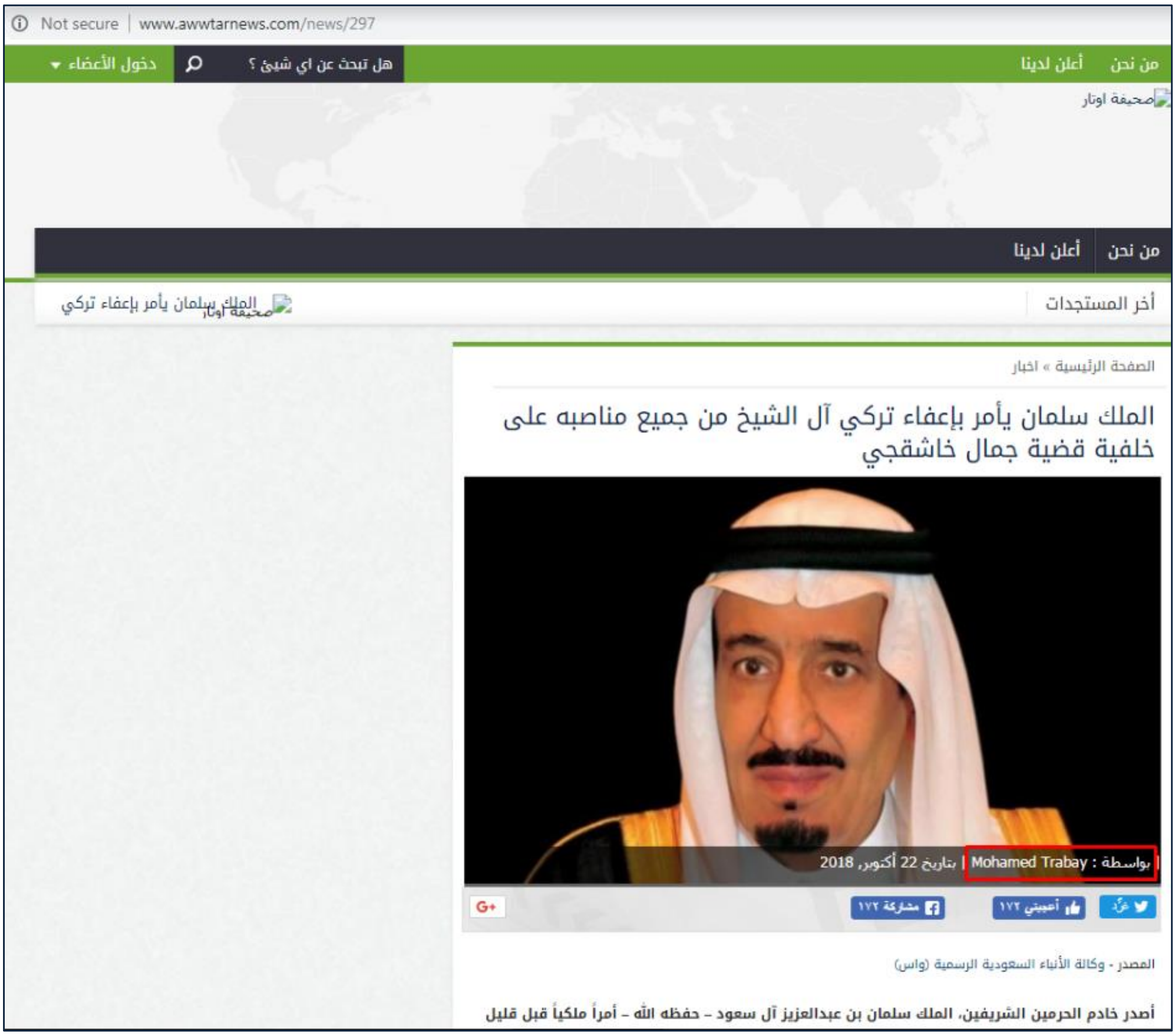
عاجل: وزير الخارجية عادل الجبير يعلن مقتل جمال خاشقجي قبل دخوله السفارة بأسطنبول
شارك الخبر عبر الواتس اب: شارك الخبر عبر الواتس اب whatsapp

The Whois details of the websites revealed that a founder of one the websites is an Egyptian named Mohammad Trabay. On one of the websites, Trabay is identified as the photographer of a picture of King Salman – one of the official and most familiar pictures of the king.

On the other hand, in another website in the network that is almost completely identical to the first website, another person was identified as the photographer. When Reuters asked him about it, he denied any connection to the infrastructure. Note

233 https://www.justice.gov/eoir/page/file/986541/download
234 https://www.reuters.com/article/us-saudi-khashoggi-disinformation/fake-news-network-vs-bots-the-online-war-around-khashoggi-killing-idUSKCN1N63QF
235 Jamal Khashoggi is a Saudi Journalist that was known for his stark opinions against the Saudi regime. On October 2nd, he was missing after visiting the Saudi consulate in Istanbul. The Turkish government blamed Saudi Arabia for murdering him. At first, the Saudis denied any connection to the event, but on October 19th they admitted that Khashoggi was killed during a fight in the consulate.

that the actors operating the infrastructure used the same severs used for Iranian disinformation that we previously identified.



Not secure | www.awwtarnews.com/news/297

من نحن أعلن لدينا

هل تبحث عن اي شيئ ؟

دخول الأعضاء

صحيفة اوتار

من نحن أعلن لدينا

أخر المستجدات

الملك سلمان يأمر بإعفاء تركي

الصفحة الرئيسية » اخبار

الملك سلمان يأمر بإعفاء تركي آل الشيخ من جميع مناصبه على خلفية قضية جمال خاشقجي

بواسطة : Mohamed Trabay | بتاريخ 22 أكتوبر, 2018

غرّد أعجبني ١٧٢ مشاركة ١٧٢

المصدر - وكالة الأنباء السعودية الرسمية (واس)

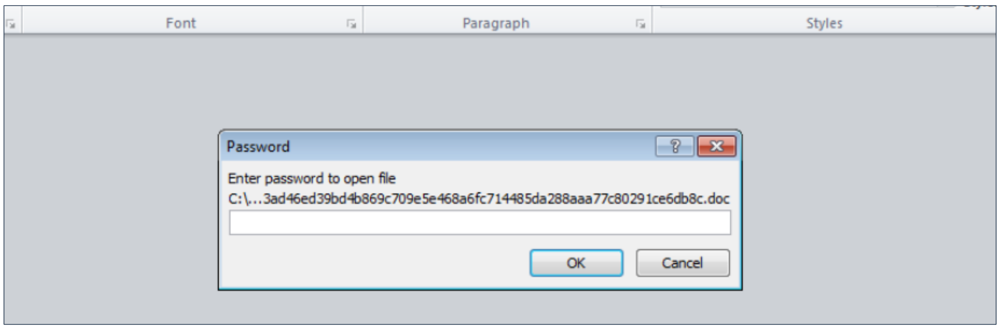
أصدر خادم الحرمين الشريفين، الملك سلمان بن عبدالعزيز آل سعود – حفظه الله – أمراً ملكياً قبل قليل

Note that most of the websites were taken down before the Reuters report was published; however, some of the websites can still be seen on Google's cache.

January

New OilRig attack vector via a fraudulent Intel security program file | New OilRig Malware

The Iranian threat agent OilRig is amongst the most significant groups currently operating in the Middle East. In January we reviewed one of their attacks executed against an entity in Lebanon. This attack is of note because this was the first time that the group used a password protected file. I.e. only the target, who presumably receives the password with the email or via fraudulent phone call, can open the malicious document:



Password

Enter password to open file
C:\...3ad46ed39bd4b869c709e5e468a6fc714485da288aaa77c80291ce6db8c.doc

The infection is executed via a Word document by the name strategy preparation.dot, which contains a malicious Macro that compiles the malware and creates a timed execution task. The malware is displayed in the end of the document as base64, and is translated to the executable file by the Macro code.

Later in January we detected a new OilRig Malware that was used against an unknown entity in United Arab Emirates. Based on the sample's metadata we found a direct link to two other malwares written by the Iranian OilRig group.

New Charming Kitten social engineering attack vector

Charming Kitten group is constantly improving and evolving their social engineering attack vectors. In January we reviewed an attack executed against an Israeli individual. The attack was comprised of two stages: stage one – establishing a believable background story; stage 2 – sending a spear phishing email.

Stage 1 – establishing the narrative - In this stage the attackers send to the target a preliminary email with no malicious content, establishing the next stage of attack. In the recent case, the email contained real content stolen from a University of Chicago's press release, regarding a former senior advisor to President Obama named Valerie Jarrett, who joined the University law school.

The attackers copied the content of the article, created a fraudulent email impersonating University of Chicago news press, and sent the email to their target.

Note three suspicions aspects with the email:

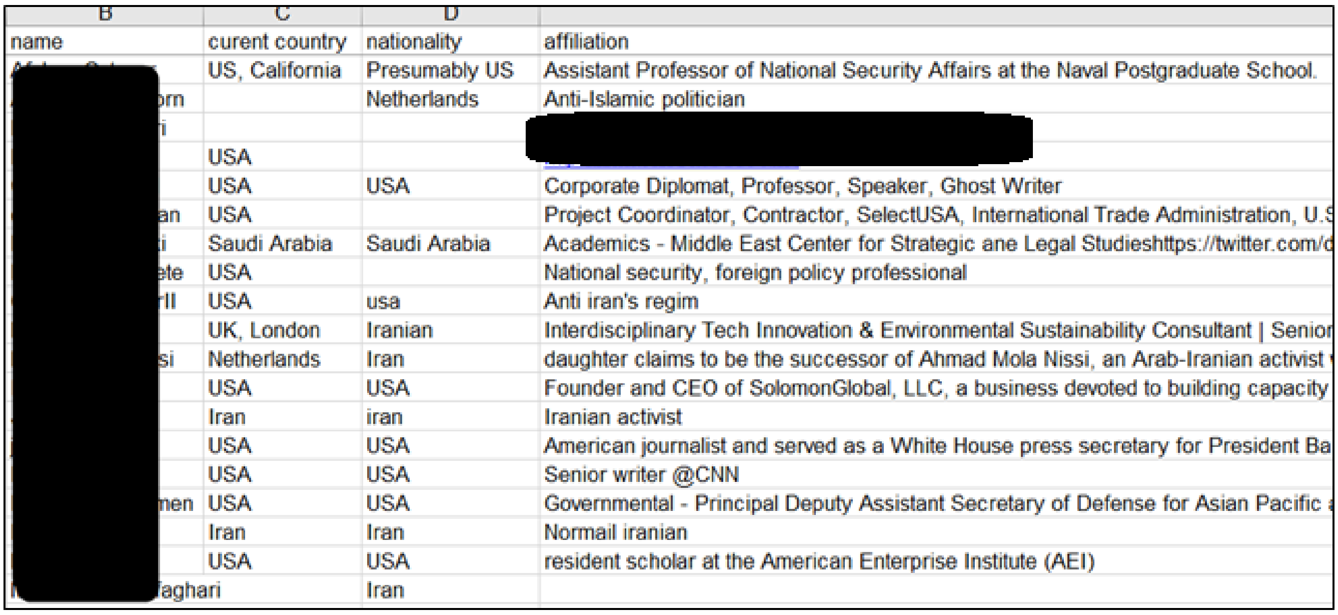
1. **The email was sent from a Gmail account** (broadcasertnewsagency@gmail.com), not from a University of Chicago email account.
2. **The publication date of the article** is December 11th, 2017, however the email was sent over a month later. This is a remarkably long time to distribute a published news article.
3. **The links in the article do not direct directly to the university's website**, but go through an Ad service - advmailservice.com. While this service is not malicious, as reported previously by us, the threat actor Charming Kitten often use it in order to monitor malicious emails.

Stage 2 – sending the malicious phishing email - About an hour later, the attacker sends a phishing email, seemingly unrelated to the first email, in which an individual by the name Valerie Jarrett request a "Hangout" conversation with the respondent.

This email is sent from a different address - hangouts.messenger.service@gmail.com. Note however that it too was created by the attackers. The email contains a bit.ly shortened URL link that directs the target to a custom spear phishing page - hangout.com-messagecenters[.]name (this domain was registered by the attackers).

Additional targets - As in previous incidents, by investigating the attack infrastructure, we identified about 50 additional targets, out of which, three are Israeli, who we contacted and notified regarding the attack. The other targets are mostly American and Iranian individuals who work in politics, foreign relations, human rights, academia, journalism, and social activists involved in various causes.

Blow are the job description\affiliation of several of the targets we identified:



B	C	D	
name	curent country	nationality	affiliation
[redacted]	US, California	Presumably US	Assistant Professor of National Security Affairs at the Naval Postgraduate School.
[redacted]rn		Netherlands	Anti-Islamic politician
[redacted]i			[redacted]
[redacted]	USA		[redacted]
[redacted]	USA	USA	Corporate Diplomat, Professor, Speaker, Ghost Writer
[redacted]an	USA		Project Coordinator, Contractor, SelectUSA, International Trade Administration, U.S
[redacted]i	Saudi Arabia	Saudi Arabia	Academics - Middle East Center for Strategic ane Legal Studieshttps://twitter.com/c
[redacted]ete	USA		National security, foreign policy professional
[redacted]ll	USA	usa	Anti iran's regim
[redacted]	UK, London	Iranian	Interdisciplinary Tech Innovation & Environmental Sustainability Consultant | Senior
[redacted]si	Netherlands	Iran	daughter claims to be the successor of Ahmad Mola Nissi, an Arab-Iranian activist
[redacted]	USA	USA	Founder and CEO of SolomonGlobal, LLC, a business devoted to building capacity
[redacted]	Iran	iran	Iranian activist
[redacted]	USA	USA	American journalist and served as a White House press secretary for President Ba
[redacted]	USA	USA	Senior writer @CNN
[redacted]men	USA	USA	Governmental - Principal Deputy Assistant Secretary of Defense for Asian Pacific
[redacted]	Iran	Iran	Normail iranian
[redacted]	USA	USA	resident scholar at the American Enterprise Institute (AEI)
[redacted]aghari		Iran	

New Charming Kitten Infrastructure

In January we identified new domains and servers used by the Iranian threat agent Charming Kitten. This group primarily targets journalists, academic researchers and human rights activists. Charming Kitten appears to have created this infrastructure in a quick response to the recent protests. One of the fraudulent domains that we identified is a phishing page that impersonates the instant messaging app Telegram (the most popular IM app in Iran), and was likely used to steal Telegram log-in details of Iranian citizens who took part in the riots.

February

New OilRig malware

In early February we detected a new malware that impersonates an office file and used against the UAE. Based on the sample's metadata we found a direct link to two other malwares written by the Iranian OilRig group. The malware creates a VBS file, and then executes a PowerShell code that communicates with the attackers. Later, the malware establishes persistency by creating two timed tasks with the name " AdobeAcrobatLicenseVerify" and "Conhost". These tasks periodically execute the VBS file and PowerShell code.

March

Exposing a link between the Iranian groups Chafer and OilRig

In our investigations, we detected in March multiple indicators linking between Chafer and OilRig. Accordingly, it is likely that the two groups share intelligence and resources. Chafer has been active since at least July 2014 and its operations were exposed in December 2015. Chafer primarily focuses on targeted surveillance, tracking and collection of intelligence on Middle Eastern targets, including Israel. We suspect a strong link between this group and the Oilrig group. Chafer's modus operandi consists of the following outline:

1. Utilizing public and legitimate tools (open-sourced) so as to disguise malicious activity. If an attack is exposed, the public tools render it difficult to attribute the attack with any specific group.

2. Targeting the supply chain – these types of attacks are more intricate and difficult to accomplish. When successfully executed, their yield is high and they provide attackers with access to a vast pool of potential targets, namely end-user customers.

MuddyWater campaign - malicious documents targeting Middle East, USA and India

In March, we detected a number of malicious documents[236][237] linked to the MuddyWater threat agent. The group focuses on targets in the Middle East, USA and India, including governments, telecoms and oil companies. It is most likely espionage motivated. Note that this actor appears to be largely inactive in Israel, as reports signify that there have been less than five victims in the country.

The group is characterized by a repeated use of a custom PowerShell backdoor dubbed POWERSTATS. It also possesses a database of malicious files bearing the legitimate names and/or logos of various governments and institutions, which prompts victims to access spoofed macro documents. These malicious documents appear to the victims in protected view, propelling them to "Enable Content." On doing so, the malicious macro code is executed.

Please note that the use of names and insignias of government institutions does not necessarily indicate that they themselves were targeted, but only that the threat agent is abusing its victims' trust in these entities. Among the spoofed institutions were the US' NSA and Iraq's National Intelligence Service.

New CopyKittens and GreenBug attack infrastructure

In March we exposed infrastructure related to the ISMdorr malware, which belongs to the Iranian **Greenbug** threat actor, as well as indicators of the Iranian **CopyKittens** threat actor. These groups have previously targeted Israeli entities. However, it is still unclear whether the aforementioned infrastructure was used against any Israeli targets.

[236] https://twitter.com/ClearskySec/status/969245779545280514
[237] https://twitter.com/ClearskySec/status/969252946327298048

We therefore recommend verifying if these indicators appear in your monitoring system, as GreenBug infrastructure was previously involved in a highly destructive campaign against computer networks in Saudi Arabia.

April

New MuddyWater indicators embedded in spoofed National Assembly of Pakistan document

In a follow-up to the detection of the malware attributed to Iranian threat actor MuddyWater, we identified in the following weeks new indicators of a payload embedded in a malicious document that masqueraded as a report written by the National Assembly of Pakistan. The document contains macro code sections that drop a variant of this malware.

Detection of new Cadelspy Malware variant of Iranian threat group Cadelle

In April, we detected a variant of the Cadelspy malware that is attributed to Iran-based threat group Cadelle and was attached to an installation of an English-Arabic dictionary. This threat actor was first exposed by Symantec in 2015[238], however it has not been reviewed since. In the report, Cadelle was linked with Chafer, another Iran-based attack group.

The two groups used custom made Cadelspy and Remexi backdoor variants respectively in order to conduct surveillance on targets largely consisting of Iranian individuals, as well as several airlines and telecom providers across the Middle East. The groups also conducted attacks on entities in Saudi Arabia, Afghanistan and a US-based organization, among others, which were recorded from as early as July 2014 and until December 2015.

Cadelspy is initially deployed on the target host as a dropper that loads two installer components, one for Windows 32-bit and another for Windows 64-bit. The dropper then executes the appropriate installer on the system - this leads to the execution of loader and backdoor DLL files, which launch Cadelspy's malicious payload. Cadelspy is capable the following functions:

- Log keystrokes and the titles of open windows
- Gather clipboard data and system information
- Steal printer information and any documents that were sent to be printed
- Record audio
- Capture screenshots and webcam photos

Exposing Iranian threat agent MuddyWater's attack infrastructure and malicious documents

In late April, we detected two malicious documents designed to target entities in Pakistan and Turkey. We attribute these to Iranian threat group MuddyWater due to several identifying characteristics, such as attack vectors, unique OLE details and a compatibility with the Yara rules we have predetermined for this actor. Our analysis of the malicious documents exposed the use a new attack infrastructure, as well as the use of compromised servers and various URIs.

- First document - Punjab's Provincial Disaster Management Authority Impersonation
- Second document: Turkish Finance Ministry Impersonation

[238] https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

May

New MuddyWatter attack tactics and malicious document

In early May we detected a new MuddyWater attack tactic and infrastructure, as well as a new spoofed malicious document. A week prior we exposed a MuddyWater document spoofing Punjab's Provincial Disaster Management Authority in Pakistan; however the following week, we found that the aforementioned document contains malware equipped with Empire.[239]

This is an open-source post-exploitation agent for deploying malicious tools. Note that this is different to previous malicious documents we have seen from the threat actor. Namely it **is the first detected instance of Empire being used by MuddyWater.**

On April 26, 2018, a malicious document we attribute to MuddyWater was submitted to VirusTotal from Pakistan. Analysis of the document yielded URL address that are likely used as the malware's C2 infrastructure. In our assessment, the addresses are those of compromised servers that are being leveraged by the threat group.

The document impersonates Punjab's regional police. According to its OLE details, it was last saved one day before being submitted to VirusTotal – evidence to the recent nature of the attack. In addition, the document shares similar characteristics and tactics with those previously used by MuddyWater, including the following:

- **A blurry document screenshot in the background.**
- A message spoofing a Microsoft Office alert requesting users to enable the documents content – this leads to the execution of **malicious macro script**.
- An MD5 field and an "Enter" button. Upon clicking on it, a message delcaring a missing dll file, prompting victims to restart their computer to complete the process.
- A system reboot leads to the processing of data from a file called **WindowsDefenderService.ini**, which is downloaded from the malicious macro that is embedded in the word document.
- The malware ensures its persistancy on the infected host by adding a value to Autorun and a scheduled task named **Microsoft\WindowsDefenderUpdater**

New attack infrastructure of Iran-based groups - Greebug and CopyKitten

In May we detected new infrastructure used by the Iranian threat groups Greenbug and CopyKitten, as we have detected during our monitoring activity.

Malicious MuddyWater documents containing POWERSTATS malware

In May we exposed new malicious documents created by the Iranian threat group MuddyWater. Among these documents are those spoofing Iraq's Ministry of Foreign Affairs, the Iraqi General Secretariat of the Council of Ministers and Saudi Arabia's King Saud University.

One of the documents was uploaded to VirusTotal from Azerbaijan, a new target for the group. These malicious documents contain the POWERSTATS malware, a variant attributed to MuddyWater.

[239] https://github.com/EmpireProject/Empire

June

OilRig - Malicious Document Involved in Attack in Dubai

In early June we detected a malicious file that was likely used for an attack on the official media organization of Dubai's government, Dubai Media Incorporated (DMI). We have previously reported this domain as being a part of the infrastructure used by Iranian threat group OilRig, and have attached a list of indicators attributed to this actor's activity (sent on May 16, 2018). Note that in our Cyber Intelligence Report from February 4, 2018, we reviewed a malicious document from the UAE named **Invoice-NO48935.doc** that behaves in a fairly similar way to this latest document.

MuddyWater – new indicators of a Malicious Document

In early June we detected indicators for a malicious document uploaded to VirusTotal from Jordan, which is attributed to Iranian threat actor MuddyWater. The document contains a macro script that unloads a version of the POWERSTATS malware, which is attributed to the threat actor. Upon execution, we identified four queries made to C2 servers.

Detection of a New Malicious MuddyWater Document

About a week late we detected another malicious document impersonating King Saud university in Saudi Arabia. The document contains malicious macro script that unloads a variant of the POWERSTATS malware, which is attributed to the threat actor.

July

New Iranian attack infrastructure – MuddyWater, Greenbug and CopyKittens | malicious MuddyWater document

In our ongoing monitoring and investigation of Iranian threat agents, we detected new Iranian attack infrastructure attributed to the three groups. Also in July we detected a malicious document impersonating the Turkish police.

New Charming Kitten Attack Infrastructure

On July 11, 2018, the Israeli CERT issued an advisory regarding an attack that we attribute to the Iranian threat group Charming Kitten. Note that the advisory did not detail the nature of the malicious activity and included indicators that were not attributed to the threat actor.

The ClearSky cyber intelligence team analyzed the indicators provided in the advisory and detected additional infrastructure related to this attack. We estimate with moderate certainty that this activity can be attributed to Charming Kitten. Moreover, we have discovered malware that communicates with one of the addresses that is being used for C2 purposes. At this stage, the malware's infection vector is unknown. The sample was uploaded to VirusTotal from Iran.[240]

New GreenBug Infrastructure | Electric Powder – Detection of New Infrastructure Attributed to IEC Attacker

In late July we detected new infrastructure of Iranian threat actor GreenBug. Concurrently we also detected new infrastructure and malware samples attributed to a threat actor that has previously targeted the Israel Electric Corporation (IEC). We first exposed this threat campaign, which we dubbed Electric Powder, in March 2017.[241]

240 ID Key: 39cc455d
241 https://www.clearskysec.com/iec/

New Infrastructure of Russian Threat Group APT28

In late July we detected a number of samples and infrastructure attributed to APT 28 (sometimes referred to as Fancy Bear or Sofacy), a threat actor affiliated with Russia's military intelligence.

New attack infrastructure and malware of the Iranian threat agent OilRIG

In late July, a malicious email was sent to an organization located in an Arab country in the Middle East. Attached to the email was a ZIP file with a malware. The file contained the malware QUADAGENT, which we reported on in early July. While investigating an infection incident we detected a new malware, possibly a new variant of OopsIE[242].

New Greenbug and Charming Kitten Attack Infrastructure

Throughout July we identified new indicator and attack infrastructures of the Iranian threat group Greenbug by monitoring investigating network infrastructures. Additionally, on July 11, 2018, the Israeli CERT issued an advisory regarding an attack that we attribute to the Iranian threat group Charming Kitten. Note that the advisory did not detail the nature of the malicious activity and included indicators that were not attributed to the threat actor.

ClearSky's cyber intelligence team analyzed the indicators provided in the advisory and detected additional infrastructure related to this attack. We estimate with moderate certainty that this activity can be attributed to Charming Kitten. The payload is a Meterpreter variant, the bridgehead of the Metasploit exploit kit, which is packed with Veil Framework as a Pyinstaller-based executable.

Electric Powder – Detection of New Infrastructure Attributed to IEC Attacker

In July we detected new infrastructure attributed to a threat actor that has previously targeted the Israel Electric Corporation (IEC). We exposed this threat campaign, which we dubbed Electric Powder, in March 2017.[243]

New Infrastructure of Russian Threat Group APT28

In July we detected a number of samples and infrastructure attributed to APT 28 (sometimes referred to as Fancy Bear or Sofacy), a threat actor affiliated with Russia's military intelligence.

DarkHydrus - Iranian Threat Actor Weaponizes SettingContent-MS

On November 19, 2017, we reported about the renewed activity of Iranian threat actor CopyKittens. In late November we detected a malicious sample that is affiliated with that same infrastructure; possibly indicating the resurfacing of this actor. Please note that this attribution is made with moderate/low certainty. It is possible that the file belongs to a new and yet-to-be identified threat group. At this stage, we have adopted the name that Palo Alto use for the actor, DarkHydrus.

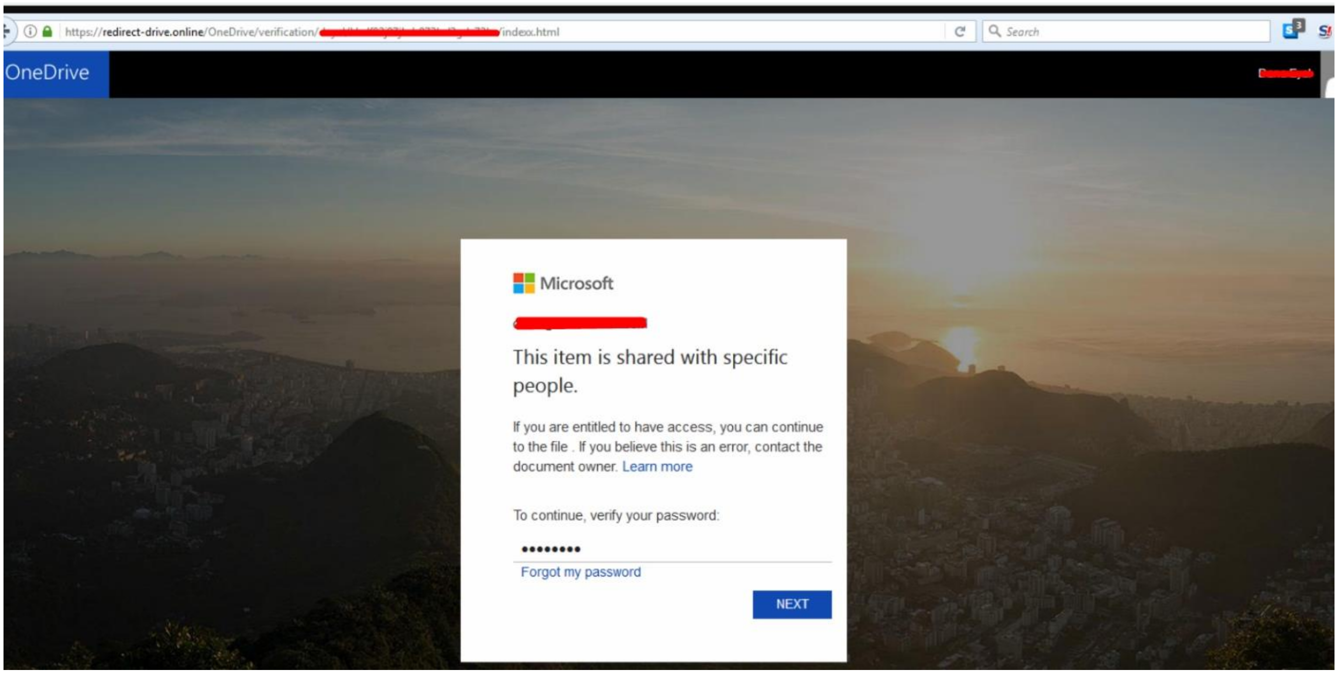
The delivery vector of the malicious file exploits the Windows 10 **SettingContent-ms** file format, which can be weaponized to bypass certain Windows defenses such as Attack Surface Reduction (ASR) and detection of OLE-embedded dangerous file formats. This attack technique was first uncovered in June this year,[244] and has since been leveraged in a wide range of attacks, embedded within PDF and Office files.[245]

Charming Kitten Spear-Phishing Campaign Targets Israeli Academics

242 https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/
243 https://www.clearskysec.com/iec/
244 https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39
245 https://www.proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-flawedammyy-rat

In late July we assisted in the management of a targeted attack that was launched against Israeli academics. The campaign was initially focused on gaining access to the computer of an Israeli researcher. Once such access was gained, the attackers leveraged the content of an email the researcher sent several weeks prior, and resent it to their chosen targets. **Therefore, the text within the email was legitimate and appeared credible.**

Within the email, the threat actor added what appears to be Microsoft One Drive link that supposedly leads to a research paper document; however, the link in fact redirected users to a phishing website.



https://redirect-drive.online/OneDrive/verification/[redacted]/index.html

OneDrive [redacted]

Microsoft

[redacted]

This item is shared with specific people.

If you are entitled to have access, you can continue to the file . If you believe this is an error, contact the document owner. Learn more

To continue, verify your password:

••••••••

Forgot my password

NEXT

Please note that the phishing webpage is tailored specifically to the targeted individual – it includes the individual's name and legitimate email address, rendering it highly very convincing.

After the target types in their password, they are redirected to a document mentioned within the email. This document is indeed hosted on OneDrive and it was likely uploaded by the attackers after it was stolen from the researcher, its author. This fact further lends to the difficulty in detecting the phishing attack, as the real document is shown as promised in the email message.

August

New attack infrastructure and malware of the Iranian threat agent OilRIG

In late July, a malicious email was sent to an organization located in an Arab country in the Middle East. Attached to the email was a ZIP file with a malware. The file contained the malware QUADAGENT, which we reported on in early July (d51c2ffce844d42bab2f2c3131e3dbd4). While investigating an infection incident we detected a new malware, possibly a new variant of OopsIE[246]. About two weeks later we detected additional attack infrastructure, partly used throughout the month against governmental bodies within the Persian Gulf.

New attack infrastructure of the Iranian threat agent CopyKittens

By monitoring characteristics of CopyKittens' attack infrastructures we detected in August additional malicious domains. By examining the historical records of IP 210.16.101.36 via Shodan, we revealed that it used to host a

[246] https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/

suspicious JavaScript. The script appears to run an unknown check when the domain is accessed, and possibly even an attempt of infecting the user. One of the hosted domains on this IP is radixxuat[.]services, which impersonates Radixx, a passenger service system provider. Note that after the script is executed the user is redirected to the Redixx genuine website.

New Iranian Group "DarkHydrus" Targeting Organizations in The Middle East Via Phishing Attacks

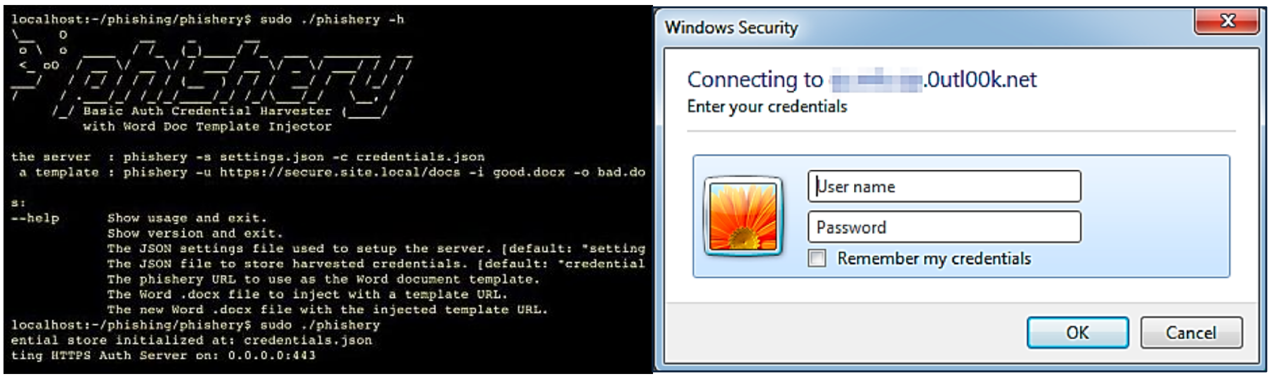
In early August, we reported on a new Iranian Threat Agent dubbed DarkHyrdus. This group executes attacks by stealing identification credentials, and targets organizations in the Middle East across multiple sectors, including governmental and education organization. According to the report, the group has been active since late 2017, with indications of attacks as recently as June 2018.

The group executes its attacks via spear-phishing emails attached with a malicious Microsoft Office documents with the name “attachedTemplate”. The file opens a Template from a remote server and requests from the user for his credentials, claiming they are needed to open the file. The credentials are exfiltrated to the attackers' remote server.

According to PaloAlto's Unit 42's analysis, it seems that the attackers used an open-sourced phishing tools by the name "Phishery" to create fraudulent Word files. This tool has two main features:

- Creating malicious Word files by remotely injecting Template URL.
- Hosting C2 servers that gathers the compromised credentials.

On June 24, 2018, Unit 42 initially reported a phishing attack on academic organizations in the Middle East. Below is a screen-captures of Phishery and the malicious dialog box that requests the log-in credentials.



```
localhost:~/phishing/phishery$ sudo ./phishery -h
      /_/ Basic Auth Credential Harvester (____/
          with Word Doc Template Injector

the server   : phishery -s settings.json -c credentials.json
 a template : phishery -u https://secure.site.local/docs -i good.docx -o bad.do

s:
--help       Show usage and exit.
             Show version and exit.
             The JSON settings file used to setup the server. [default: "setting
             The JSON file to store harvested credentials. [default: "credential
             The phishery URL to use as the Word document template.
             The Word .docx file to inject with a template URL.
             The new Word .docx file with the injected template URL.
localhost:~/phishing/phishery$ sudo ./phishery
ential store initialized at: credentials.json
ting HTTPS Auth Server on: 0.0.0.0:443
```

Windows Security

Connecting to [redacted].0utl00k.net
Enter your credentials

As seen in above, the authentication prompt says “Connecting to <redacted>. 0utl00k[.]net”, which is a DarkHydrus C2 server. Further, it is similar to the legitimate Microsoft domain outlook.com. If the user inputs his credentials, they are they sent to the C2 server hosted on: https://<redacted>.0utl00k[.]net/download/template.docx

Once the dialog box is gone, a Word file is opened. In this specific attack, the doc was empty; however, the authentication prompt may have caused the victim to enter their credentials, believing that it is needed to view the contents of the document.

PaloAlto found two additional Word documents using the 0utl00k[.]net domain to harvest credentials. These were first detected in September and November 2017. This may indicate that DarkHydrus has been executing this type of attacks close to a year.

New Infrastructure of Iranian Threat Actor OilRig

In August we detected an attack infrastructure used by Iranian threat group OilRig. Note that some of the infrastructure was leveraged in August in attacks against government entities in the Persian Gulf.

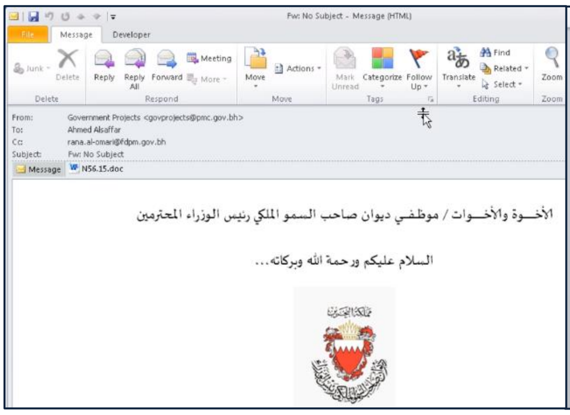
September

OilRig Attack Leverages a Compromised Government of Bahrain Email Account

On August 27, 2018, a security researcher known by the Twitter handle @blu3_team, exposed[247] a malicious Word file that unpacks a custom PowerShell malware. Taking into consideration the targets and method of operation, **we asses with high certainty that the malware was written by the Iranian threat group OilRig**. The attached Word file was uploaded to VirusTotal for examination. It was sent from the office of Bahrain's Prime Minister to communication expert working in the Deputy Primes Minister's office, with a copy to a human right activist in Bahrain.

Analysis of the email headers revealed that it lacks SPF, DKIM or DMARC details, which may indicate the credibility of the email records. In our assessment, the email was sent via the servers of the Prime Minister's office. Accordingly, it is likely that an email account associated with the office was compromised and used to propagated the malware. In our assessment, the escalation of relations between Bahrain and Iran stems, amongst other reasons, from Bahrain stripping the citizenship of the Shia politician Ayatollah Isa Qassim in June 2016[248].

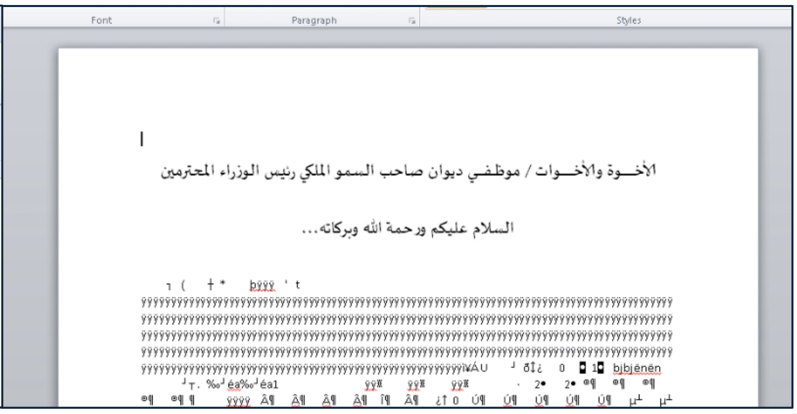
The email contains a greeting in Arabic to the employees of the Bahrain's Deputy Prime Minister Office. The text in the document was identical to that in the email, with additional characters that indicate that the file is corrupted.



From: Government Projects <govprojects@pmc.gov.bh>
To: Ahmed Alsaffar
Cc: rana.al-omari@fdpm.gov.bh
Subject: Fw: No Subject
N56.15.doc

الأخـــوة والأخـــوات / موظفـي ديوان صاحب السمو الملكي رئيس الوزراء المحترمين

السلام عليكم ورحمة الله وبركاته...



الأخـــوة والأخـــوات / موظفـي ديوان صاحب السمو الملكي رئيس الوزراء المحترمين

السلام عليكم ورحمة الله وبركاته...

ConnectWise - RDP Tool Used for Spear-Phishing Attacks on Israel

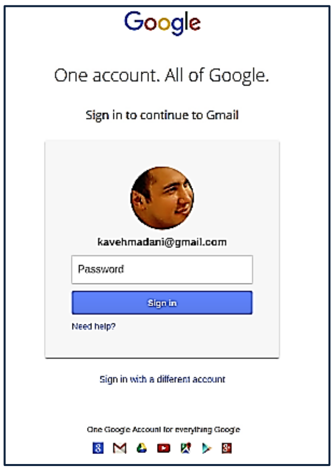
As part of our ongoing monitoring of cyberattacks on Israeli entities, we identified in September an install file of a RDP legitimate tool by the name ConnectWise, that communicates with a suspicious C2 server. In our assessment, this file was used for spear-phishing attack that was executed over recent months. The download site is walla[.]tech, which impersonates tech.walla.co.il. Note that the file was signed by an outdated digital certificate by Elsinore Technologies, who wrote the original software.

247 https://twitter.com/blu3_team/status/1034022553159979010
248 https://www.reuters.com/article/us-bahrain-shiites-iran-idUSKCN0ZC0DH
http://en.mehrnews.com/news/117517/Revocation-of-Qassim-s-citizenship-sign-of-Al-Khalifa-s-last
https://www.theguardian.com/world/2016/jun/20/bahrain-strips-influential-shia-cleric-isa-qassim-citizenship

Charming/Rocket Kitten's Spear Phishing Infrastructure

In our ongoing monitoring of Iranian threat agents, we detected an attack infrastructure containing dozens of domains and hundreds of sub-domains, that was active since 2017 up until April 2018.

Included in the infrastructure is a phishing website impersonating a Google login page[249]. This site targets Dr. Kaveh Madani; an Iranian scientist who currently serves as the Vice President of the UN Environmental Assembly. Additionally, we also identified several sites with pages impersonating Google Accounts' Two-Factor Authentication[250].


Google

One account. All of Google.

Sign in to continue to Gmail

kavehmadani@gmail.com

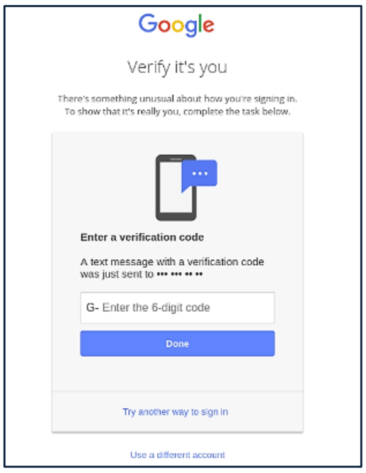
Password

Sign in

Need help?

Sign in with a different account

One Google Account for everything Google


Google

Verify it's you

There's something unusual about how you're signing in. To show that it's really you, complete the task below.

Enter a verification code

A text message with a verification code was just sent to •••• ••• •• ••

G- Enter the 6-digit code

Done

Try another way to sign in

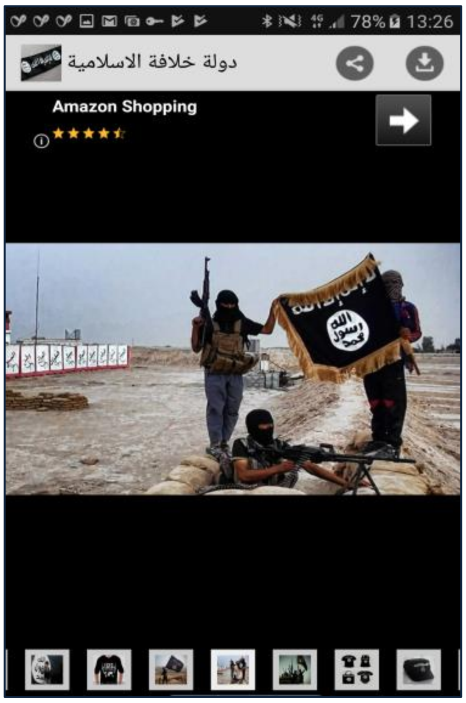
Use a different account

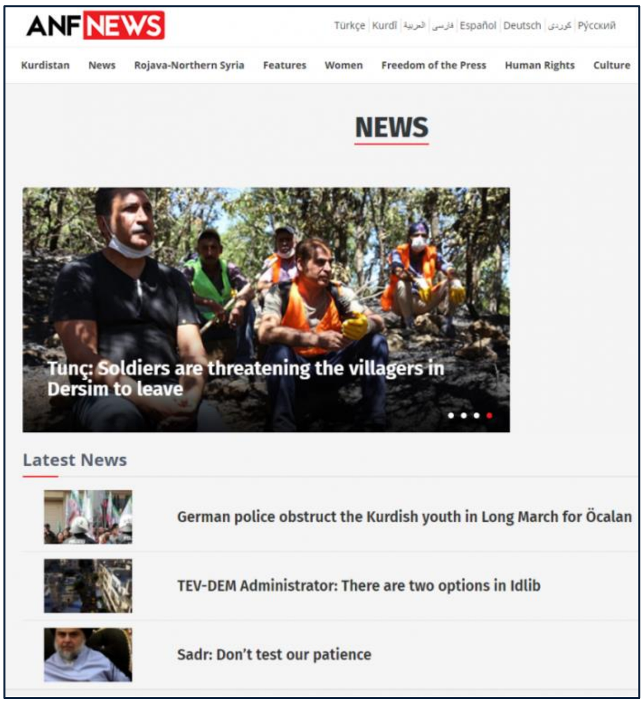
October

Iranian attack campaign Domestic Kitten and Clearsky detection of additional infrastructures

In early September CheckPoint reported[251] on an Iranian attack campaign dubbed Domestic Kitten, that spear targets pro-ISIS Iranian citizens, as well as Kurdish and Turkish ethnic Iranian citizens. Since 2016 the Iranian threat group gathered intelligence from the targets' mobile devices by using geo-political content distributed alongside the malware.

Amongst the fraudulent apps was a background app with ISIS theme, a fake app for the Kurdish news agency ANF News, and a fake version of the IM app Vidogram. Below are screen-captures from two of the apps:




ANF NEWS
Türkçe | Kurdî | العربية | فارسی | Español | Deutsch | کوردی | Русский
Kurdistan News Rojava-Northern Syria Features Women Freedom of the Press Human Rights Culture

NEWS

Tunç: Soldiers are threatening the villagers in Dersim to leave

Latest News

German police obstruct the Kurdish youth in Long March for Öcalan

TEV-DEM Administrator: There are two options in Idlib

Sadr: Don't test our patience

249 https://urlscan.io/result/40d0e42e-9a6f-460f-b06e-2cf7e8ae9a06/
250 https://urlscan.io/result/d71c9a58-9d36-4661-9258-f812ff50bf4b/
https://urlscan.io/result/1238b2e6-abc0-4c6d-a65a-65836ead7aed/
251 https://research.checkpoint.com/domestic-kitten-an-iranian-surveillance-operation/

In the investigation, several unique characteristics were identified:

- Spelling and grammar errors both in Arabic and in English.
- In certain segments of the code, the characters "~~~" were used to differentiate between the fields of the stolen data.
- In segments of the code there was a list of applications. This tells the attackers what apps are installed on the victim's device. The list includes the following terms: 'Daesh4' (ISIS4), 'Military News', 'Weapon2', 'Poetry Kurdish'.
- The attackers hosted three domains on an IP address that is attributed with them, using the following templet: tld {family name} {sir name}

In early October we detected an additional IP address that we were able to link to the infrastructure. Further we identified three URL address that we assess were/are being used by the group for their C2 servers. These indicators in addition to the other indicators are currently being monitored by us.

Detection of malicious document disguised as a meeting protocol between Mohammed Dahlan and the Egyptian Intelligence

As part of our monitoring cyber activity within the Palestinian Authority, we in October detected a PDF file disguised as a meeting protocol between Mohammed Dahlan, a Palestinian politician (and former official in Fatah), and the Egyptian Intelligence. Currently the target for the attacks is unknown.

Note that content of the document is blurred. This leads the victim to click on a link to update Adobe Reader, but in fact downloads a malicious android application. Following initial analysis of the application, we attribute the attack with intermediate certainty to APT-C-23, who is associated with Hamas.

New Iranian attack infrastructure attributed to Charming Kitten group

In October we exposed domains malicious domains hosted on a dedicated server used by Charming Kitten. Additionally we detected infrastructures and malicious documents of the group, likely intended to be used against targets in Iraq and Kuwait.[252]

New malicious documents attributed to the Iranian APT MuddyWater

Throughout September and October we identified a number of malicious documents, created by the MuddyWater group, that impersonate governmental bodies in the Middle East such as the Prime Minister of Afghanistan's office, the National IT Center of Jordan. Additionally, one of the documents impersonated a cryptocurrency startup company by the name inc 21 that develops a dongle that can turn any computer into a crypto-miner.

Over the cross of the group's operation, it has systematically created and propagated dozens of fraudulent documents with geo-political aspects regarding the Middle East, and countries that neighbor Iran in particular. **This is one of the first time that the group has distributed a document regarding cryptocurrency.** However, it seems that the group did not due an in-depth investigation on the company as in late October 2018 it changed its name to Earn.com and begun using a new logo[253].

252 https://www.hybrid-analysis.com/sample/a87c1a87d90f742614c61cf4fb15fdc400d2212fd14e96cd55bb9c1a0f09220f/5b2109b87ca3e15fa30bde03
253 https://news.bitcoin.com/21-inc-launches-lists-allowing-anyone-to-earn-bitcoin-for-microconsulting/21-4/

Regarding the group's method of operation, in three of the recently detected document we identified that the group modified the frequency of execution of the timed tasks responsible for running the malware (the tasks are named MicrosoftOfficeService or Microsoftoutlook). It was changed from once every 5 minutes to only once a day at 12:00 PM.

Large-scale campaign targeting numerous critical companies and organizations around the world

In September and October we detected and monitored a large-scale live phishing campaign that targets the employees of academic organizations and critical service and infrastructure including finance, aviation, electric, petroleum and chemicals in the U.S., UK, Germany, Singapore and UAE.

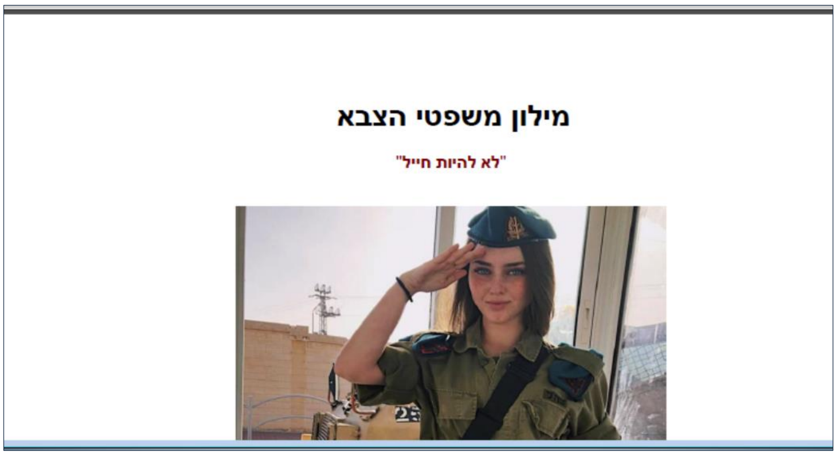
The infrastructure of the campaign was created on July 18 and is comprised of 24 domains and 120 sub-domains. It should be noted that as of writing this report, several of the domains are no longer live or have been flagged as malicious by Google. At this stage of the investigation we have not yet attributed the campaign to a specific actor.

Below is a list of companies and organizations targeted in the campaign:

Company / Organization	Country	Sector/industry
University of Brighton	UK	Academia
United Arab Emirates University	UEA	Academia
Bond Interiors	Dubai (UEA)	Interior design firm
OnTime Facilities Management	Dubai (UEA)	Consulting
Singapore Airlines	Singapore	Aviation
BASF (Baden Aniline and Soda Factory)	Germany	Chemicals
TruEnergy Australia	Australia	Power provider
Gexa Energy	USA	Power provider
Navy Federal Credit Union	USA	Finance
Fidelty	USA	Finance
Weatherford	USA	Petroleum
WOWaccess	USA	ISP
Murray Resources	USA	HR Firm
TRP International	USA	light and medium duty trailer manufacture
Black Knight Inc	USA	Mortgages and real estate
Salloum Law Firm	USA	Law firm
Ellie Mae	USA	Cloud service provider for a mortgage and financial platforms
NRC National Response Corporation	USA	commercial Oil Spill Response Organization
Elm Street Technology	USA	IT and restate marketing
Outsourcedacc	UK	Accountant outsourcing service provider

In our investigation, we identified several servers with exposed indexes, that contain targets' visit logs, emails and user agents.

New activity "Electric Powder" group attacks targets in Israel


מילון משפטי הצבא
"לא להיות חייל"

In October we detected a new activity of the group; chiefly, three samples that indicate active attacks in the last few weeks. One of them appears to target soldiers. Below is the bait file which opens when the malware is executed.

The malware is executed concurrently to the opening of the document. Upon execution it begins gathering data, as well as establishing persistency and communication with the C2 server.

November

Phishing Campaign Targeting Critical Infrastructure and Security Organizations

Jointly with security researcher known by the handle James_inthe_box[254], we detected a live Iranian phishing campaign against firms in the oil and gas, chemical, aviation and security sectors. Within this campaign, we have detected a new attack infrastructure linked to old APT33 and Charming Kitten infrastructures, who operate several tools such as Cobal Strike, Cobint, Empite, Unicorn, and NanaCore Rat.

When analyzing the infrastructure, we discovered that it overlaps with infrastructure that was published in a report by FireEye about APT33, on September 2017. For example, it seems that the domain mynetwork.ddns[.]net resolved to the address 64.251.19-214, which was used to store domains from APT33's infrastructure mentioned in the report.

Furthermore, we identified that the domain mynetwork.ddns[.]net resolved to the address 192.119.15-35. This address was used for storing domains from Charming Kitten's infrastructure that we exposed in a report on December 2017. Below is a chart illustrating the connection between Charming Kitten's infrastructure and the infrastructure in the new campaign.

New Unique Attack Campaign by Iranian Group MuddyWater

In November, we detected two samples of malicious Word files that were created by the Iranian group MuddyWater, that were **used with high probability to attack two targets in Lebanon.** The malicious documents were disguised as blurred CV documents that impel the victim to run a malicious code. As part of the research, **we detected that the group hacked two domains (one of them Israeli**). They were used to store malicious code that leads to running the second sage – a POWERSTATS malware attributed to the MuddyWater group. This was done using different TTPs properties than ones we have previously seen:

[254] https://twitter.com/James_inthe_box/status/1059087094612602881

- Attempt to conceal and prevent detection of the malware by downloading the hostile code in the second stage from hacked servers and domains. This is different from previous attacks by the group, where the backdoor code was unloaded from the macro code and was integrated in the document.
- Executing an **Excel process** from a macro segment of a Word document.
- Executing a **PowerShell command** as an Excel child process.
- When opening the document, **showing an authentic error message** worded by the attackers.
- Using VBE[255] and Javascript code to decipher the second stage.

December

New OilRig Attacks Against Companies in the UAE

In December, there were various Iranian cyber attacks in response to new sanctions by the US. The attempts were not only intelligence gathering and compromising computer systems, but also executed with the intention of causing significant damage to oil and energy companies in the Gulf area.

- Attacks on various energy companies in the Persian Gulf, including an attack on the Italian oil and gas company Saipem. The attackers used "version 3" of the Shamoon malware against computer systems in the Gulf, as well as the company's center in Scotland.
- Hacking into the UAE national oil company, and stealing information.
    - Attempts to hack into American nuclear scientists' email inboxes and computers by the Iranian group Charming kitten, who specialize in compromising email inboxes (throughout the years we detected in Israel numerous penetration attempts targeting Iranian researchers).
- Attempts to hack into computer systems of American officials involved in the decision to impose sanctions.

In our assessment, we are currently in the midst of a wave of Iranian attacks, some which are aimed at causing damage. As of now, we did not detect destructive attacks in Israel. This is likely due to the strong Israeli deterrence, rather than lack of capabilities.

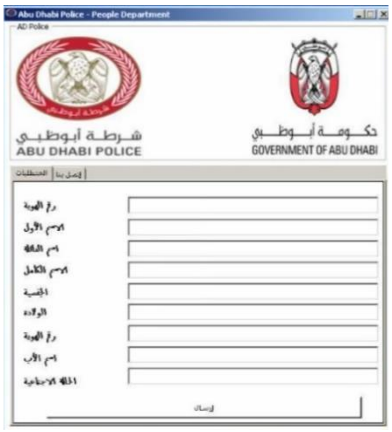
With that in mind, we cannot rule out a possible Iranians attack on companies in Israel in the future. We detected a certain improvement in Oilrig's attack vector. Notably, they use vulnerabilities **very shortly** (within hours) from when they become public, against preordained targets.

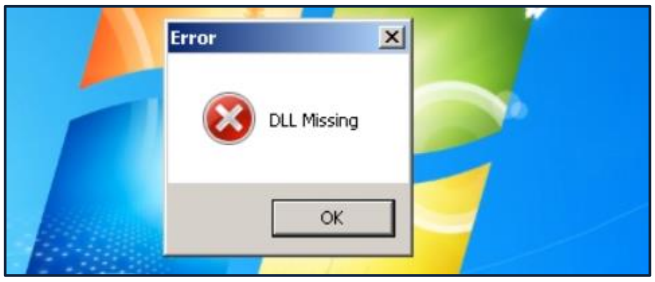
Oilrig Attacks Against Organizations in Abu Dhabi Impersonating Local Police

The attack beings by sending a malicious exe file disguised a UAE police report form that was hosted in the address: https://**adpolicer[.]org**/Download[.]aspx?DL=KLNOMKMK

[255] An encoded VBScript code segment.

The file contains a malicious component named ticket-inv-45482212.exe. When it runs, it creates a malicious PowerShell file named wuapp.ps1, which creates a scheduled task. The malware communicates with a control server we have previously reported: lowconnectivity[.]com. While running, a fake error message is shown:




Error

DLL Missing

OK

New Attack by the Iranian Group Chafer in Kuwait

In our ongoing monitoring and investigation of Iranian threat-groups, we detected in an attack in Kuwait executed by the group Chafer. The attackers attempted to obfuscated the malware by impersonating "Souq", the largest online retail company in the Arab world; a subsidiary of Amazon.

In contrast to what we've seen up until now, the malware uses an XML file that contains settings, commands and triggers. In addition, we identified that the attack vector is very similar to previous attacks by Oilrig and Chafer. The following TTPs were reused:

- Using an AutoIt3 based Backdoor which connects to the C2 server while using DNS Tunneling on TXT records. One of the methods used to do this is an Nslookup command.
- Unloading malicious and legitimate files to the routing: %AppData%\Local\Microsoft\Taskbar\
- Creating a scheduled task named "SC Scheduled Scan".
- The activity of the malware changes according to the operating system (32-bit/64-bit).

This attack is similar to the attack we reported on in the item "Oilrig's new attack methods and tools" on April 15th. Note that the attack is attributed with high certainty to Chafer[256]; however, due to the reuse of tools and infrastructure, it may be an attack by Oilrig[257].

APT28 Attacks and Infrastructure Targeting Israel

In late December, in cooperation with fellow researchers, we detected a malicious malware sample used against an unknown entity in Israel. We are attributing the sample with high certainty to the Russian group APT28; attributed to the Russian military's Main Intelligence Directorate (GRU). We are also currently conducting research on the group's infrastructure and tools.

We collected all the known infrastructures of the group, and we are trying to locate more infrastructure and give attribution to the tools they use. Indicators from previous events, alongside infrastructure that we detected are attached to the report. Below is an example of one of the incidents that we detected in December. A malicious email was sent to an unknown individual in Macedonia. The email contained a document "UDS 2019 Current Agenda.doc" – an invitation to a conference about underwater protection that contained a malicious macro code.

[256] https://www.vkremez.com/2018/03/investigating-iranian-threat-group.html
[257] https://www.nyotron.com/wp-content/uploads/2018/03/Nyotron-OilRig-Malware-Report-March-2018C.pdf

Cyber Events in Israel 2018

Below is a review of the most significant events that took place or were exposed this

Hamas Attack - Impersonating "Red Alert" App, Cellcom TV and News Websites

Fraudulent website hosting a malicious "Red Alert" mobile app

During our regular monitoring of attack infrastructures and campaigns launched against Israeli entities, we detected a new, recently created attack infrastructure. This infrastructure includes a website impersonating a website for a "Red Alert" mobile application, which is designed to alert users in Israel about air raid sirens in real time.

The fraudulent website impersonated the original application's website, and appears nearly identical. However, the fraudulent site contains a download link for the malicious, fake application, which is based on the original one but contains a dropper payload that enables attackers to drop additional malware onto the victim's device.

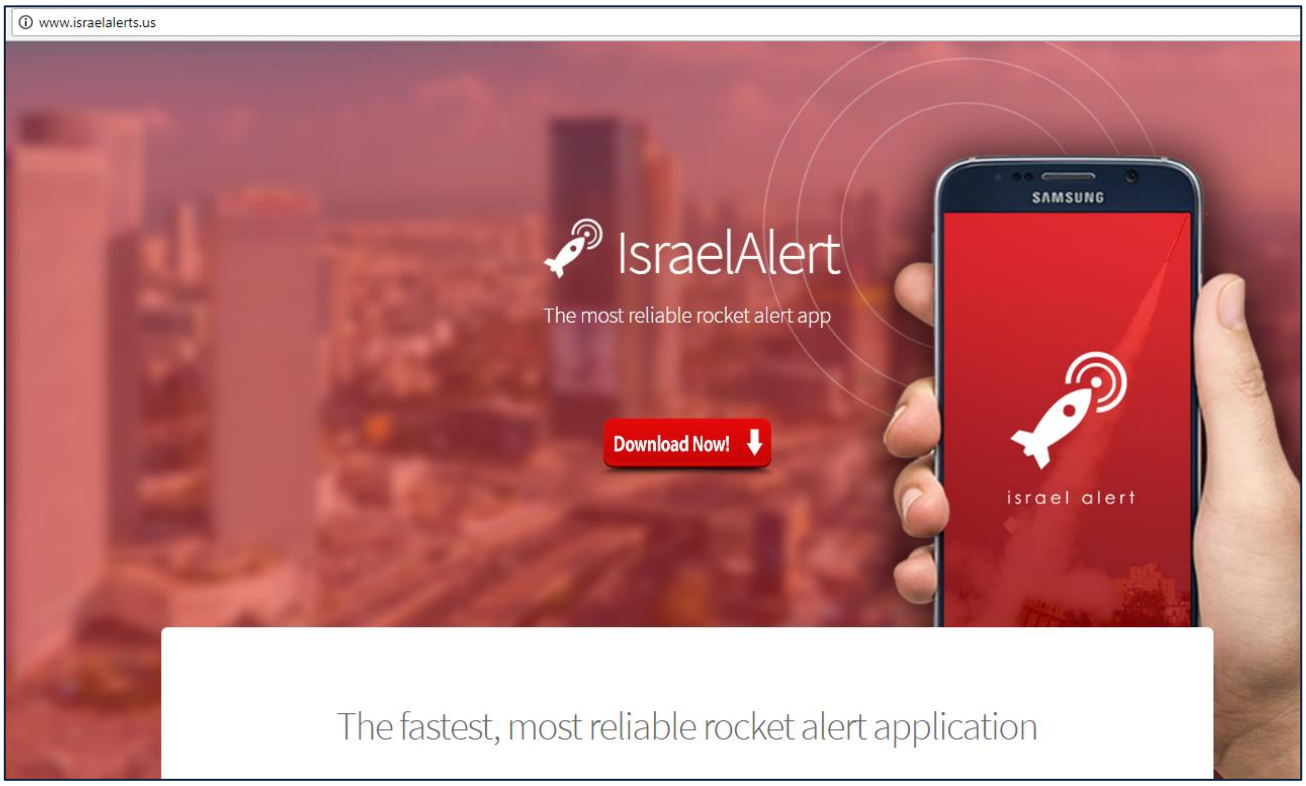
The discovery of this infrastructure was the result of long term research, together with our security research partners, of attack infrastructures used in campaigns against Israel. This recent infrastructure is linked with the attack on the Israel Electric Company (Operation Electric Powder) in 2017, which we reviewed in our blog at https://www.clearskysec.com/iec/. Based on our examining of the shared infrastructure of these two campaigns, we assess with a moderate to high certainty that this attack can be attributed to Hamas.

The fake "Red Alert" application directs users to download an application called Israel Alert App-release.apk, which has been flagged as malicious by a large number of antivirus vendors in the VirusTotal database. Both the application's characteristics and the infrastructure's IOCs were reported to Google and the major antivirus vendors.

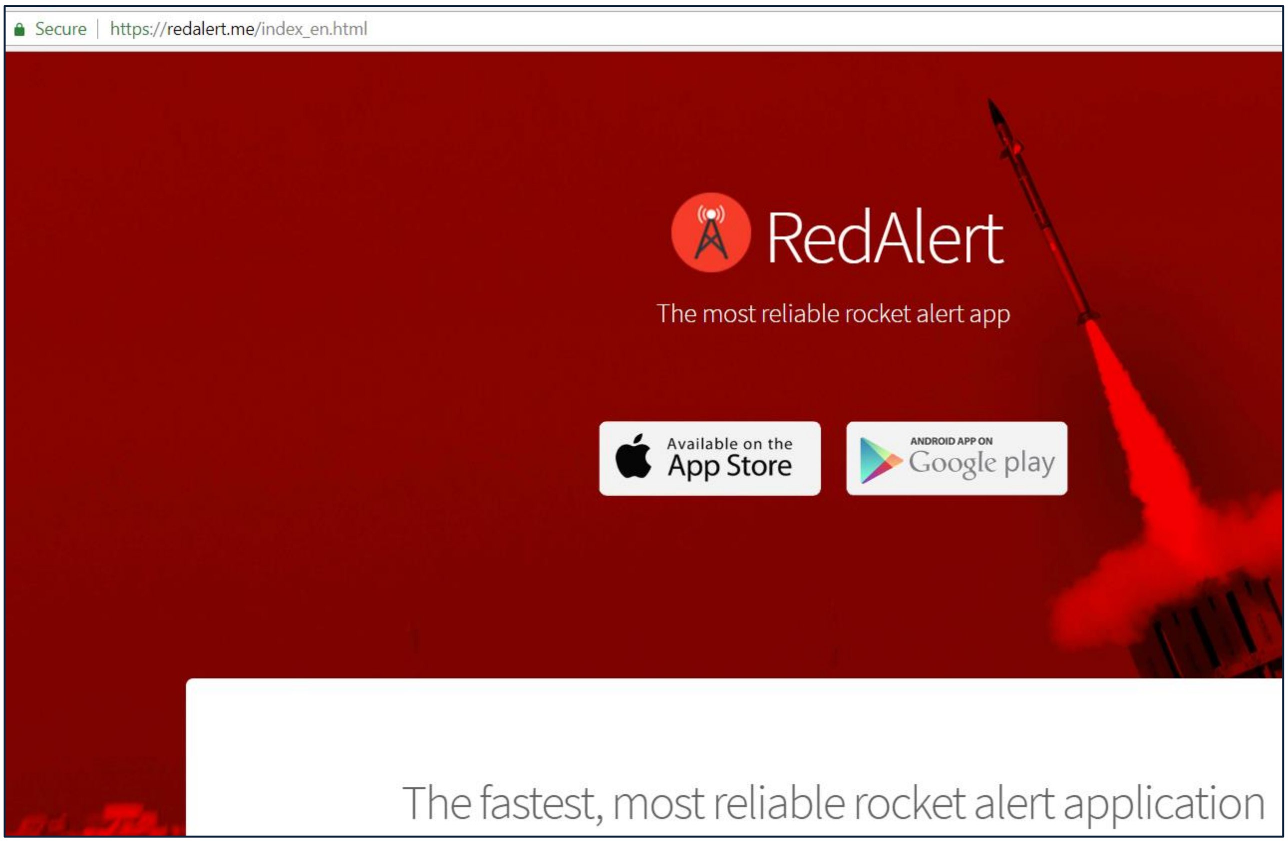
In our assessment, the discovery of the infrastructure shortly after its creation prevented the attackers from executing a widespread infection among Israelis. We believe the attackers intended to lure Israeli social media users to download the application, as in the case of Operation Electric Powder.

An additional unverified attack vector is compromising Israeli websites and directing users to the application, or inserting ads that redirect users to the applications on legitimate websites. Note that this attack campaign appears credible to the lay mobile application user and therefore it had a high infection potential.

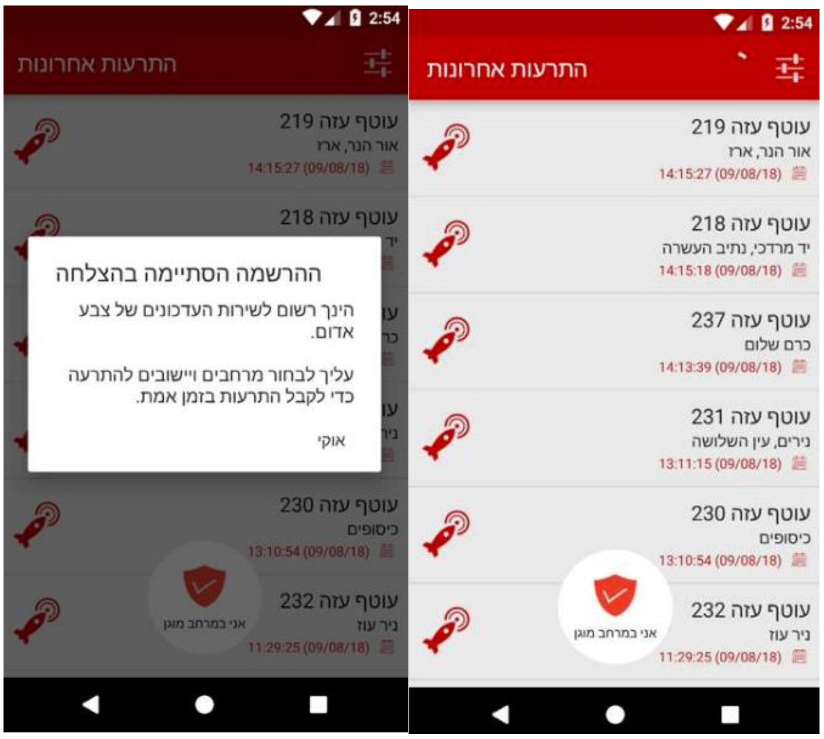
Below is a screen-capture of the malicious website


www.israelalerts.us
IsraelAlert
The most reliable rocket alert app
Download Now!
SAMSUNG
israel alert
The fastest, most reliable rocket alert application

Below is a screen-capture of the legitimate website


Secure
https://redalert.me/index_en.html
RedAlert
The most reliable rocket alert app
Available on the App Store
ANDROID APP ON Google play
The fastest, most reliable rocket alert application

Below is a screen-capture of the fake app



2:54

התרעות אחרונות

ההרשמה הסתיימה בהצלחה

הינך רשום לשירות העדכונים של צבע אדום.

עליך לבחור מרחבים ויישובים להתרעה כדי לקבל התרעות בזמן אמת.

אוקי

עוטף עזה 219
אור הנר, ארז
14:15:27 (09/08/18)

עוטף עזה 218
יד מרדכי, נתיב העשרה
14:15:18 (09/08/18)

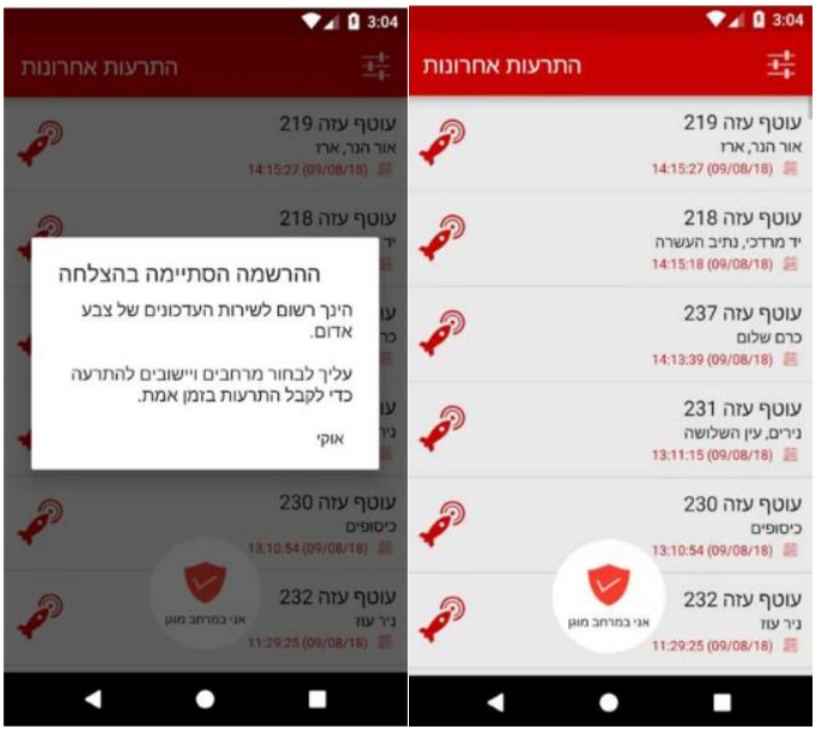
עוטף עזה 237
כרם שלום
14:13:39 (09/08/18)

עוטף עזה 231
נירים, עין השלושה
13:11:15 (09/08/18)

עוטף עזה 230
כיסופים
13:10:54 (09/08/18)

עוטף עזה 232
ניר עוז
11:29:25 (09/08/18)

Below is a screen-capture of the legitimate app. Note that they are visually identical.



3:04

התרעות אחרונות

ההרשמה הסתיימה בהצלחה

הינך רשום לשירות העדכונים של צבע אדום.

עליך לבחור מרחבים ויישובים להתרעה כדי לקבל התרעות בזמן אמת.

אוקי

עוטף עזה 219
אור הנר, ארז
14:15:27 (09/08/18)

עוטף עזה 218
יד מרדכי, נתיב העשרה
14:15:18 (09/08/18)

עוטף עזה 237
כרם שלום
14:13:39 (09/08/18)

עוטף עזה 231
נירים, עין השלושה
13:11:15 (09/08/18)

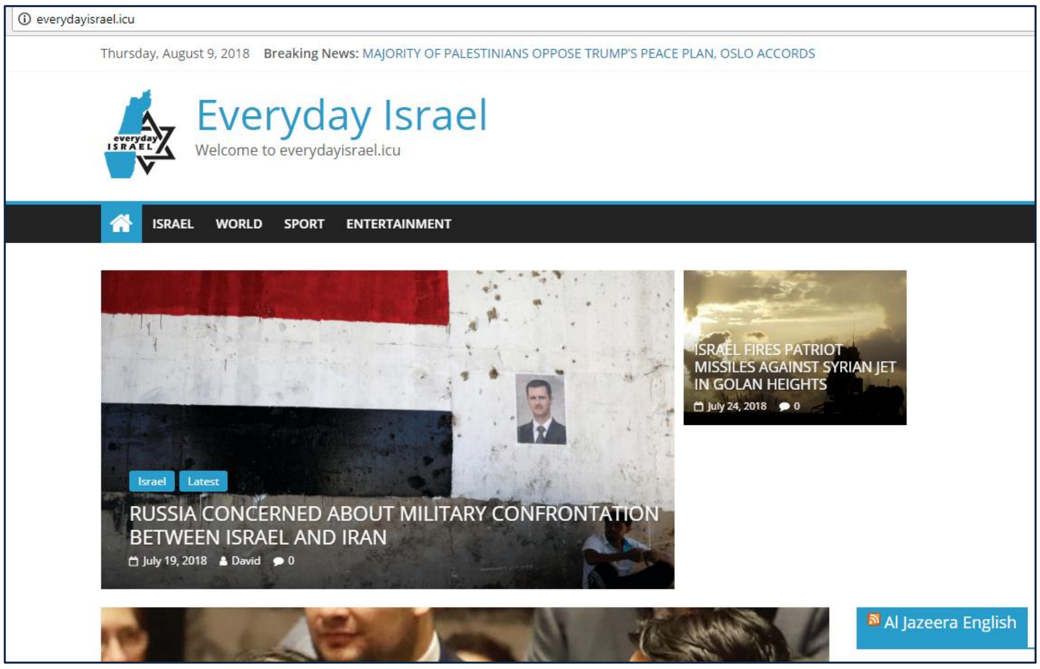
עוטף עזה 230
כיסופים
13:10:54 (09/08/18)

עוטף עזה 232
ניר עוז
11:29:25 (09/08/18)

Both the malicious app and the fake website are hosted on the same server, alongside additional file and photos used to create the fraudulent content.

Fraudulent news website propagate malware and disinformation

In our investigation, we identified that hosted on the same infrastructure is a supposed news website by the name "Everyday Israel". Our current assessment is that it was created to disseminate fake new, and/or as a malicious phishing site to infect visitors; i.e. watering hole attack. As of writing this report, the site's content is directly taken from Al Jazeera official website.



everydayisrael.icu

Thursday, August 9, 2018 Breaking News: MAJORITY OF PALESTINIANS OPPOSE TRUMP'S PEACE PLAN, OSLO ACCORDS

Everyday Israel
Welcome to everydayisrael.icu

ISRAEL WORLD SPORT ENTERTAINMENT

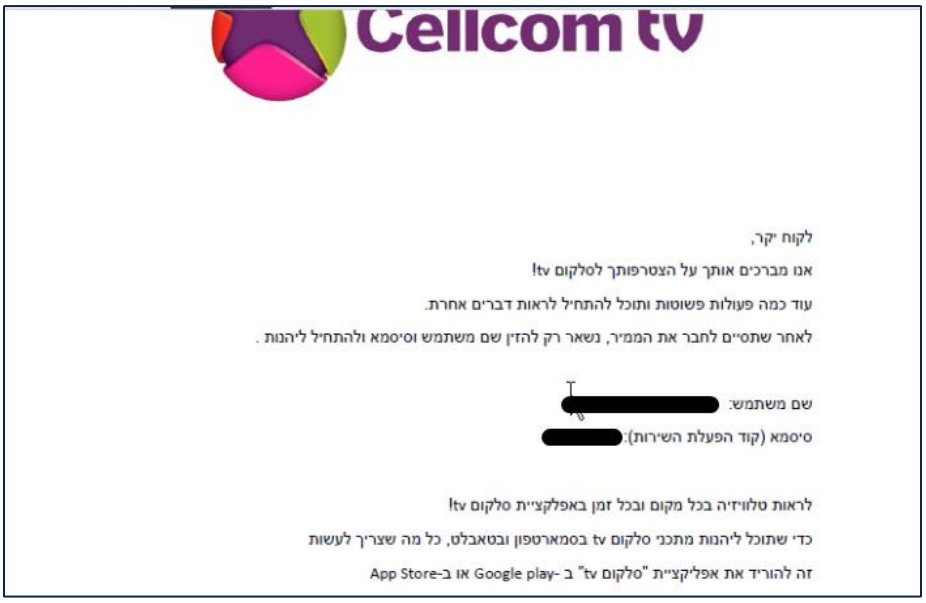
Israel Latest
RUSSIA CONCERNED ABOUT MILITARY CONFRONTATION BETWEEN ISRAEL AND IRAN
July 19, 2018 David 0

ISRAEL FIRES PATRIOT MISSILES AGAINST SYRIAN JET IN GOLAN HEIGHTS
July 24, 2018 0

Al Jazeera English

Phishing Attack Impersonating Cellcom TV to Propagate Malware

As part of their attack campaign, the attackers used an executable file by the name - "username and password cellcom tv Israel Ltd .exe" When executed this file opens a fake Cellcom TV document congratulating users for "joining" their service.



Cellcom tv

לקוח יקר,

אנו מברכים אותך על הצטרפותך לסלקום tv!

עוד כמה פעולות פשוטות ותוכל להתחיל לראות דברים אחרת.

לאחר שתסיים לחבר את הממיר, נשאר רק להזין שם משתמש וסיסמא ולהתחיל ליהנות .

שם משתמש: [redacted]

סיסמא (קוד הפעלת השירות): [redacted]

לראות טלוויזיה בכל מקום ובכל זמן באפלקציית סלקום tv!

כדי שתוכל ליהנות מתכני סלקום tv בסמארטפון ובטאבלט, כל מה שצריך לעשות

זה להוריד את אפליקציית "סלקום tv" ב -Google play או ב-App Store

Concurrently a backdoor that runs in the background and gathers data on the compromised station's IP address and OS.

Further, the backdoor creates a text file with the name - domains.txt - that contains two URL addresses. The first is used for a C2 server. The purpose of the second address is currently unclear, as the sample did not request it. Nevertheless, it is highly likely used in some capacity by attack campaign. Note, the infrastructure was created in July, however the malware was created in August.

OpIsrael – Continued Failure of Anti-Israeli Hacktivism

2018's OpIsrael was characterized by a low-level of activity and did not produce any major results as opposed to those seen in previous years. In recent years the campaign has significantly lost momentum since it was launched in 2013. This year's campaign was led by four dominant actors, compared to the over ten major players seen in 2017. Most of these actors had previously operated under one group.

We estimate the operation's failure stemmed from the following reasons

- The existence of strong Israeli deterrence in the cybersphere has influenced and will continue to influence the number of participants in these campaigns, as well as their capabilities and willingness to confront Israeli entities in a cyber environment.
- Social media and text storage websites, most notably Twitter, Facebook and Pastebin, have carried out concentrated efforts to "clean" and remove the accounts of attackers and their supporters. The websites also removed posts and publications related to attacks or leaked private data.
- High levels of data security among Israeli firms and organizations along with thorough preparation for the campaign. Additionally, Israel's CERT implemented certain measures that reduced the campaign's public promotion, while encouraging the sharing of information and insight on the campaign on its Cybernet network.
- A decreased interest in the Palestinian cause in the Arab world, resulting in less promotional activity and media coverage that traditionally induces hacktivist activity. The recent Gaza border protests did not garner a sufficient reaction from hacktivist groups around the world. Consequently, only a **small number** of capable hackers (four) participated; reducing the potential volume of damage.
- The evening before April 7, Iran's web infrastructures were attacked and significantly damaged due to a vulnerability in Cisco router-switches. The result was that the majority of Iranian groups had turned their focus towards this incident and did not concentrate their efforts on the campaign against Israel. (The actors involved in the attack on Iran had left American flags and a slogan reading "don't mess with our elections," on the impacted hosts).
- Other recent regional events, such as the summit between the presidents of Russia, Iran and Turkey, the visit of Saudi Arabia's crown prince to the US and his pro-Israel statements, as well as the Egyptian presidential election, had reduced the interest levels of regional threat actors in the campaign.
- Even while in its preparation stage, 2018's campaign had received a decreased level of interest from international hacktivist groups. Only several hundred individuals, some using fictitious accounts, expressed interest in the main OpIsrael Facebook event, which Indonesian threat actor MinionGhost created. **The latter had ultimately not participated in the campaign itself.** In addition, there had been a marked decrease in OpIsrael-related activity in other social media platforms – no designated Telegram channel was created, while darknet and Facebook activity remained minimal. Note that three days before the operation, MinionGhost's Twitter account was blocked, which may explain the group's absence during the campaign.
- The campaign began four days before its official scheduled date, on April 3, when dozens of Israeli municipality websites were defaced, including those of Netanya, Herzliya and Acre. In addition, the websites of several Israeli hospitals and organizations were also targeted and defaced

- Several hours later, the attackers leaked thousands of Israeli email addresses; in some cases, telephone numbers and other personal information was included. During the days that followed, several other small websites were defaced.
- Towards the end of the campaign, an Israeli actor attempted to carry out a counter-campaign, dubbed OpIslam. This campaign was less extensive than similar counter-campaigns seen in previous years. As part of OpIslam, the actors leaked the access credentials for several Arab-language websites took down sever used by a key OpIsrael actor.

Operational insight

Raising awareness of existing vulnerabilities in the hosting services of websites, storage sites and website builders - the majority of defacements in this campaign were carried out through attacks on hosting services, such as those provided by Daronet Internet Solutions and Interdeal Inc. Most Israeli ISPs allow clients to rent virtual servers for hosting various services and applications - a small number of these servers were hacked during the campaign. As a result, hundreds of websites hosted on the servers were defaced – over 400, according to the attackers (these virtual servers were not fully protected by the providers).

Penetration of virtual servers endangers all websites hosted by the same ISP. Therefore, we recommend verifying that all hosting services or website builders offer full website protection. Moreover, we advise the enforcement of security regulations among hosting service providers, similar to the recent new regulations issued for financial institutions and the IT security supply chain.

Verifying the security of small and medium-size companies - the majority of OpIsrael's victims involved small to medium-size businesses in possession of large amounts of customer data. These companies have little to no defense and security infrastructure; any attack targeting them may expose their customers. In 2017, the most significant cyber threat consisted of attacks on supply chains. Therefore, we recommend verifying the existence of at least a basic security infrastructure prior to carrying out transactions with such small and medium-size providers.

Data leaks involving employees - we recommended drafting a standard procedure to be followed in case any employee information is leaked online. These guidelines should include a standard notification procedure and a prompt change of the exposed information. Furthermore, the employee must be instructed on how to prevent a reoccurrence.

Intelligence Insight

Preventing OpIsrael actors from posting on social media reduces their motivation to act - the campaign is first and foremost a propaganda operation used by participants to promote and glorify themselves and their abilities. In the months leading to the campaign, the Facebook and Twitter accounts of threat actors were increasingly being removed.

As a result, MinionGhost, as well as several Arab groups that participated in OpIsrael 2017, such as FallagaTeam and GatorLeagur, were prevented from spreading their potential "achievements" during the campaign. We estimate that this has proved a significant deterrent and subsequently prevented the groups from participating in the operation.

Events with international interest utilized for incitement - despite a series of highly-covered events relating to the Israeli-Palestinian conflict, pro-Palestinian hacktivists have largely failed to garner a significant response from the international hacktivist community. One exception was the death of Palestinian journalist Yasser Murtaja in the April 7 clashes in Gaza, after which dozens of hacktivist groups joined the campaign's Facebook and IRC groups. In addition, the coverage of the funeral resulted in increased activity from actors in Saudi Arabia and Morocco, who were not previously active in the campaign.

It is also worth noting that US President Donald Trump's recognition of Jerusalem as Israel's capital led to a large-scale "flash" campaign against Israel. This leads us to conclude that these operations are increasingly organized only after specific internationally-circulated events, and are not solely a reaction to an internal conflict.

Theft of Sensitive Data from NSO Group by Disgruntled Employee

On July 2018, a former NSO employee was indicted with attempting to sell proprietary and sensitive data. Following a hearing before dismissal, the employee used his credentials as lead programmer to steal the firm's products' source code, valued at hundreds of millions of dollars. Afterwards, he attempted to sell them the data on the darknet for $50 million worth of cryptocurrencies. The ex-employee worked at NSO for a year and a half, developing automation solutions for the company's products and doing QA, and had access to sensitive systems and data.

NSO Technologies Group provides various solutions and services for mobile platforms, notably extracting data for security and defense operations. The firm develops tools and software that enable her, according to its license in Israel, to extract any information necessary to prevent a terror act, and keep protect national interests. NSO has around 500 employees and has a market value of about $1 Billion dollars.

Its main product is a spy-software named "Pegasus", which is used by law enforcement agencies to take full control of mobile devices. Pegasus enables users to records calls, view photos and SMS and monitor devices' online activity. This is done by exploiting various OS vulnerabilities, including 0-days (i.e. previously unknown or reported vulnerabilities). The software, which works both on Android and iOS, is highly covert and leaves no traces. In 2017, it was reported that the Mexican government used Pegasus to spy on members of its position.

The company's computer was installed with anti-leak software, named Mcafee DLP, that prevents the use of any external storage on the systems. On February 2017, three months after he began working at NSO he searched online on how to disable this software. On April 29th, 2018, he was called for hearing before dismissal. As an act of revenge, he disabled the software, and stole various proprietary tools and products source codes. **Note that the company did not detect the breach, despite being alerted by McaFee.**

After obtaining the data he attempted to sell in on the Darknet, however one of the potential buyers contacted NSO's CEO and alerted him on the matter. The company then engineered a plan to apprehend the seller, who was later revealed as the employee. According to NSO, no real damage was caused and the stolen data was not compromised.

Additional incidents of data theft by employees in Israel

This is not the first time such an attempt took place in Israel. For example, in September of 2017, Lior Shar'avi was indicted with attempted extortion of several companies and Bank Yahav, threatening to expose sensitive databases of client information, unless he receives 1 million NIS in Bitcoin. Shar'avi worked as a technical support manager for Activetrail, a company that provides mailing services for numerous organizations in Israel, including banks, insurance companies and governmental offices. As part of his job, he had access to sensitive information such as usernames, passwords, and ID keys of Activetrail's clients.

After his employment with the company was ended, he used his remote access credentials and accessed the company's systems and stole the database. This was possible as the Activetrail did not disable Shar'avi's user or changed their systems' authorization keys.

Another previous event of note is the attempted extortion of Leumi Card by Eliran Rosnes in 2014, who stole Leumi Card's database with 2 million credit card details, by copying a hard drive. Following a joint international law enforcement operation, Rosnes was arrested in Thailand and was later sentenced to 11 years in prison.

Insight from employee data theft events

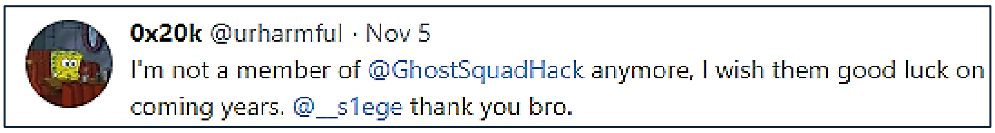
- It is ineffective to install an anti-leak system if it is does not alert in real time. Moreover, the effectiveness of such a system or of it does, is significantly hindered if there is no one to respond to the alert in real time.
- Real-time and continuous monitoring and alerting of any anomalous activity on the organizational network can prevented most data breach from employees. This should be done in concurrence to hardening the company's outer shell security framework.
- In all of the above cases, the employees had knowledge of how to copy data; however, they failed in their extortion attempts, as their actions were impulsive. Furthermore, they operated with no real understanding of the Darknet, in regard to both obfuscating their identity, and pulling off such a sale of proprietary data.
- It is advised to implement a policy of "least privilege" – i.e. segmenting departments, and limiting authorizations for sensitive systems to only those who require access for their ongoing work.
- Promptly disabling and removing authorizations to any employee as soon as his employment has ended.

FICORA Botnet - DDOS Tool Exploits Apache Hadoop Vulnerabilities; Used Also in Israel

On October 25th, 2018, Radware posted an article[258] about a new bot called DemonBot, which attacks Hadoop database-installed servers. In relation to this, the hacker 0x20k (aka URHARMFUL from the attack group Ghost Squad Hackers[259]) published an attack tool against servers using Apache Hadoop called **FICORA Botnet[260]**. FICORA is designed to perform DDOS attacks while exploiting zero-day vulnerabilities on the Apache Hadoop[261] system (A tool package based on open source code designed to enable Big Data processing).

Ghost Squad Hackers is an activist hacker group responsible for attacks on central banks, security organizations and communications in **Israel** and the rest of world, since 2016. The group was responsible for leaking information from Israeli government websites and the US military, hacking the President of Afghanistan's twitter account, attacking Fox News, CNN, and even ISIS, amongst others.

The group was active in the OpIsrael campaign in 2016. The group cooperated with anonymous and together they leaked an IDF database with sensitive information about soldiers and the air force. In an article on SecurityAffairs, it is mentioned that 0x20k is part of the group, although on his twitter account he states that he does not work with them anymore[262].


0x20k @urharmful · Nov 5
I'm not a member of @GhostSquadHack anymore, I wish them good luck on coming years. @__s1ege thank you bro.

According to the hacker 0x20k, DemonBot does not deserve the credit it receives. The author of the DemonBot malware took the original code from one of the authors of the Owari malware and stole the code from their servers before they posted the code online. Therefore, 0x20k decided to release his code to the world. Moreover, in his YouTube account, he posted videos showing how he operates the tool[263]. Both of the malwares function differently. For example, DemonBot communicates with port 6982, 22 or 32 (SSH/TELNET), depending on the availability and

[258] https://blog.radware.com/security/2018/10/new-demonbot-discovered/
[259] https://en.wikipedia.org/wiki/Ghost_Squad_Hackers
[260] https://securityaffairs.co/wordpress/77565/malware/hadoop-zero-day-exploit-leaked.html
[261] https://en.wikipedia.org/wiki/Apache_Hadoop
[262] https://twitter.com/urharmful/status/1059423035600515072
263 https://www.youtube.com/watch?v=QoEsrPDcBO4

versions of python or PERL on the attacked severs, while FICORA runs on port 8088. Another difference between them is the type of attack. DemonBot executes a TCP/UDP denial of service attack, while FICORA uses URG Flood.

Researchers define the script not as a bug that enables executing a code remotely, but as a script that enables running tasks remotely. Also, there is a contradiction between what the attacker claims and what the firm claims. The Hadoop developers claim that the malicious code is not a zero-day vulnerability, but an attack that creates tasks on Hadoop servers which are not secured and exposed to the world.

Clearsky's Findings

In late September, we scanned a compressed folder on VirusTotal. The folder contained two files containing code written in C which lead to the infection of network components or Huawei routers. Next to the code files there is a text file where 0x20k takes responsibility for writing the code:

We analyzed the code and conclude that there is a mechanism for sending a POST request to the network component or Huawei router, which leads to downloading a malicious code from the domain botnet[.]ficora[.]net. We assess that it is a malicious firmware update or a file disguised as firmware update. Downloading the malicious code from the server is done by sending a POST request to the network component with the routing /ctrlt/DeviceUpgrade_1, under the Realm[264]: "HuaweiHomeGateway."

Israeli Organization Infected by RETADUP via USB Flash Drive

On March 11, 2018, the Israeli CERT issued an alert[265] regarding a threat campaign against Israeli organizations, which appears to be related to a previous attack on Israeli hospitals in late June 2017[266]. The current campaign consists of a RETADUP infection, which leverages AutoIT and AutoHotKey (operating system automation tools) to run malicious code. The attack vector was most likely carried out via an infected USB flash drive that was connected to a work station.

According to our estimations, **this re-infection with RETADUP was done unwittingly,** possibly via a connection of a portable device that was involved last year's campaign. This event may also prove to be a targeted attack against Israeli organizations, as the C2 servers in this incident have a certain affiliation with Palestinian entities.

Date	Event
29/06/2017	CERT issues an alert[267] concerning an attack targeting the Israeli health sector, which leverages the AutoIT automation tool.
	Trend Micro publishes a report[268] on a threat targeting Israeli hospitals via propagation of the RETADUP worm, through exploitation of AutoIT. This is likely the same event as the aforementioned attack.
30/06/2017	Kaspersky publishes a report[269] on malware that leverages AutoIT as part of a phishing campaign against Israeli targets on Facebook.
17/07/2017	Trend Micro publishes a report[270] on Android malware known as GhostCtrl, which spread in the Israeli health sector during the campaign in June 2017.
20/09/2017	Trend Micro publishes a report[271] on new variants of RETADUP that spread in Latin America in May 2017.
11-13/03/2018	CERT issues an alert[272] on a threat campaign against Israeli organizations, which is related to the June 2017 attack on Israeli hospitals. In this event, a Facebook-affiliated domain was used as a C2 server.

264 A parameter that defines secured areas with a password on a server as part of authentication processes such as WWW-Authentication. https://tools.ietf.org/html/rfc7235#section-2.2
265 https://www.gov.il/he/Departments/publications/reports/autoit2
266 https://www.gov.il/he/Departments/publications/reports/hospital_guidelines
267 https://www.gov.il/he/Departments/publications/reports/hospital_guidelines
268 https://blog.trendmicro.com/trendlabs-security-intelligence/information-stealer-found-hitting-israeli-hospitals/
269 https://securelist.com/facebook-malware-tag-me-if-you-can/75237/
270 https://blog.trendmicro.com/trendlabs-security-intelligence/android-backdoor-ghostctrl-can-silently-record-your-audio-video-and-more/
271 https://blog.trendmicro.com/trendlabs-security-intelligence/new-retadup-variants-hit-south-america-turn-cryptocurrency-mining/
272 https://www.gov.il/he/Departments/publications/reports/autoit2

Analysis of the dropped files yielded that the AutoHotKey-based malware is highly similar to the AutoIt-based variant. It also mostly shares similar functions as the RETADUP worm, which is executed with an AutoIT script. The malware is uploaded with WMI.

As part of its functions, it first checks for a CPUChecker process in the infected end station. If such a process is detected, the malware removes itself; this may be due to the existence of a certain security tool or perhaps the presence of a different tool the actor has deployed on the station.

Upon researching the process, we have discovered a mining tool known as CPUChecker. We estimate that RETADUP is used by the threat actor to deploy this cryptomining tool, similar to the Monero mining tool spread by the malware in South American countries.

RETADUP source

RETADUP's unique code shares many similarities with a malware variant known as ROWMANTI, which has the same functionalities and spreading capability as RETADUP. ROWMANTI began spreading in 2015; its source is embedded in the code of a worm known as IPPEDO, which began spreading in 2014. IPPEDO is known in darknet web forums as "RAD Worm," and is controlled by a Visual Basic Script based Remote Access Trojan (RAT) called DUNIHI.

In 2015, ROWMANTI's C2 server contained the string "RAD," this fact strengthens the connection between the latter and RETADUP. While analyzing the Whois details of the C2 server, which were provided by CERT, we discovered that most of the domains are registered under "RAD," and all had the same Palestinian telephone number and email account details.

This email address is associated with a Facebook account. A search of the account's profile picture yielded a Twitter account, @MuAmAl00957883, which is most likely Palestinian. The account was created in August 2017 and its tweets consist of romantic lyrics.

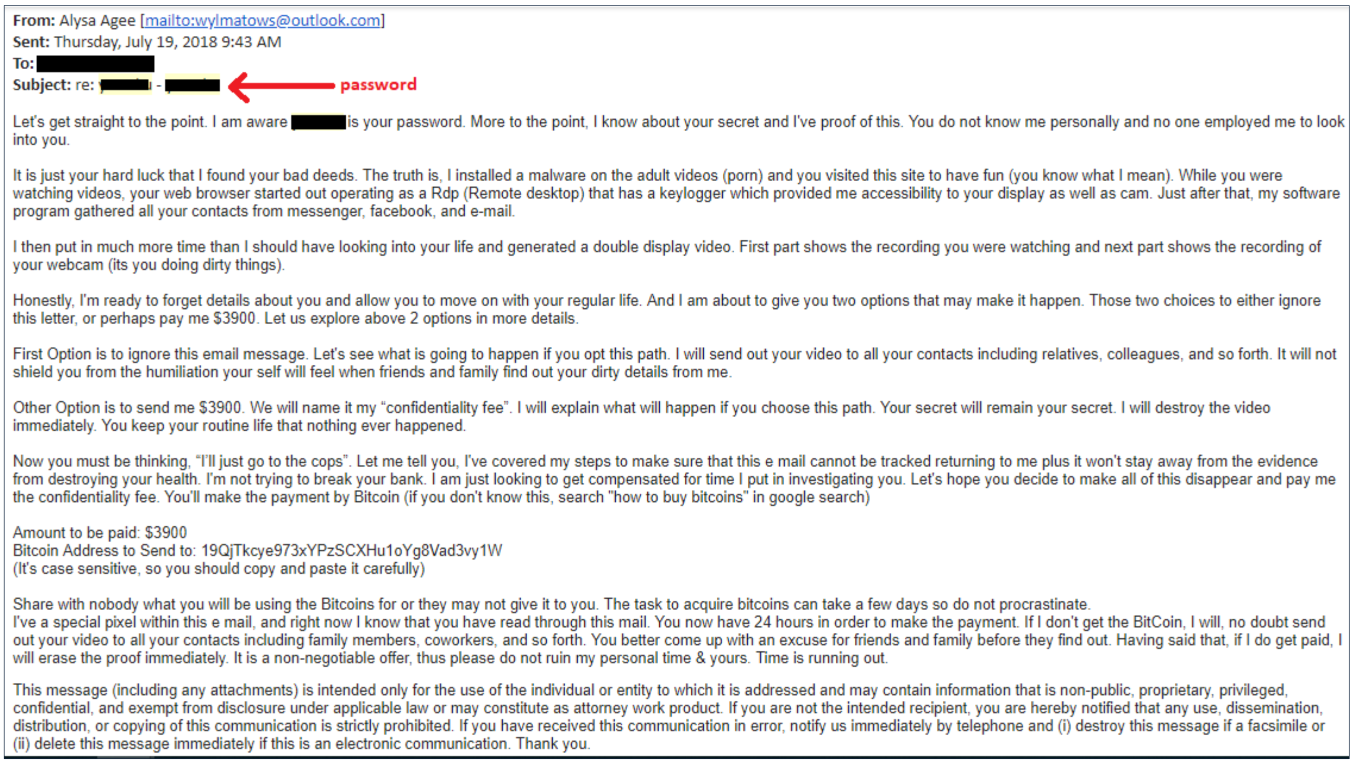
Upon checking the Whois details of the C2 at palestineop[.]com, the domain appeared to be protected by confidentiality services. Nevertheless, in December 2016, the domain was registered under the name **Ramy Hajjeh from Hebron,** who is affiliated with the number +972.599758613 and the email address eng.ramy.h@hotmail.com. One of the seven domains registered under these same details is aljazzerra\.com, a website impersonating Arabic Al-Jazeera and is currently offline. We attribute this domain to the attack infrastructure on the Israeli hospitals in June 2017.

In late March, we detected several files related to the propagation of RETADUP in the recent campaign targeting Israel, as well as related to recent incidents involving IPPEDO, DUNIHI, ROWMANTI and RETADUP.

Sextortion Attempts Targeting Employees of Israeli Companies

In July, we received multiple requests for assistance from organizations and companies whose employees had been targeted with an attempted extortion. The extortionist in question sent the employees emails demanding money in exchange for not distributing personal and compromising sexual footage of the employee. The footage and data was supposedly collected from the victims' computer.

The content of these messages appears to be a fraudulent attempt to extort Bitcoin from victims. Below we have detailed an example of such an email sent to an employee at an Israeli company. The subject of the email consists of a password supposedly stolen from the recipient.


From: Alysa Agee [mailto:wylmatows@outlook.com]
Sent: Thursday, July 19, 2018 9:43 AM
To: [redacted]
Subject: re: [redacted] - [redacted] ← password

Let's get straight to the point. I am aware [redacted] is your password. More to the point, I know about your secret and I've proof of this. You do not know me personally and no one employed me to look into you.

It is just your hard luck that I found your bad deeds. The truth is, I installed a malware on the adult videos (porn) and you visited this site to have fun (you know what I mean). While you were watching videos, your web browser started out operating as a Rdp (Remote desktop) that has a keylogger which provided me accessibility to your display as well as cam. Just after that, my software program gathered all your contacts from messenger, facebook, and e-mail.

I then put in much more time than I should have looking into your life and generated a double display video. First part shows the recording you were watching and next part shows the recording of your webcam (its you doing dirty things).

Honestly, I'm ready to forget details about you and allow you to move on with your regular life. And I am about to give you two options that may make it happen. Those two choices to either ignore this letter, or perhaps pay me $3900. Let us explore above 2 options in more details.

First Option is to ignore this email message. Let's see what is going to happen if you opt this path. I will send out your video to all your contacts including relatives, colleagues, and so forth. It will not shield you from the humiliation your self will feel when friends and family find out your dirty details from me.

Other Option is to send me $3900. We will name it my "confidentiality fee". I will explain what will happen if you choose this path. Your secret will remain your secret. I will destroy the video immediately. You keep your routine life that nothing ever happened.

Now you must be thinking, "I'll just go to the cops". Let me tell you, I've covered my steps to make sure that this e mail cannot be tracked returning to me plus it won't stay away from the evidence from destroying your health. I'm not trying to break your bank. I am just looking to get compensated for time I put in investigating you. Let's hope you decide to make all of this disappear and pay me the confidentiality fee. You'll make the payment by Bitcoin (if you don't know this, search "how to buy bitcoins" in google search)

Amount to be paid: $3900
Bitcoin Address to Send to: 19QjTkcye973xYPzSCXHu1oYg8Vad3vy1W
(It's case sensitive, so you should copy and paste it carefully)

Share with nobody what you will be using the Bitcoins for or they may not give it to you. The task to acquire bitcoins can take a few days so do not procrastinate.
I've a special pixel within this e mail, and right now I know that you have read through this mail. You now have 24 hours in order to make the payment. If I don't get the BitCoin, I will, no doubt send out your video to all your contacts including family members, coworkers, and so forth. You better come up with an excuse for friends and family before they find out. Having said that, if I do get paid, I will erase the proof immediately. It is a non-negotiable offer, thus please do not ruin my personal time & yours. Time is running out.

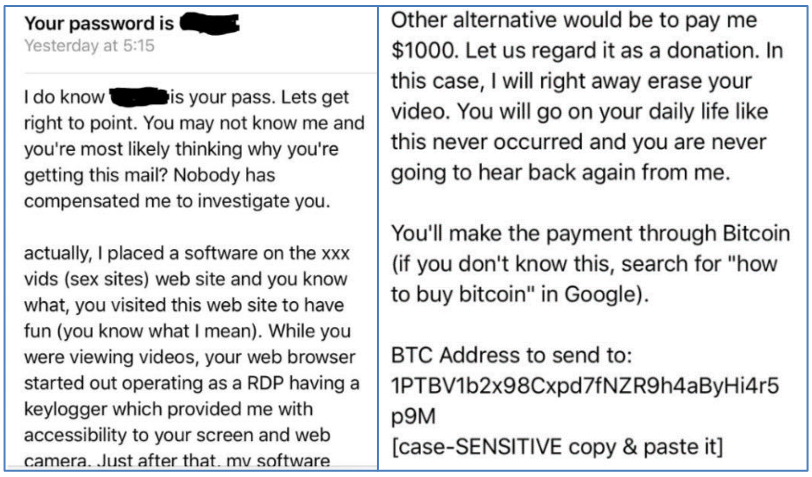
This message (including any attachments) is intended only for the use of the individual or entity to which it is addressed and may contain information that is non-public, proprietary, privileged, confidential, and exempt from disclosure under applicable law or may constitute as attorney work product. If you are not the intended recipient, you are hereby notified that any use, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, notify us immediately by telephone and (i) destroy this message if a facsimile or (ii) delete this message immediately if this is an electronic communication. Thank you.

In October, we received additional requests from companies targeted by another wave of attacks claiming that they have sex photos and videos allegedly obtained from employees' computers. The content of the messages is almost identical to the extortion messages from July, with a minor change to the account details and one of the phrasings.

It should be noted that the massage notes a **personal password** that allegedly belongs to the targets. This is done do add credibility to the extortion attempt, however the password appears to come from various database leaks, including from porn websites. Below are screen-captures of the email:

This is a phishing campaign that is not backed by any real information. These types of emails are almost always fraudulent and are used to extorted cryptocoins from targets. Accordingly, there is no reason to respond to these emails or comply to their requests.

Nevertheless, it is advised for the employees who received the email to change their passwords on any website or system they have access to. If you received such as an email, please notify us so we may further investigation this campaign.


Your password is [redacted]
Yesterday at 5:15

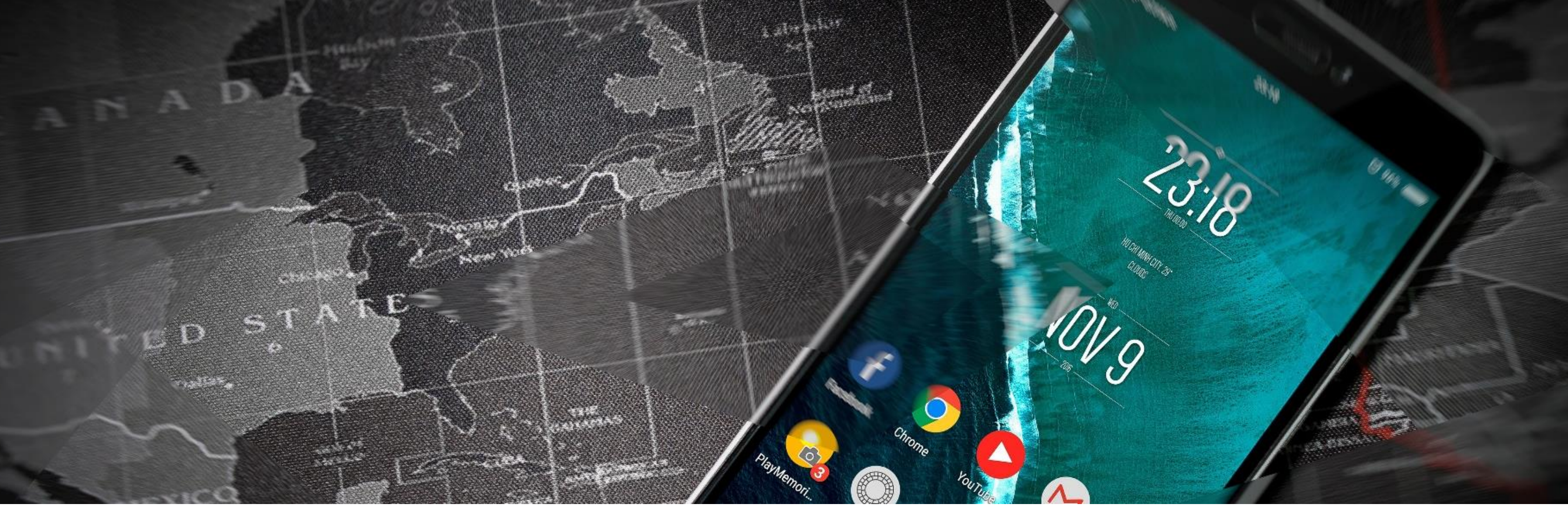
I do know [redacted] is your pass. Lets get right to point. You may not know me and you're most likely thinking why you're getting this mail? Nobody has compensated me to investigate you.

actually, I placed a software on the xxx vids (sex sites) web site and you know what, you visited this web site to have fun (you know what I mean). While you were viewing videos, your web browser started out operating as a RDP having a keylogger which provided me with accessibility to your screen and web camera. Just after that, my software

Other alternative would be to pay me $1000. Let us regard it as a donation. In this case, I will right away erase your video. You will go on your daily life like this never occurred and you are never going to hear back again from me.

You'll make the payment through Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address to send to:
1PTBV1b2x98Cxpd7fNZR9h4aByHi4r5p9M
[case-SENSITIVE copy & paste it]



Timeline – Events and Attacks in 2018

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
January				
Texas police department	USA	Ransomware	Law enforcement	Due to the attack, the department lost 8 years of video evidence [273]
Malaysian organ donors	Malesia	Data leak	Government - healthcare	Personal records of 220,000 Malaysian organ donors and next of kin leaked online [274]
Metrolinx - Ontario transit agency	Canda	Malware	Local government - Transportation	The agency claims that the attacker was from North Korea [275]
City of Farmington	USA	Ransomware - SamSam	Government	The city chose not to pay the ransom of 3 bitcoins (about $35,000 at the time). They restored the systems from un-affected backups [276]
Bell Canada	Canda	Data breach	Telecommunication	100K clients' identifying (but no financial) info was compromised.This is the second breach [277] within 8 months. In the previous breach, 1.9M clients were affected [278]
Turkish Defense Contractors	Turkey	Espionage campaign – Spear phishing and malware	Government and Defense	The campaign likely began in November 2017. [279] Used Remcos RAT espionage malware[280]
National Stores, Inc.	USA	Hacking and PoS malware	Retail	The event took place between July 16 and December 11, 2017, however was only detected in late December and reported in late January [281]
Harris County	USA	Phishing - BEC	Government	Close to a 1 million was stolen, but was later retrieved [282]
Coincheck	Japan - Global	Hacking and Data breach	Financial	534 million in crypto coins was stolen [283]
Several major Dutch banks (including ABN Amro and ING); Dutch tax authority	The Netherlands	DDoS	Financial	The attacks disrupted operation [284]

273 https://www.csoonline.com/article/3163045/security/ransomware-steals-8-years-of-data-from-texas-police-department.html
274 https://www.lowyat.net/2018/153125/personal-details-220000-malaysian-organ-donors-next-kin-leaked-online/
275 https://www.cbc.ca/news/canada/toronto/north-korean-cyber-attack-metrolinx-1.4500918
276 https://eu.daily-times.com/story/news/local/farmington/2018/01/18/farmington-recovering-after-ransomware-attack/1044845001/
277 https://www.theglobeandmail.com/report-on-business/police-probing-bell-canada-data-breach-up-to-100000-customers-affected/article37701579/
278 https://www.theglobeandmail.com/report-on-business/bell-apologizes-to-customers-after-data-breach-hits-19-million-e-mail-addresses/article35004027/
279 https://www.infosecurity-magazine.com/news/espionage-campaign-turkish/
280 https://secrary.com/ReversingMalware/RemcosRAT/
281 https://www.securityweek.com/clothing-retailer-fallas-hit-payment-card-breach
282 https://www.houstonchronicle.com/news/houston-texas/houston/article/Harris-County-looks-to-boost-cyber-security-after-12524738.php
283 https://cointelegraph.com/news/story-of-coincheck-how-to-rebound-after-the-biggest-theft-in-the-history-of-the-world
284 https://www.dutchnews.nl/news/2018/01/renewed-cyber-attacks-on-dutch-banks-abn-amro-ing-at-weekend/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Multiple companies in the Middle East	Multiple countries in the Middle East	Attack via the supply chain	Critical sectors	Executed by Iranian group Chafer
Hancock Regional Hospital	USA	Ransomware	Healthcare	The hospital paid a ransom of $55,000 [285]
BlackWallet	Global	DNS Hijacking	Financial	$400K in Lumen coins was stolen[286]
Numerous shipping companies around the world	Global	Phishing - BEC	Maritime	The campaign was executed by Gold Galleon[287]
February				
Pyeongchang Winter Olympics	South Korea	Hacking and malware - Attack via the supply chain	Sports and IT	Several systems were disrupted or taken down. Later it was discovered that the main IT provider was hacked several months prior [288]
City of Allentown, Pennsylvania	USA	Ransomware	Municipal	Emotet trojan. Recovery efforts were estimated at $1 million
Applebee's	USA	PoS malware	Fast food	Over 160 branches were affected
Jemison Internal Medicine	USA	Ransomware	Healthcare	Affected a database of over 6,500 patients [289].
BitGrail	Global	Hacking	Financial	Between $170 and $190 in cryptocoins were stolen[290]
Github	N/A	DDoS	Website	Amplified ddos attack - 1.3TB attack via vulnerable Memcached servers[291]
Mobistealth and Spy Master Pro	USA	Data breach	Spy software developers	A hacker hacked both companies and stole hundreds of sensitive data[292]
Punjab National Bank (PNB)	India	Data breach	Financial	10,000 clients' credit card were compromised[293]
Children's Aid Society of Oxford County Family and Children's Services of Lanark, Leeds and Grenville	Canada	Ransomware	NGO	Both organizations were infected but reportedly only one paid 5K to unlock its systems[294]
Inland Revenue Department	New Zealand	Phishing and ransomware	Government	The attack took place in November 2017 but was only reported on February 2018 [295]
City of Pittsburgh, Kansas	USA	Phishing	Government	W-2 tax forms were compromised[296]
Wallace Community College Selma	USA	Phishing	Academia	W-2 tax forms were compromised[297]
The Travel Corporation (TTC)	USA	Phishing	Tourism	W-2 tax forms and SSNs were compromised[298]
TerraSond	USA	Phishing	Geo-mapping	W-2 tax forms were compromised .[299]
City of Batavia, Illinois	USA	Phishing	Government	W-2 tax forms were compromised[300]
Waldo County, Maine	USA	Phishing	Government	W-2 tax forms were compromised[301]
City of Keokuk , Iowa	USA	Phishing	Government	W-2 tax forms were compromised[302]
The Los Angeles Philharmonic	USA	Phishing	Entertainment	W-2 tax forms were compromised[303]

285 https://www.healthcare-informatics.com/news-item/cybersecurity/hancock-health-hit-ransomware-attack-pays-55k-recover-data
286 https://bitcoinmagazine.com/articles/blackwallet-hacked-warns-stellar-community-not-log-site/
287 https://threatpost.com/gold-galleon-hacking-group-plunders-shipping-industry/131203/
288 https://www.cyberscoop.com/atos-olympics-hack-olympic-destroyer-malware-peyongchang/
289 https://www.databreaches.net/jemison-internal-medicine-discloses-ransomware-event/
290 https://bitcoinist.com/bitgrail-cryptocurrency-exchange-hacked-170-million-nano-allegedly-stolen/
291 https://techcrunch.com/2018/03/02/the-worlds-largest-ddos-attack-took-github-offline-for-less-than-tens-minutes/
292 https://motherboard.vice.com/en_us/article/7x77ex/hacker-strikes-stalkerware-companies-stealing-alleged-texts-and-gps-locations-of-customers
293 https://www.databreaches.net/punjab-national-bank-data-breach-10000-credit-and-debit-cards-and-associated-details-affected-report/
294 https://www.thestar.com/news/insight/2018/02/22/ransomware-attacks-hit-two-ontario-childrens-aid-societies.html
295 https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/
296 https://www.databreaches.net/pittsburgh-employees-notified-after-their-w-2-data-stolen-in-phishing-scheme/
297 https://www.selmatimesjournal.com/2018/02/24/cyber-criminals-target-wallace-employees/
298 https://dojmt.gov/wp-content/uploads/TravelCorp.pdf
299 https://dojmt.gov/wp-content/uploads/TerraSond.pdf
300 http://kanecountyconnects.com/2018/02/alert-batavia-employees-w-2-forms-compromised-irs-warns-of-major-w-2-phishing/
301 https://www.scmagazine.com/home/security-news/cybercrime/waldo-county-maine-phishing-attack-results-in-data-breach/
302 https://www.scmagazine.com/home/security-news/phishing/phishing-scam-exposes-w-2-forms-of-keokuk-iowa-employees-and-officials/
303 https://abc7.com/la-phil-employees-w-2-info-stolen-in-cyberattack/3125933/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Kinetics Systems, Inc.	USA	Phishing	Process and mechanical contractor	W-2 tax forms were compromised .[304]
Aperio Group	USA	Phishing	Financial	Sensitive employee data as well as system credentials was stolen [305]
Tesla	USA	Cryptomining	Automobile	The company's servers were hacked and infected with Cryptomining malware [306]
Tim Hortons	Canada	Malware	Fast food	Over 1,000 branches were affected[307]
Italian Democratic Party (PD)	Italy	Data breach	Government	AnonPlus hacked the party's systems, stole and leaked info about the former prime minister Matteo Renzi[308]
Province of Milan	Italy	SQL injection	Government	AnonPlus hacked the province's systems[309]
Swisscom	Switzerland	Data breach	Telecommunication	The company claims it was not hacked and that the event was due to human error[310].
German government agencies	Germany	Spear attack	Government	Executed by Russian group APT28[311]
Nova Poshta	Ukraine	Data breach	Shipping	Largest shipping company in the country. Half a million customers' data leaked on the darknet[312]
		March		
UK government and military contractor	UK	Attack via the supply chain	Government and military	Executed by Chinese group APT15 [313]
US engineering and defense companies	USA	Espionage and attack campaign	Engineering and defence	Executed by Chinese group TEMP.Periscope[314] - targeted companies linked to the South China Sea dispute
US and European critical infrastructures	US and several European countries	Ongoing attack campaign	Government and critical infrastructures	Russian APT Energetic Bear[315], aka Dragonfly [316]
Queensland Transport Department	Australia	Attack via the supply chain	Government	The department systems were hacked and leveraged to attack additional departments[317]
MBM - Limogés Jewelr	USA/Canada	Data breach - S3 Bucket misconfiguration	Jewellery	1.3 million people's data compromised [318]
Scottsboro City Schools	USA	Phishing	Education	W-2 tax forms were compromised [319]
Boeing	USA	Malware	Aviation	Affected one of the company's plants
Applebee	USA	PoS Malware	Fast food	160 branches were affected [320]
Colorado Department of Transportation (CDOT)	USA	Ransomware	Government	Attacked twice within days by SamSam[321]
Binance	China	Hacking	Financial	Hackers sold users coins despite having 2fa [322]

304 https://www.doj.nh.gov/consumer/security-breaches/documents/kinetics-systems-20180207.pdf
305 https://www.databreaches.net/aperio-group-client-account-data-breached-by-successful-phishing-attack/
306 https://www.coindesk.com/tesla-public-cloud-was-briefly-hijacked-by-crypto-miners
307 https://securityaffairs.co/wordpress/69718/data-breach/tim-hortons-canada-malware.html
308 http://www.ansa.it/english/news/politics/2018/02/06/florence-pd-hacked-renzi-data-published-2_e65dc016-237d-482b-80d6-0072e65ee307.html
309 https://www.huffingtonpost.it/2018/02/06/larghe-intese-anti-hacker-anonplus-attacca-il-sito-del-pd-firenze-online-il-cellulare-di-renzi-che-incassa-la-solidarieta-m5s_a_23354307/
310 https://www.zdnet.com/article/swisscom-data-breach-800000-customers-affected/
311 http://www.dpa-international.com/topic/cyberattacks-brought-control-says-german-interior-ministry-180228-99-282593
312 https://www.databreaches.net/personal-data-of-500000-nova-poshta-clients-allegedly-leaked-to-dark-web/
313 https://threatpost.com/china-linked-apt15-used-myriad-of-new-tools-to-hack-uk-government-contractor/130376/
314 https://www.bloomberg.com/news/articles/2018-03-16/china-hackers-hit-u-s-firms-linked-to-sea-dispute-fireeye-says
315 https://www.us-cert.gov/ncas/alerts/TA18-074A
316 https://www.theregister.co.uk/2018/03/15/dhs_fbi_blame_russian_government_for_dragonfly_attack_on_infrastructure/
317 https://www.abc.net.au/news/2018-03-14/hackers-breach-queensland-department-of-transport-security/9544218
318 https://mackeepersecurity.com/post/walmart-jewelry-partner-exposed-millions-customer-details
319 https://localtvwhnt.files.wordpress.com/2018/03/20180305125630793.pdf
320 http://securityaffairs.co/wordpress/69877/data-breach/applebee-payment-card-breach.html
321 https://securityaffairs.co/wordpress/69946/cyber-crime/cdot-second-ransomware-attack.html
322 https://www.zdnet.com/article/binance-cryptocurrency-sell-off-disaster-blamed-on-mass-phishing-campaign/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Russian Defense Ministry	Russia	DDoS	Government and Defence	The attacks took place during the general elections.[323]
Italian Ministry of Education	Italy	Data breach	Government and education	Data of 26,000 teachers was compromised by Lulzsec Italia [324]
Maersk - Svitzer	Australia	Data breach	Maritime Shipping	For almost a year 3 employees' email accounts auto-forward all emails to an external and unauthorized email address [325]
Frost Bank	USA	Data breach	Financial	The attack affected 140 corporate clients [326]
Under Armour – MyFitnessPal app	USA	Data breach	Clothing	150 million customers' records were compromised [327]
Puerto Rico's Power Utility, PREPA	Puerto Rico	Data breach	Energy	The company claims no customer data was compromised[328]
Bank Negara - Malaysia's Central Bank	Malaysia	SWIFT breach	Financial	The bank thwarted a SWIFT attack[329]
UK Anti-Doping Agency	UK	Hacking	Government	Attempted attack by Russian group APT28[330]
City of Atlanta	USA	Ransomware	Municipal	SamSam Malware. Recovery efforts are estimated at $17 million [331]
Turkish financial sector	Turkey	Malware	Financial	Executed by North Korean group Hidden Cobra[332]
April				
MyEtherWallet	Global	DNS Hijacking	Financial	$150,000 in Ethereum coins was stolen[333]
BMW	Global	Vulnerability	transportation	14 vulnerabilities in car computer components were identified that may enable attackers with control of various car systems [334].
Great Western Railway	UK	Data breach	Transportation	About 1,000 passengers' details were compromised
Inogen	USA	Data breach	Healthcare	Records of 30,000 customers of the medical supplier may have been compromised
Multiple healthcare providers	USA, Europe, Asia	Data breach	Healthcare	Attack campaign executed by Orangeworm group
Multiple pipeline companies	USA	Hacking	Infrastructure	At least four gas networks were hit by a cyber attack. Unknown if customer data was compromised[335]
Sint Maarten	Sint Maarten	N/A	Government	A cyber attack with unknown vector took down the country's IT infrastructure
India's Ministry of Defense	India	Defacement	Government	The official website was hacked and defaced
"Operation Power-Off" - webstresser	Global	Law enforcement operation	Website - DDoS-as-a-service	International law enforcement takedown dubbed "Operation Power Off"[336]
H-E Parts International	USA	Data breach	Mining equipment	The company was attacked by TheDarkOverlord who claimed that it obtained access to all of the company's databases[337]

323 https://travelwirenews.com/massive-ddos-attack-on-russias-defense-ministry-website-during-vote-on-new-arms-names-780197/
324 https://medium.com/@arturodicorinto/anonymous-has-hacked-and-put-into-the-net-26-thousand-email-addresses-of-italian-teachers-b94e679d2743
325 https://www.abc.net.au/news/2018-03-15/sensitive-data-stolen-from-global-shipping-company-svitzer/9552600?section=technology
326 https://www.ksat.com/news/sa-based-frost-bank-investigating-breach-contacting-affected-customers
327 https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/
328 https://www.darkreading.com/attacks-breaches/puerto-ricos-electric-utility-hacked-in-weekend-attack/d/d-id/1331328
329 https://www.bankinfosecurity.com/malaysias-central-bank-blocks-attempted-swift-fraud-a-10758
330 https://ukad.org.uk/news/article/uk-anti-doping-statement-on-cyber-attack
331 https://www.beckershospitalreview.com/cybersecurity/atlanta-s-ransomware-attack-may-cost-the-city-17m.html
332 https://www.bankinfosecurity.com/bankshot-trojan-targets-turkish-financial-sector-a-10707
333 https://www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum
334 https://thehackernews.com/2018/05/bmw-smart-car-hacking.html
335 https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts
336 https://krebsonsecurity.com/2018/04/ddos-for-hire-service-webstresser-dismantled/
337 https://www.databreaches.net/h-e-parts-morgan-hacked-thedarkoverlord/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Trusted Quid	UK	Data breach	Financial	The company's website was breached for over 6 months exposing data of 66K clients[338]
Unnamed online casino and additional targets	Unnamed country in Central America	Wiper malware	Gambling	North Korean group Lazarus; used KillDisk malware[339]
Japan Ministry Employees	Japan	Data breach	Government	Thousands of ministries email addresses and passwords leaked and sold online[340]
[24]7.ai	USA	Attack via the supply chain	Various sectors	The company, that provides AI based services was hacked, exposing data of various companies in the US including Delta, Kmart and Sears [341]
Ukrainian Energy Ministry	Ukraine	Ransomware	Government	Due to the attack various websites of the Ukrainian government, including the Energy Ministry were Shut-down[342]
Unnamed online casino and additional targets	Unnamed country in Central America	Hacking/ malware	Gambling	Lazarus APT attacked multiple targets in central America with various malware including the wiper KillDisk[343]
HealthEquity	Data Breach	USA	Healthcare	The data breach compromised records of 23,000 Individuals
		May		
Banco de Chile	Chile	Hacking and wiper malware	Financial	Attackers stole $10 million dollar via the SWIFT system and attempted to cover their tracks via a wiper malware[344]
Two Canadian banks Bank of Montreal Canadian Imperial Bank of Commerce (CIBC)	Canada	Extortion	Financial	The banks got ransom demands threatening to leak financial data of 90K clients[345]
Several Russian Banks	Russia	Data breach	Financial	The attacks are attributed to the Russian APT Cobalt [346]
Nuance	USA	Data breach	Software	A former employee of the firm breached their servers and accessed private data of 45,000 individuals. Includes full named, DOB, medical records, etc. [347]
Securus Technologies	USA	Data breach	High-tech	The company provides cell location monitoring and tracking services to private and defense organizations. It confirmed that the attackers gained access to records of some of its clients [348]
LifeBridge Health and LifeBridge Potomac Professionals	USA	Data breach	Healthcare	The attack affected half a million clients
200 million accounts of Japanese citizens	Japan	Espionage	Websites	A hacker, presumed Chinese, sold data of 200 million user accounts of about 50 different Japanese websites [349]

338 https://www.databreaches.net/trusted-quid-notification-of-web-site-data-breach-affecting-loan-applicants/
339 https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/
340 https://www.databreaches.net/jp-massive-data-leak-from-government-ministries/
341 https://www.infosecurity-magazine.com/news/sears-kmart-and-delta-hit-with/
342 https://threatpost.com/ransomware-attack-hits-ukrainian-energy-ministry-exploiting-drupalgeddon2/131373/
343 https://securityaffairs.co/wordpress/71074/apt/lazarus-online-casino.html
344 https://www.scmagazineuk.com/wiper-attack-at-chilean-bank-provided-cover-for-10m-swift-heist/article/773649/
345 https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/two-canadian-banks-contacted-by-fraudsters-about-potential-data-theft/
346 https://www.bleepingcomputer.com/news/security/cobalt-hacking-group-still-active-despite-leaders-arrest/
347 https://www.scmagazine.com/speech-recognition-software-firm-breach-exposes-thousands-of-patient-records/article/767531/
348 https://motherboard.vice.com/en_us/article/gykgv9/securus-phone-tracking-company-hacked
349 https://www.bleepingcomputer.com/news/security/data-of-over-200-million-japanese-sold-on-underground-hacking-forum/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Allied Physicians	USA	Ransomware	Healthcare	The practice did not disclose whether a ransom was in fact demanded in this incident, nor if any sum was ultimately paid, but clarified that the incident was contained. No additional information was disclosed
MedEvolve	USA	Misconfiguration of a public FTP server	Software, Healthcare	Misconfigured FTP Server Compromises Data of 205,000 Patients
AgentRun	USA	Misconfigured of an S3 Bucket	Software, Healthcare, Insurance	The incident exposed personal and medical data.
Minnesota-based Associates in Psychiatry and Psychology (APP)	USA	Ransomware	Healthcare	The attackers, who are believed to be located in Eastern Europe, infected several of APP's computers with a TripleM ransomware variant
Aultman Health Foundation	USA	Phishing	Healthcare	The attack compromised medical data of 42,600 patients.
Russian-speaking Telegram users	Russia	Malware	Individuals	Cisco exposed a malware that exfiltrates victims' data.
Three Florida Hospital websites	USA	malware	Healthcare	The attack potentially exposed patient names, email addresses, phone numbers, birthdates, height, weight, insurance carriers and the last four digits of individuals' Social Security numbers. No financial information was compromised. The malware did not affect any other hospital infrastructure.
Texas Health Physicians Group	USA	Data breach	Healthcare	An unauthorized third party may have gained access to a number of Texas Health email accounts in October 2017, potentially exposing sensitive patient information
PageUp	Australia	Data breach	HR software provider - provides services to companies and organizations across multiple sectors	Client data, including client names, street addresses, email addresses, and telephone numbers, may have been compromised. [350]
June				
Liberty Holdings Limited	South Africa	Hacking and extortion	Financial	Sensitive data was compromised.[351] The ransom was not paid [352]
CarePartners	Canada	Hacking and extortion	Healthcare	Sensitive and medical data was compromised. It is unknown if the ransom was paid [353]
Flightradar24	Sweden	Data breach	Aviation	The website was breached exposing some data [354]
Med Associates	USA	Data breach	Healthcare	270,000 patient records were compromised [355]
Bithumb	South Korea	Hacking	Financial	Hackers stole $30 million in cryptocoins[356].
Coinrail	South Korea	Hacking	Financial	Over $37 million in cryptocoins stolen [357].

350 https://www.zdnet.com/article/pageup-confirms-some-data-compromised-in-breach/
351 https://mybroadband.co.za/news/security/264799-hackers-want-millions-from-liberty-or-will-start-releasing-sensitive-data-report.html
352 https://www.bloomberg.com/news/articles/2018-06-17/south-africa-s-liberty-says-payment-demand-refused-after-breach
353 https://latesthackingnews.com/2018/07/19/carepartners-data-breach-update-hackers-hold-the-data-to-ransom/
354 https://www.theregister.co.uk/2018/06/21/flightradar24_data_breach/
355 https://www.scmagazine.com/home/security-news/data-breach/270000-med-associates-records-possibly-compromised-in-data-breach/
356 https://www.ccn.com/breaking-south-korean-crypto-exchange-bithumb-hacked-thieves-steal-30-million/
357 https://www.ccn.com/korean-cryptocurrency-exchange-coinrail-suffers-40-million-theft/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Intel	Global	Vulnerability	technology company	A vulnerability knows as Lazy FP State Restore (CVE-2018-3665) affects every modern Intel processor, and could potentially enable attackers to access sensitive data of computers and systems [358].
Chinese espionage campaign against companies and organizations in Asia	Japan and South Korea	Espionage campaign targeting air-gapped systems	N/A	Chinese APT 'Tick' attacked and stole data from air-gapped systems via malicious USB devices[359]
Chinese country-level espionage attack	Unknown state in Central Asia (possibly Mongolia)	Hacking and watering hole attack	Government	The campaign, executed by APT27 (aka LuckyMouse and EmissaryPanda), compromised a key national datacenter[360]
Adidas AG	USA	Data breach	Sport clothing	The company's US website was breached and potentially compromised data affecting millions of customers[361]
Typeform	Spain	Data breach	online forms and surveys	The attack stole a backup file with sensitive customer data [362]
Dixons Carphone	UK	Data breach	Telecommunication	Attackers gained access to 6 million credit cards and private records of 1.2 million clients, however Dixons claims the no sensitive data was compromised. [363]
US Navy Contractor	USA	Data breach	Defence	Chinese Nation-State Hackers Stole 614GB of Data from a U.S. Navy Contractor[364]
Satellite, Geospatial Imaging, Defense Companies	USA	Data breach	Defence	A Chinese threat group, Thrip, has been targeting satellite, communications, geospatial imaging, and defense organizations
NHS	UK	Data leak due to employee error	Healthcare	150,000 individuals'' data was exposed [365]
Exactis	USA	Data breach	Big Data advertising	The attack compromised 2 Terabytes of data with 340 million records [366]
TicketMaster	USA	Data breach/attack via the supply chain	Entertainment	Personal and financial data of customers was stolen. The attack was likely part of a larger campaign [367]
PumpUp	Canada	Data breach	Mobile	A core backend server hosted on Amazon's cloud was accessible without a password, exposing message metadata and contents[368]
Orange[369]	Belgium	Data breach	Telecom	Data leak compromised the personal information of some 15,000 customers of telecommunications company Orange in Belgium.
MyHeritage	Israel	Data breach	Healthcare	The genealogy and DNA testing company experienced a data breach that compromised the account details of 92,283,889 individuals [370]

358 https://thehackernews.com/2018/06/intel-processor-vulnerability.html
359 https://unit42.paloaltonetworks.com/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/
360 https://thehackernews.com/2018/06/chinese-watering-hole-attack.html
361 https://www.bloomberg.com/news/articles/2018-06-28/adidas-says-millions-of-u-s-customers-being-alerted-of-breach
362 https://www.bleepingcomputer.com/news/security/typeform-announces-breach-after-hacker-grabs-backup-file/
363 https://www.theregister.co.uk/2018/06/13/dixons_carphone_breach/
364 https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.49eec300dcef
365 https://www.bbc.com/news/technology-44682369
366 https://www.wired.com/story/exactis-database-leak-340-million-records/
367 https://www.zdnet.com/article/ticketmaster-breach-was-part-of-a-larger-credit-card-skimming-effort-analysis-shows/
368 https://www.zdnet.com/article/fitness-app-pumpup-leaked-health-data-private-messages/
369 http://www.brusselstimes.com/business/11653/details-of-15-000-orange-users-hacked
370 https://krebsonsecurity.com/tag/myheritage-breach/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Bio-chem Labs and Financial Institutions	Russia, Ukraine, and several European countries	Hacking, Malware, Spear Phishing	Government, Financial, Research	Olympic Destroyer executed a sophisticated attack campaign following the recent Olympics attack [371]
Rex Mundi Cybercrime Group	Multiple countries	Law enforcement operation	Cybercrime group	In a joint international operation between various law informant agencies, Europol arrested 15 members of the hacker extortion group over the past year.
July				
Domain Factory	Germany	Data breach	Website hosting services	The breach exposed customer data including names, numbers, physical addresses, email addresses, phone numbers, and dates of birth[372]
Yatra	India	Data breach	Online travel booking website	The breach exposed customer data including email address & physical addresses, phone numbers & plain text passwords & PINs of 5 Million users[373]
Australian National University	Australia	Data breach	Academia and defence	Chinese hackers breached the Uni's systems and stole sensitive governmental project's data[374]
B&B Hospitality Group	USA	PoS Malware	Food - Restaurants	The company identified the malware at nine different restaurants in the New York metropolitan area[375]
VSDC	Global	Hacking + Malware	Online services - free video and audio editor	In three different incidents hackers changed the download links on the VSDC website with malicious links that downloaded three different malwares[376]
Blizzard Entertainment	USA	DDoS	Computer gaming	The attack affected players of multiple games[377]
Timehop	USA/Global	Data breach	Online services – mobile App	The breach compromised names and emails of 21 Million users. 4.7 Million of the affected users also had their phone number compromised[378]
Bancor	Israel	Data breach	Financial	The attackers stole $13.5 Million in Cryptocoins [379]
Inbenta	USA	Attack via the supply chain	AI-based services	This attack presumably enabled the attack on Ticketmaster [380]
Cambodia	Cambodia	large-scale phishing and hacking campaign	Government	The attack is attributed to China-based group TEMP.Periscope APT[381]
US Air Force	USA	Data breach	Defence	Sensitive data including data of military drones was exposed online [382]
Chlorine distillation plant	Ukraine	Malware	Critical infrastructure	Ukrainian intelligence thwarted the attack, executed via VPNFilter malware and by Russian attackers[383]
Pennsylvania Department of Health	USA	Data breach	Government and Healthcare	The attack disabled the organization systems for a week [384]

371 https://thehackernews.com/2018/06/olympic-destroyer-malware.html
372 https://www.zdnet.com/article/user-data-exposed-in-domain-factory-hosting-security-breach/
373 https://www.thenewsminute.com/article/yatracom-breach-how-check-if-your-data-compromised-and-what-do-if-it-84247
374 https://www.smh.com.au/politics/federal/chinese-hackers-breach-anu-putting-national-security-at-risk-20180706-p4zq0q.html
375 https://www.prnewswire.com/news-releases/bb-hospitality-group-reports-findings-from-investigation-of-payment-card-security-incident-300677177.html
376 https://www.bleepingcomputer.com/news/security/popular-software-site-hacked-to-redirect-users-to-keylogger-infostealer-more/
377 https://www.technobuffalo.com/2016/09/18/blizzard-ddos-battlenet-down-overwatch-wow-hearthstone/
378 https://techcrunch.com/2018/07/09/timehop-discloses-july-4-data-breach-affecting-21-million/
379 https://www.coindesk.com/token-platform-bancor-goes-offline-following-security-breach
380 https://www.zdnet.com/article/inbenta-blamed-for-ticketmaster-breach-says-other-sites-not-affected/
381 https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html
382 https://www.recordedfuture.com/reaper-drone-documents-leaked/
383 https://www.bleepingcomputer.com/news/security/ukraine-says-it-stopped-a-vpnfilter-attack-on-a-chlorine-distillation-station/
384 https://www.databreaches.net/pennsylvania-birth-certificate-system-hacked-no-records-stolen/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
LabCorp	USA	Data breach	Healthcare	One of the largest medical diagnosis companies in the US. The attack compromised data of 1 million patients [385]
Italian Military	Italy	Data breach	Defence	The campaign, dubbed Roman Holiday, is attributed to APT28 [386]
Mega	New Zealand	Data breach	Cloud storage services	Clear text file with 15K users' names, passwords and file names was leaked [387]
Liverpool FC	UK	Data breach	Sports	150 members' data was leaked [388]
SingHealth	Singapore	Data breach	Healthcare	Largest healthcare services provider group – the attack exposing data of patients including the prime minister [389]
PIR Bank	Russia	Hacking	Financial	The attack is attributed to MoneyTaker group. The attackers stole $1 Million[390]
COSCO Shipping	China	Ransomware	Maritime Shipping	The attack disrupted COSCO's American operations and took its US website offline[391]
KICKICO	Russia	Hacking	Financial	The attackers stole about $7.7 million[392]
US state and local government agencies	USA	Malware	Government	Several local and federal agencies receive malware infected disks sent from China [393]
VSDC	Global	Hacking + Malware	Online services - free video and audio editor	In three different incidents hackers changed the download links on the VSDC website with malicious links that downloaded three different malwares[394]
NSO Group	Israel	Data Breach	Software developer	A disgruntled ex-employee attempted to sell proprietary data for $50M on the Darknet[395]
Telefonica	Spain	Data Breach	Telecoms	The attack exposed sensitive data including mobile and landline numbers, residential addresses, national ID numbers, names, banks, billing records and call history[396]
LabCorp[397]	USA	Brute force RDP + Malware	Healthcare diagnostics	Thousands of systems were infected by SamSam via a brute force RDP attack. LabCorps claims that the attack was contains within an hour
Level One Robotics[398]	Canada/Global	Server misconfiguration	Multiple manufacturing industries	The third-party supplier left over 150GB of sensitive data regarding over 100 manufacturing firms including VW, Chrysler, Ford, Toyota, GM, Tesla, and ThyssenKrupp.
NHS[399]	UK	Data leak – coding error	Healthcare	The error disclosed data on 150,000 patients
August				
Amnesty International	Global	Spy malware attack	NGO	Executed via NSO spy software[400]
Hong Kong's Department of Health	China – Hong Kong	Ransomware	Government and healthcare	1.5 million patients' records were lost due to the attack[401]

385 http://fortune.com/2018/07/17/labcorp-security-breach/
386 https://securityaffairs.co/wordpress/74460/apt/operation-roman-holiday-apt28.html
387 https://www.zdnet.com/article/thousands-of-mega-logins-dumped-online-exposing-user-files/
388 https://latesthackingnews.com/2018/07/21/liverpool-fcs-fan-database-hacked/
389 https://www.telegraph.co.uk/news/2018/07/20/cyber-attack-singapore-health-database-steals-details-15m-including/
390 https://www.hackread.com/hackers-attack-russian-bank-to-steal-1m-using-an-outdated-router/
391 https://arstechnica.com/information-technology/2018/07/shipping-companys-networks-in-the-americas-crippled-by-ransomware-attack/
392 https://www.hackread.com/ico-hacked-hackers-steal-millions-kickico-blockchain/
393 https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/
394 https://www.bleepingcomputer.com/news/security/popular-software-site-hacked-to-redirect-users-to-keylogger-infostealer-more/
395 https://www.theregister.co.uk/2018/07/06/nso_group_employee_charged/
396 https://www.hackread.com/spanish-telecom-firm-telefonica-suffers-massive-security-breach/
397 https://www.csoonline.com/article/3291617/security/samsam-infected-thousands-of-labcorp-systems-via-brute-force-rdp.html
398 https://www.infosecurity-magazine.com/news/robotics-supplier-error-leaks/
399 https://www.theinquirer.net/inquirer/news/3035205/nhs-blames-coding-error-for-breach-that-disclosed-data-on-150-000-patients
400 https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/
401 https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2158023/after-singapore-medical-data-hack-hong-kongs

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Elbit Systems	Israel	Data breach	Defence and aerospace	Account details of 10,000 users (including Admins) were leaked by a hacker known as DarkCode (Th3Falcon)[402]
TSMC (Taiwan Semiconductor Manufacturing Co.) [403]	Taiwan	Malware – WannaCry variant	Technology manufacturing	The attack disrupted operation, shutting down several factories
Mention	France	Attack via the supply chain	Social media monitoring services	Users' data such as full names and passwords was compromised [404]
Royal Air Force[405]	UK	Hacking - phishing	Military	RAF airwoman's Tinder account hacked in an attempt to steal classified information about Britain's F-35 from RAF serviceman who also used dating app
Livecoin	USA	Exploitation of a vulnerability	Financial	A vulnerability in Monero Code enabled hackers to steal $1.8 Million[406]
PGA of America	USA	Ransomware	Sports	A ransom in bitcoins was demanded to unlock the organization's systems [407]
Cosmos Bank	India	Malware	Financial	The attackers stole $13.4 Million dollars [408]
Superdrug Stores PLC	UK	Data breach	health and beauty retailer	20K customers' data was stolen [409]
Multiple Banks in Spain	Spain	Malware	Financial	BackSwap malware campaign against at least six banks[410]
Banco de España	Spain	DDoS	Financial	Executed by Anonymous Catalonia [411]
T-Mobile	USA	Data breach	Telecommunication	Data of 2 million customers was exposed [412]
Schneider Electric	France	Malware	Solar energy	Flash drive delivered to clients with the company's products was infected with malware[413]
Huazhu Group Ltd.	China	Data breach	Tourism and hospitality	The attack affects 130 million people [414]
TheTruthSpy	USA	Data breach	Spy software developer	Hacker stole sensitive data[415]
Air Canada	Canda	Data breach	Aviation	The company's cellphone app compromised [416]
NS Bank and Banca Comercială Carpatica / Patria Bank	Russia and Romania	Phishing and malware	Financial	Russian APT Cobalt [417]
September				
Facebook	USA	Data breach	Social media	Attackers exploited a 0-day vulnerability stealing 30 million users access tokens (early reports reported 50M) [418]
US military – 'Defend Forward' Cyber Strategy	USA	New cyber-defence strategy	Military - Defense	The new strategy has an aggressive stance against foreign nation-state actors who target the US. It grants the army more authority to launch preventative cyber-strikes [419]

402 https://www.cyberwarnews.info/2018/08/02/aerospace-corp-elbit-systems-breached-10-000-accounts-leaked/
403 https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html
404 https://latesthackingnews.com/2018/08/04/mention-suffered-data-breach-due-to-a-third-party-service-provider/
405 https://www.dailymail.co.uk/news/article-6027207/Honeytrap-spy-stole-secrets-new-RAF-stealth-jet-hacking-Tinder-profile.html
406 https://icobrothers.media/2018/08/04/livecoin-crypto-exchange-lost-more-than-18-million-because-of-monero-code-vulnerability/
407 https://www.cbsnews.com/news/2018-pga-championship-hackers-reportedly-target-pga-of-americas-servers-steal-files-related-to-tournament-and-ryder-cup/
408 https://www.bankinfosecurity.com/police-investigate-cosmos-bank-hack-a-11379
409 https://www.theregister.co.uk/2018/08/21/superdrug_hackers_claims/
410 https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/
411 https://www.bleepingcomputer.com/news/security/anonymous-catalonia-claims-ddos-attack-on-bank-of-spain-website/
412 https://motherboard.vice.com/en_us/article/a3qpk5/t-mobile-hack-data-breach-api-customer-data
413 https://securityaffairs.co/wordpress/75986/malware/schneider-usb-drives-malware.html
414 https://www.hotelmanagement.net/tech/data-leak-from-huazhu-hotels-may-affect-130-million-customers
415 https://motherboard.vice.com/en_us/article/mb4y5x/thetruthspy-spyware-domestic-abusers-hacked-data-breach
416 https://nakedsecurity.sophos.com/2018/08/30/air-canada-resets-1-7-million-accounts-after-app-breach/
417 https://asert.arbornetworks.com/double-the-infection-double-the-fun/
418 https://thehackernews.com/2018/10/hack-facebook-account.html
419 https://edition.cnn.com/2018/09/18/politics/us-military-cyberattacks-authority/index.html

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
The United Nations	Global	Data leak – misconfiguration of multiple services	Intergovernmental organization	The UN accidentally exposed published passwords, internal documents, and technical details about its websites[420]
REDICO	USA	Phishing	Real estate	W-2 tax forms were compromised [421]
British Airways	UK	Data Breach - Magacart malware	Aviation	The breach compromised personal and payment information of about 380,000 customers. The attack is attributed to Megacart
Bristol Airport	UK	Ransomware	Aviation	The attack caused disturbances to operation and blackout of flight information screens [422]
US State Department	USA	Data breach	Government	The breach affected hundreds of employees, compromising personal information [423]
Japanese media sector	Japan	Data breach	Media and entertainment	Chinese group APT10 [424]
Italian National Institute for Social Assistance (INAS)	Italy	Data breach	Government	The portal was hacked exposing users' data [425]
Indian governmental websites	India	Cryptojacking	Government	Several websites were infected by cryptomining malware [426]
Newegg, Groopdealz and Feedly	N/A	Malware	Several different sectors	Magecart group[427]
Zaif	Japan - Global	Breach	Financial	60M in Cryptocoins was stolen [428]
pigeoncoin	USA	Vulnerability	Financial	By exploiting a coin fork the attackers stole $150,000 [429]
Port of Barcelona **Port of San Diego**	Spain USA	Ransomware	Government and transport	Both ports were infected by ransomware one week apart [430]
SHEIN	USA	Data breach	Online fashion retailer	The breach affects 6.42 Million customers [431]
Toyota Industries North America, Inc.	USA	Data breach	Automobile	The attacker accessed the company's email system and compromised data of 66K employees and clients [432]
Fiserv Inc.	USA	Vulnerability disclosure	Technology services provider for financial institutions	A web platform flaw exposed personal and financial account information on hundreds of bank websites [433]
Arran Brewery	UK	Ransomware	Whisky Brewery	The attackers sent to a job application a CV with a malicious attachment [434]
Blue Cross and Blue Shield of Rhode Island (BCBSRI)	USA	Data Breach	Healthcare	The breach exposed personal health-care information of 1,567 people. The company is blaming the breach on an unnamed vendor [435]

420 https://theintercept.com/2018/09/24/united-nations-trello-jira-google-docs-passwords/
421 https://www.doj.nh.gov/consumer/security-breaches/documents/redico-20180924.pdf
422 https://www.zdnet.com/article/ransomware-attack-blacks-out-screens-at-bristol-airport/
423 https://www.zdnet.com/article/state-department-reveals-email-data-leak/
424 https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html
425 https://gdpr.report/news/2018/09/17/cyber-attack-on-italian-national-institute-for-social-assistance-threatens-users-personal-data/
426 https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/hackers-mined-a-fortune-from-indian-websites/articleshow/65836088.cms
427 https://threatpost.com/magecart-threat-group-racks-up-more-hack-victims/137439/
428 https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft
429 https://www.coindesk.com/bitcoin-bug-exploited-on-crypto-fork-as-attacker-prints-235-million-pigeoncoins
430 https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/
431 https://threatpost.com/malware-on-shein-servers-compromises-data-of-6-4m-customers/137684/
432 https://www.dataprivacyandsecurityinsider.com/2018/10/hacker-hits-toyota/
433 https://krebsonsecurity.com/2018/08/fiserv-flaw-exposed-customer-data-at-hundreds-of-banks/
434 https://www.scmagazine.com/home/news/scottish-brewery-ransomware-attack-leverages-job-opening/
435 http://www.providencejournal.com/news/20180912/blue-cross-blames-vendor-for-breach-of-customer-information-in-ri

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
UK Ministry of Defense and GCHQ	UK	Launch of Offensive Cyber Force	Defense and surveillance service	It was announced that a £250m cyber task force is being launched to enhance the nation's offensive capabilities [436]
RCN	USA	Data leak	Internet and cable service provider	It was revealed that the ISP stored customer passwords in cleartext [437]
Unnamed E-marketing Database	Global	Data Leak - Unprotected MongoDB	Online Marketing	The database of 43.5GB contains 11 million customer records, including personal details, such as email, full name, gender, physical address (zip code, state, city of residence) [438]
EOS.IO	Global	Data Breach	Online services – Gambling App	The hacker stole $200,000 [439]
October				
Cathay Pacific	China – Hong Kong	Data breach	Aviation	Personal and identifying data of 9.4 million people was compromised[440]
Google +	USA	Data breach	Social media	A flaw in the platforms system exposed 500,000 users' data since 2015. No exploitation of the flaw was report; however, following the reveal Google shut down the platform [441]
Pentagon Travel Provider	USA	Data breach	Government and tourism	The attack compromised data of 30,000 people [442]
Mumbai branch of State Bank of Mauritius (SBM)	India and Mauritius	Hacking	Financial	The attackers attempted to steal 20 million dollars [443]
Hetzner South Africa ISP	South Africa	Data breach	IT and Communication	Data of 40,000 customers was exposed. See item in report.
Icelandic citizens	Iceland	Phishing and Malware campaign	Individuals	A massive phishing campaign targeting Iceland and distributing the Remcos remote access tool.
Onslow Water and Sewer Authority (ONWASA)	USA	Malware & Ransomware	Critical infrastructure	The water and sewer service provider was hit by a sophisticated malware attack.
City of West Haven[444]	USA	Ransomware	Municipality	The city paid $2,000 to decrypt 23 servers. According to officials no data appears to have been exfiltrated.
City of Muscatine[445]	USA	Ransomware	Municipality	Several servers were affected. No additional information is known as of Nov. 21.
Indiana National Guard[446]	USA	Ransomware	Government and Defense	According to reports the attack compromised a non-military server that contained identifying information of civilian and military personnel
US Indicts Chinese Spies and Insiders for Aviation Theft	USA	Espionage	Aviation	Two intelligence officers, two insiders and six hackers, were indicted by US government for allegedly conspiring to steal aviation secrets
Cathay Pacific	USA	Data Breach	Aviation	The breach my affect over 9M customers.
Girl Scouts US	USA	Data Breach	N/A	The breach may affect as much as 2,800 girl scouts in Orange County.
MapleChange	Canada	Security breach	Financial	The attackers stole $6M [447]
Burgerville	USA	Security breach	Fast food	The US fast food chain was attacked by Fin7 APT

436 https://www.infosecurity-magazine.com/news/mod-gchq-set-launch-offensive/
437 https://www.zdnet.com/article/us-isp-rcn-stores-customer-passwords-in-cleartext/
438 https://www.linkedin.com/pulse/another-e-marketing-database-11-million-records-bob-diachenko/
439 https://thenextweb.com/hardfork/2018/09/14/eos-gambling-app-hacked/
440 https://www.theregister.co.uk/2018/10/25/cathay_pacific_hacked_up_to_94_million_passenger_deets_exposed/
441 https://www.wired.com/story/googles-privacy-whiplash-shows-big-techs-inherent-contradictions/
442 https://www.bankinfosecurity.com/pentagon-data-breach-exposed-30000-travel-records-a-11600
443 http://pushpmagazine.com/hackers-hacked-server/
444 https://www.scmagazine.com/home/security-news/west-haven-indiana-national-guard-muscatine-hit-with-ransomware-attacks/
445 https://www.muscatineiowa.gov/ArchiveCenter/ViewFile/Item/2776
446 https://www.theindychannel.com/news/state-news/indiana-national-guard-server-attacked-by-ransomware
447 https://ethereumworldnews.com/maplechange-crypto-exchange-hacked-for-913-bitcoin-btc-exit-scam-likely/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Pocket iNet	USA	Data leak	IT and Communication	The ISP left a AWS database of 73GB of sensitive data exposed [448]
Multiple Nuclear Energy Firms	Russia, Iran and Egypt	Hacking and Malware	Critical infrastructure	Companies related to nuclear energy, telecommunications, IT, aerospace, and R&D [449]
Centers for Medicare & Medicaid Services	USA	Data Breach	Insurance	The breach compromised data of about 75,000 individuals
Pentagon[450]	USA	Data Breach	Government and Defense	A Defence Department third-party provider was breached. Personal and financial info of U.S. military and civilian personnel was compromised
Italian Naval Industry	Italy	Targeted Cyber-Espionage Campaign	Government and Defense	The attackers used a malware dubbed MartyMcFly [451]
Eurostar[452]	France & UK	Hacking attempt	Transportation	Customers' login passwords were reset following attempts to break into an unspecified number of accounts.
Internet Solutions (IS)[453]	South Africa	Data breach	IT and Communication	The company detected “irregular activity” on some of its virtual services
70 Gabon Government Websites[454]	Gabon	DDoS	Government	The attack was executed by Anonymous as part of “anti-dictatorships” campaign.
FIFA[455]	N/A	Security breach	Sports	The organizations admitted that in March its systems were hacked for the second time this year
November				
Extradition of hacker - Guccifer[456]	Romania & USA	Extradition	Government and law enforcement	Notorious hacker Guccifer was extradited to the US from Romania to finish serving a prison sentence for cybercrimes including exposing Hillary Clinton’s personal email account use while serving as secretary of state
Austal Ltd	Australia	Security breach and extortion attempt	Maritime defense	Australian Cyber Security Centre (ACSC) determined the attack was most likely executed by Iranian hackers[457]
St. Francis Xavier University	Canada	Cryptojacking	Academia	The Uni had to shut down its entire computer and IT system after it was hacked and used to mine cryptocoins[458]
HSBC	USA	Data breach	Financial	The attack compromised customers' data [459]
Ingerop	France	Data breach	critical infrastructure	The attackers store sensitive documents regarding, amongst other things, prisons and nuclear power plants [460]
Altus Baytown Hospital (ABH)	USA	Ransomware	Healthcare	In early November the hospital reported[461] that it was infected by Dharma ransomware [462]
LPL Financial / Capital Forensics, Inc.	USA	Attack via the supply chain	Financial	By hacking a service provider, the attacker compromised sensitive data regarding LPL clients [463]

448 https://www.upguard.com/breaches/out-of-pocket-how-an-isp-exposed-administrative-system-credentials
449 https://www.zdnet.com/article/kaspersky-says-it-detected-infections-with-darkpulsar-alleged-nsa-malware/
450 https://phys.org/news/2018-10-pentagon-reveals-cyber-breach.html
451 https://securityaffairs.co/wordpress/77195/malware/martymcfly-malware-cyber-espionage.html
452 https://www.bbc.com/news/technology-46048597
453 https://mybroadband.co.za/news/cloud-hosting/281167-internet-solutions-warns-of-security-breach.html
454 https://www.news24.com/Africa/News/gabon-official-websites-hacked-anonymous-group-20181029
455 https://www.nytimes.com/2018/10/30/sports/soccer/fifa-uefa-hack.html
456 https://www.washingtontimes.com/news/2018/nov/13/guccifer-romanian-hacker-extradited-us-finish-pris/
457 https://www.theguardian.com/technology/2018/nov/02/defence-shipbuilder-austal-hit-with-data-breach-and-extortion-attempt
458 https://news.softpedia.com/news/bitcoin-cryptojacking-attack-forces-university-to-disable-entire-network-523646.shtml
459 https://www.forbes.com/sites/daveywinder/2018/11/06/hsbc-bank-usa-admits-breach-exposing-account-numbers-and-transaction-history/
460 https://www.dw.com/en/hackers-obtain-nuclear-power-plant-plans-in-france/a-46126878
461 https://news.softpedia.com/news/dharma-ransomware-hits-altus-baytown-hospital-s-systems-523692.shtml
462 https://www.bleepingcomputer.com/news/security/new-brrr-dharma-ransomware-variant-released/
463 https://news.bloomberglaw.com/privacy-and-data-security/lplisprobing-a-breach-at-vendor-that-put-personal-data-at-risk

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Pakistan Air Force	Pakistan	Nation-state attack campaign	Military	The attackers used 0-day vulnerabilities and sophisticated attack tools [464]
Russian financial institutions	Russia	Large-scale phishing campaign	Financial	The campaign was executed by two groups – MoneyTaker and TheSilence [465]
Hacker known as "Tessa88"	Russia	Doxing	Criminal	The identity the hacker behind LinkedIn, Dropbox Databases breaches, was exposed as Russia citizen Vladimirovich Donakov (Максим Владимирович Донаков) [466]
Pathé's	The Netherlands	Phishing - BEC	Media	The head of the group was scammed out of over 19M Euro[467]
Malta Lands Authority[468]	Malta	Data leak	Government	A security flaw exposed since early 2017 over 10GB of citizens' personal data
Media Prima[469]	Malaysia	Ransomware	Media	Attackers demanded 1,000 bitcoins (about US$6.45M)
American Express India[470]	India	Data leak – misconfigured MongoDB server	Financial	Personal info of nearly 700,000 Amex India customers was exposed
December				
UNNAMED1989 / WeChat Ransomware	China	Ransomware	Private people/Various sectors	Within days over 100K people and companies were infected [471]
The Democratic National Committee (DNC)	USA	Data breach	Government	In December it was reported that the party's systems were breached, exposing data and thousands of emails [472]
Ukraine judicial system	Ukraine	Phishing and Malware	Government	According to Security Service of Ukraine (SBU), they thwarted a massive Russian attack on the country's judicial system [473]
Quora	Global	Data breach	Website	The attack compromised records of 100 million users [474]
Moscow's Cable Car System	Russia	Hacking and ransomware	transportation	Two days after the service was launched its systems were hacked and infected by ransomware [475]
Sotheby's	Global	Malware	Auctions	The auction house's website was infected by Megacart malware for over a year [476]
Marriott International Inc.	Global	Data breach	Tourism and hospitality	The attack compromised data of 500 million customers since 2014. [477] Possibly executed by a Chinese nation-state APT [478]
USPS	USA	Data breach	Postal services	A API vulnerability exposed account details of 60 million USPS online service users
Save the Children Federation	USA	Phishing - BEC	NGO	The organization lost $1 million dollars [479]

464 https://securityaffairs.co/wordpress/77982/apt/operation-shaheen-campaign.html
465 https://www.zdnet.com/article/russian-banks-hit-by-major-phishing-attacks-from-two-hacker-groups/
466 https://thehackernews.com/2018/11/tessa88-russian-hacker.html
467 https://www.infosecurity-magazine.com/news/dutch-film-boss-sacked-after-19m/
468 https://www.timesofmalta.com/articles/view/20181123/local/massive-lands-authority-security-flaw-dumps-personal-data-online.694982
469 https://securityboulevard.com/2018/11/hackers-infect-malaysias-largest-media-company-with-ransomware-then-demand-6-45-million/
470 https://www.zdnet.com/article/data-of-nearly-700000-amex-india-customers-exposed-via-unsecured-mongodb-server/
471 https://www.bleepingcomputer.com/news/security/chinese-police-arrest-dev-behind-unnamed1989-wechat-ransomware/
472 https://www.infosecurity-magazine.com/news/republican-party-breached/
473 https://www.infosecurity-magazine.com/news/ukraine-blocked-major-russian/
474 https://threatpost.com/quora-breach-exposes-a-wealth-of-info-on-100m-users/139606/
475 http://www.ehackingnews.com/2018/12/moscows-first-cable-car-system-hacked.html
476 https://www.infosecurity-magazine.com/news/southebys-site-infected-magecart/
477 http://www.ehackingnews.com/2018/12/marriott-hotel-hack-exposes-500-million.html
478 https://securityaffairs.co/wordpress/78741/data-breach/starwood-chinese-hackers.html
479 https://threatpost.com/save-the-children-federation-duped-in-1m-scam/139925/

Entity/Target	Country	Event/ Attack Vector	Sector/ Industry	Notes
Cadastro de Pessoas Físicas (CPF)	Brazil	Data breach - Apache Misconfig	Government	Identifying details of 120 million Brazilian citizens were exposed online due to misconfiguration of a server[480]
Saipem	Italy, Saudi Arabia, UAE, Kuwait and Scotland	Wiper malware	Oil services firm	The Italian company's servers located in various countries were attacked with a wiper malware. The attack originated from Chennai, India [481]
Multiple industries across at least 12 countries	Multiple countries	Long term espionage campaign	Multiple sectors	Chinese group APT10 [482] - Brazil, Canada, Sweden, India, Switzerland, Finland, Japan, Germany, France, the UAE, the UK, and the U.S.
German politicians	Germany	Data breach	Government	Private data and records regarding hundreds of German politicians and public employees including Angela Merkel was leaked online [483]

480 https://www.bleepingcomputer.com/news/security/taxpayer-id-numbers-for-120-million-brazilians-exposed-online/
481 https://www.infosecurity-magazine.com/news/middle-east-servers-targeted-in/
482 https://www.bleepingcomputer.com/news/security/historic-apt10-cyber-espionage-group-breached-systems-in-over-12-countries/
483 https://www.reuters.com/article/us-germany-politics-cyber/german-politicians-data-hacked-government-cyber-team-in-crisis-meeting-idUSKCN1OY0IW

Email: info@clearskysec.com
Website: clearskysec.com

CLEARSKY
Cyber Security

Ahead of the Threat Curve

ClearSky cyber security solutions assists companies and organizations in preparing, identifying and resolving cyber security threats. Our team of security experts helps prevent security breaches by detecting early attack indicators, and providng in-depth analysis and intelligence that enable you to make informed mitigation decisions in real time.

ClearSky is comprised of intelligence researchers and cyber experts, who monitor, research and expose attack groups and cyberattacks around the globe. Our unique ClearSkySec© methodology is based on years of experience in mitigating cyberattacks targeting numerus sectors, including the financial sector, the pharma sector, as well as public and critical infrastructure sectors.