2019 H1
Cyber Events Summary Report

Ahead of The Threat Curve

www.ClearSkysec.com - info@ClearSkysec.com

Preface

The below report provides an in-depth review reviews significant trends, as well as major attack events in the cyber landscape that took place on the first half of 2019. The report follows our Cyber Events Summary Report of 2018 and presents changes and developments in the political and economic scenes as well, as these has had a crucial impact on the cyber arena.

In recent months we have observed multiple targeted ransomware attacks against major companies, including international corporations – undoubtfully, this is the most significant attack vector of the first half of 2019. The main penetration vector in these attacks includes the use of decoy email carrying malicious content and RDP (Remote Desktop Protocol) attack. In our assessment, this year RDP has become a significant vector through which computer systems are infected worldwide.

The most notable example of targeted ransomware operation is the Norsk Hydro Attack which we classified as the most significant attack of the first half of 2019. Forensic investigations covering the attack on Norsk Hydro, as well as other companies who suffered from similar incidents, revealed an extensive attack infrastructure aided by sophisticated, evasive tools and designated zero-day vulnerabilities. And indeed, the LockerGoga ransomware infrastructure has managed to infiltrate hundreds of companies worldwide and extort tens of millions of USD. Norsk Hydro alone stated that the damage caused by the attack is estimated at around 75 million USD.

Significant increase of targeted ransomware attacks on large companies and organizations globally

Behind several of these attacks are nation-state actors that execute ransomware attacks with the end goal of causing harm rather than financial gain. Several of the most notable ransomware attacks so far are – Norsk Hydro, ASCO, SonAngol and Verint. In contrast to the rising popularity of targeted ransomware, destructive ransomware attacks – in which the files are corrupted without a recovery option – were not reported during the first half of 2019. This could be the result of intense hindering collaborations between agencies worldwide.

Increase of BEC (Business Email Compromise) attacks

This type of an attack, in which the attacker traditionally impersonates an executive in the company or a third-party provider, is the most common type of attack globally. According to the latest data from the FBI, as of June 2018, BEC scams have compromised over 12 Billion dollars globally.[1] This figure is expected to continue rising in 2019. On the past two months, attackers begun leveraging AI (Artificial Intelligence) systems to impersonate senior employees' voices and execute financial transactions, resulting in immediate losses of millions of euros.

More Attacks against financial institutions

In 2019, financial institutes and banking users are still a desirable target for tailored cyber-attacks aimed at financial revenue. However, while the trend continues, we did not see a sharp increase in the attack rate. This appears to be a direct result of the considerable effort and resources invested by the banks in mitigating cyber threat conjunction with attackers targeting more profitable and less secure targets such as crypto-currency platforms. In 2019 these platforms continue suffering hundreds of millions of dollars in losses, being the most targeted financial platform to date. Alongside that, a

[1] https://www.ic3.gov/media/2018/180712.aspx

notable decrease in the rate of attacks targeting SWIFT system was observed – most likely as a result of the great effort invested by the security industry into protecting these systems.

Social media platforms combat the fake news phenomena

We have seen over the last six months considerble efforts by social media platforms to identify and take down fake-news sources and actors, by conducting both vast investigative efforts and routine take down actions, little by little. While this actions don't fully neutralize the phenomena, they do play a crucial role in raising awareness.

Attack attempts against Internet of Things (IoT) systems and SCADA Systems

Over the last six months we have seen alarming rise of threats to industrial IoT (Internet of Things) or ICS systems. Of note, various threat actors targeting power-grids. The most prominent actors in this regard are the USA and Russia. For example, Triton malware which was used in the attack on the Saudi oil refineries is currently being attributed to Russia

Escalation of the Digital Cold War between the US, Russia and China

The recent developments of a "digital cold war" between the US, China and Russia - amongst others - were a key event on the global cyber arena during the first half of 2019. Political conflicts resulted in immediate actions in the cyber landscape and led to parallel efforts by many power countries to possess designated SCADA malware, as well as the ability to cripple their adversaries' power facilities in preparation for a time of need. For the first time, Trump administration employees reported that a payload developed in the US was planted in Russia's power network .

One of the most outstanding results of this state his can be seen in the continued weaponization of social media platforms to propagate disinformation on a massive scale, and rapid proliferation of advanced malware. The latter in particular has facilitated new threats against service providers, alongside critical infrastructure.

Accordingly, these nations and their allies have begun taking major mitigation actions; be them economic such as embargoes and global trade restrictions, or technological such as new plans to implement an "internet kill-switch".[2] These and other developments are largely reactionary backlash following large-scale campaigns on numerous industries and sectors, including critical infrastructure, large industrial operations, and military organizations.

More and more countries are claiming almost direct responsibility for major attacks

This is likely in an attempt to create deterrence and signals the next stage in the digital cold war – "who is a bigger threat/can cause the most amount of damage". Alongside the deterrence efforts we continue to see exposures of Critical zero-day vulnerabilities that pose a threat to global computer networks, such as the BlueKeep flaw. We believe that Russia will likely attempt exploiting these vulnerbilities to execute a massive cyber attack in the vain of NotPetya.

Increase in Iranian cyber capabilities alongside the expansion of their cyber operations against foreign countries

With this regard, we also saw Iran expanding their operation into new regions. The increase in Iranian offensive operations in the cyber arena is aligned with the escalation of the conflict between Iran and the United States, concerning the Nuclear deal violation, the US sanctions and more.

[2] https://www.theguardian.com/world/2019/apr/11/russia-passes-bill-internet-cut-off-foreign-servers

Table of Contents

The Most Prominent Attack of 2019 – Norsk Hydro Corporation and Other Companies Attacked by the LockerGoga Ransomware

On March 18, 2019, Norsk Hydro, one of the largest aluminum manufacturers in the world based in Norway, experienced a significant cyber-attack using a ransomware called LockerGoga. The attack took place in the firm's factories in the US and led to a shutdown of all their computer systems. It also partially damaged the manufacturing systems in additional locations around the world. As a result, some factories had to switch to manual operation, slowing the manufacturing process and resulting in significant financial losses.

This is the first LockerGoga ransomware attack to gain global public attention. Recent findings indicate that the over 1,200 companies were attacked by the ransomware to this point, most of them global corporations with multiple R&D and manufacturing centers. Prior to these attacks, the known use of LockerGoga took place on January 24, 2019, against the France-based engineering firm Altran.[3]

It should be noted that while the ransomware has successfully infected multiple targets, it was not always activated. Nevertheless, infected companies may still be in danger as the attackers have gain access to their networks, and could leverage it for additional malware infection or offer it for sale to the highest bidder on underground forums. The damages could me immense. The companies whose files were encrypted by Locker Goga suffered direct losses tens of millions of USD and additional indirect losses. In the case of Norsk Hydro, for example, the estimated damage caused by the attack as of the end of July is 75 million USD.

Attack Vector

According to the Norwegian Cert, "NorCert", the Norsk Hydro ransomware infection was probably conducted manually, after the attackers gained access and achieved persistency on the company network – an operation which probably took several months to complete. On March 19, probably several minutes after midnight, the encryption process of multiple computers and servers had begun.

As a result, some 9,000 machines were encrypted and ceased to function. The initial intrusion vector appears to have included a large number of actions including Brute Force attacks on the company's RDP servers, SQL Injection attacks on company sites, exploiting a number of zero-day vulnerabilities and privilege escalation on sensitive systems, obtained through sophisticated phishing attacks. Part of the attack included logging out of vital control systems and locking employees' accounts. Consequently, the IT staff was unable to mitigate the event. The firm probably physically

[3] https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/

disconnected part of the network in an attempt to slow down the attack, which made it more difficult to realize the full extent of the damage.

According to analysis by Nozomi Network Labs[4] the ransomware is capable of encrypting the following type of files: DLL, ppt, pot, pps, pptx, potx, ppsx, sldx and pdf. Similar cyber-attacks using other ransomware families, such as Ryuk and MegaCortex, had also been observed.

Cloud Email Services enabled Functional Survivability

The firm's email services remained protected throughout the attack because the Norsk Hydro email system is based on Microsoft 365, a cloud service. Consequently, they were able to continue basic operations and maintain contact with clients. The employees logged in to their email accounts via personal smartphones and tablets, so some work flow was maintained, and recent orders could be retrieved from the clients. The manufacturing systems were disconnected from the computers and were operated manually.

The Attackers

As of early mid-July 2019, the common estimation is that a well-funded Russian threat group is responsible for the attack. An initial analysis released by Kaspersky[5] states that some parts of the ransomware file can be affiliated to Russian cybercrime group called GrimSpider. The investigation is still in process, however based on the attack stages – which included preliminary network research, zero-day vulnerability exploit and neutralization of security systems – there is no doubt this was a targeted attack.

According to an estimation of a research team for the Dutch government, at least two threat groups collaboration together are behind the attack. Their findings offer three possible motives for the attack. The first motive is financial, because after the attack victims were prompted to pay the ransom demand, and were threatened to have the access obtained by the attackers sold to other attackers. Another assessment suggests an espionage motive, relying on the fact that some of the attacks contained internal information. The third assessment is that this campaign was carried out for the purpose of destroying and damaging critical infrastructure. It is important to note that currently there are no definite findings supporting this, but at this stage it cannot be ruled out.

Several days after the attack on Norsk Hydro was reported, American chemicals companies Hexion and Momentive revealed that they too fell victim to a LockerGoga ransomware attack. The two companies, who are controlled by the same investment fund "Apollo Global Management"[6] both suffered an attack on March 12; six days before the attack on Norsk Hydro.

[4] https://www.computing.co.uk/ctg/news/3072839/norsk-recovers-some-systems-following-confirmed-ransomware-breach ,https://www.nozominetworks.com/press-release/nozomi-networks-expands-ics-cyber-security-research-with-labs-launch/
[5] https://twitter.com/JusticeRage/status/1109065147186847745?s=08
[6] https://www.apollo.com/

Cyber Attacks On The Global Finacial Sector

Central Bank of Malta Breached - likely a SWIFT Attack; Loss of 13 Million Euro

On February 13, 2019, the central bank of Malta (BOV), which also operates as a commercial bank for half of Malta's population, identified that it fell victim to a cyber attack, which resulted in a loss of €13 million.[7] Note that the attack was detected by anti-fraud systems, and not by the security systems. Immediately after detecting the theft, the bank decided to shut down all of its systems: ATMS, credit card payment terminals, business owners' equipment, email and telephone services, their website, even shutting down all of their branches in Malta. The shut-down was in effect until the attack was neutralized and the affected systems were recovered.

The exact date during which the attack was executed is unclear as of early March. Nevertheless, it should be noted that since the bank did not report that it was able to retrieve the stolen funds, the attack was most likely carried out at least three days prior to the reveal (On February 10th, when the bank is closed). During the attack, 11 transactions were carried out, most likely via the SWIFT system, to accounts in the US, UK, Czech Republic and Hong Kong. The sum of the transactions amounted to 13 million euros. Also, worth mentioning is that the finds were transferred to Western countries. This is interesting as usually attackers try to transfer money to countries with less adequate monitoring systems.

The indirect damage included total shutdown of the bank's services for over 24 hours – a situation which hurt all its clients and credit card companies. Also, a significant amount of business owners use the bank's services, and their systems were shut down as well. The bank stated that its clients were not affected, as their funds and accounts remained unchanged. It also stated that it is working to "clean" its systems, and to bring back its services back to normal. On February 14th, the app and website returned to full activity. This attack (the first of its kind in 2019) is reminiscent of Russian and North Korean attack groups' ongoing attacks on core banking systems. Similar to other cases, these groups choose to attack banks in countries with inadequate security systems.

Large-Scare Spoofing Campaign Impersonating Major US Banks' IP addresses

A report published in late April revealed a large-scale spoofing campaign targeting US banks. According to the researchers, this campaign was detected due to heavy internet traffic caused by broad scans of the internet. More interesting however

[7] https://www.maltatoday.com.mt/news/national/92964/bank_of_valletta_shuts_down_operations_following_cyber_attack_#.XGew2yuWXDu

is that the scans were conducted via spoofed IP addresses of big U.S. banks including JPMorgan Chase, Bank of America and SunTrust.[8] Currently the reason behind this is unknown, but CyberScoop conjectures that this was executed in order to disrupt the banks' security teams and cyber security companies' ability in mitigating malicious activity.

The campaign appears to have taken place between April 19, 2019 – April 23, 2019. The spike in traffic-spoofing started on Friday the 19th and continued until late Tuesday the 23rd.

Analysis of the attack

According to Security researcher Andrew Morris, the volume of traffic is too low to be a DDoS attack. Instead he claims that it is possible that a malicious actor attempted to fool firewalls and other security products into blocking traffic originating from the banks, with the purpose of embarrassing security vendors. Further, while Traffic spoofing are common attacks, they rarely target specific entities, as was in this case. A list of the spoofed IP addresses was uploaded to Pastebin but has since been removed.[9]

Initial investigation, conducted by BRICA (Business Risk Intelligence & Cyberthreat Awareness), indicates that the attackers sent spoofed TCP packets, but made no attempt to complete the three-way-handshake. This was because they only attempted to flood security vendor with false positive. With that in mind, based on this incident, security vendors could use this attack in order to better their monitoring and blocking rules for each of their clients.[10]

Mitigating such attacks is problematic and complex. If a security service or product blocks internet scans, you should verify that the blocked IP addresses are the source of the scan. Note however that this is not an option with of SYN() and FIN() packets. It is possible to create whitelists in order to prevent false positive, however it should be taken in to account that it is impossible to create a global whitelist.

Chile-based Interbank Network Redbanc Attacked

Redbanc is a Chile-based company responsible for connecting the ATMs of all the banks in Chile. On December 2018, the company was attacked using the PowerRatankba malware, affiliated with the North Korean APT group Lazarus. Findings about the malware family were published on January 15th by Flashpoint.[11]

The Lazarus APT group is commonly associated with Bureau 121 – the cyber warfare unit of the North Korean regime. The group gained publicity thanks to its aggressive worldwide campaigns on 2009. It specializes in attacks targeting financial institutions and services, including banks and cryptocurrency exchange platforms, many of them in South America and East Asia.

The attack begun when in IT expert at Redbanc was infected by malware after opening on a message that was sent to him via a social media platform, probably LinkedIn, allegedly containing a job offer. Upon clicking the link to apply for the job, the IT expert was referred to a decoy job application page. To gain the victim's trust, a Lazarus representative had a job interview in Spanish with the expert. A day later the company announced it had been breached.

Apparently, while attempting to apply for the job the victim downloaded a file called ApplicationPDF.exe' seemingly a recruiting software. The executable is included in ThreadProc and SendUrl processes, which process parameters encoded in Base64 and run the malicious code. The downloaded file decoded the parameter code encoded in Base64, communicated with the server and run the PowerShell code in a hidden window. During the infection process, another PS

[8] https://www.cyberscoop.com/spoofed-bank-ip-address-greynoise-andrew-morris-bank-of-america/
[9] https://web.archive.org/web/20190422210240/https://pastebin.com/LrKKam3y
[10] https://brica.de/alerts/alert/public/1256953/recent-bank-ip-address-spoofing-exposes-problem-with-how-some-threat-feeds-are-generated/
[11] https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/

script is executed that decrypts a script created by PowerRatankba. The malware serves as a both a downloader and a spyware, in charge of collecting information to be used in further attacks by Lazarus.

Attack on British Metro Bank Exploiting a Vulnerability in the Two-factor Authentication System

On February 1st, it was reported that UK's Metro Bank has fallen victim to a sophisticated attack that bypassed the two-factor authentication (2FA) by exploiting a SS7 vulnerability. The authentication system sends SMS messages with codes for confirming clients' financial transactions. It appears that the attackers reached clients' devices **by remotely tracking devices and monitoring clients' SMS messages that request confirmation for transactions.**

SS7 protocol is used for routing calls and SMS and is used by telecommunication firms worldwide. By exploiting a vulnerability on the protocol, attackers are able to intercept messages and thus obtain clients' location and personal information through their cellphones. Metro Bank stated that only a few clients were affected, and no one lost money from their accounts. Metro Bank is cooperating with the relevant communication providers and the authorities to investigate the attack. The bank advises its clients to be alert and report any activity which seems suspicious.

European Banking Authority Report on SMS 2FA-Based Financial Transactions

Following the attack the UK National Cyber Security Center stated that exploiting such vulnerabilities is a known method which has already been used previously. It is a common attack vector used in fraud campaigns and in cellphone espionage attacks. The website InfoSecurity reviewed a similar attack which took place in May 2017, and assessed that using SMS messages for 2-Factor authentication is no longer reliable identification method. It is recommended to use authenticator apps or Time-based One-time Password algorithm (TOTP) for 2-Factor Authentication in order to avoid such attacks[12].

Furthermore, in June the European Banking Authority (EBA) recently published an opinion report on the elements of strong customer authentication systems for financial transactions. Below is an excerpt regarding SMS-based 2FA authentication.

"*As stated in the EBA Opinion on the implementation of the RTS (paragraph 35), a device could be used as evidence of possession, provided that there is a 'reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device'. Evidence could, in this context, be provided through the generation of a one-time password (OTP), whether generated by a piece of software or by hardware, such as a token, text message (SMS) or push notification.* ***In the case of an SMS, and as highlighted in Q&A 4039, the possession element 'would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number'***"

Below are the 2FA alternatives suggested by the EBA (note – most relay on biometric identifiers).

[12] https://www.infosecurity-magazine.com/news/flaw-in-ss7-lets-attackers-empty/

Table 1 — Non-exhaustive list of possible inherence elements

Element	Compliant with SCA?*
Fingerprint scanning	Yes
Voice recognition	Yes
Vein recognition	Yes
Hand and face geometry	Yes
Retina and iris scanning	Yes
Keystroke dynamics	Yes
Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices)	Yes
The angle at which the device is held	Yes
Information transmitted using a communication protocol, such as EMV® 3-D Secure	No (for approaches currently observed in the market)
Memorised swiping path	No

*Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.

Despite this report, several large banks in Germany have already began implementing stronger 2FA authentication process for financial transactions, phasing out the less secure SMS-based systems.[13] These new measures have been strongly pushed by European regulators in recent years.

SMS Transaction Authentication Number (aka SMS-TAN, or mTAN) is the most commonly used method by banks to authenticate financial transactions by issuing temporary passwords via SMS messages.[14] Attackers however have been manipulating this procedure to unlawfully execute transactions from bank customers. Cryptocurrency companies have also suffered from these attacks, losing tens of millions of dollars in recent months alone.

Accordingly, over the last few years various governing bodies (such as the German BSI - Federal Office for Information Security) have warned financial institutions and customers from using this technology. The most attack vectors are phishing or sim swapping.

New verification methods

Below are the new methods employed by German banks to verify transactions:

- ChipTAN – issuing Tokens by the bank to verify transactions.
- PhotoTAN – mobile apps that provide a unique barcode to work in conjunction with the SMS messages.
- PushTAN – verification via an app operating as a Token. For example, Google authenticator and Microsoft authenticator. It is unclear whether this method meets the European Banking Authority standards.
- Digital Signature – using smart encrypted cards.

65 Million USD From a Bank in Kuwait

In late March, rumors began spreading on Twitter about a 65 million USD theft from a bank in Kuwait via its SWIFT system. However, as of early July, no official announcement had been published by any bank. Over the course of the last few weeks we have been tracking the case via social media, bank portals and VirusTotal, in which we used to detect malicious files uploaded from Kuwait. Related indicators and rumors that the bank in question is the Gulf Bank of Kuwait were revealed in Twitter. The bank published a statement on March 27 claiming its systems had run into technical difficulties that damages its international money transfer system (probably the SWIFT system). No cyber-attack was mentioned.

[13] https://www.helpnetsecurity.com/2019/07/12/german-banks-sms-tan/
[14] https://en.wikipedia.org/wiki/Transaction_authentication_number

Cyber Attacks On The Fin-Tech and Crypto Firms

Advanced Spy-Malware Campaign Targeting FinTech Companies

On March 19th, Palo Alto's research team Unit42 revealed a new attack campaign against FinTech firms via an espionage malware (RAT) named Cardinal RAT. The campaign probably occurred over the last two years and was first detected in January 2019.

Malware Analysis

Cardinal RAT malware family was first identified in 2017 when Unit42 exposed a limited attack campaign (27 known samples). Since then, the research team continued to monitor the malware and recently identified a new version (1.7.2) with several changes, including advanced obfuscation functions which hinder detection and analysis.

The main obfuscation technique is based on steganography which obfuscates malicious content inside an embedded Bitmap (BMP) image file. When the .NET based malware is executed, it extracts a malicious DLL file from the image's pixels. It then deciphers it with a single-bit XOR encryption key.

Like previous versions, Cardinal RAT has many capabilities:

- Data collection on the infected system.
- Changing system settings.
- Executing commands remotely in the infected system.
- Downloading and executing files without permissions.
- Exploiting the infected system as a reverse proxy.
- Downloading updates to the malware.
- Retrieving passwords.
- Keylogging and screenshot capturing.
- Erasing cookies from browsers.
- Deleting the malware from the infected system.

Possible link to EVILNUM malware & attack vector

When the researchers examined the samples uploaded to VirusTotal, they identified a possible connection to a malware family named EVILNUM; a JavaScript based malware that collects information and achieves a foothold in the systems and

networks before using Cardinal RAT. Note that this malware was identified in only a small number of firms, similarly to Cardinal RAT.

In the campaigns of both of the malwares, the infection vector was carried out with a malicious phishing document which were very similar to one another. This document usually contained lists of names and numbers (the type of numbers was not mentioned, but possibly telephone numbers) of people who work in the forex and cryptocurrency sector.

Cryptocurrency Attacks 2.0

In late 2017, the cyber security community watched in awe as Crypto Mining malware, most notably web-based scripts, took the world by storm and climbed to the top of various Global Top malware charts. The frenzy begun with the infamous case of The Pirate Bay. The Pirate Bay is the world's largest BitTorrent indexer – it is a massive online source for digital content including movies, games and software.

Shortly after the first web-based Crypto Miners spurred, it has been discovered that The Pirate Bay had planted a crypto mining JavaScript that secretly utilizes the website visitors' computer resources to mine the Monero Cryptocurrency while visiting the portal.[15]

Website owners nowadays depend on advertising revenue to survive; however the user experience can be highly interrupted by the appearance of multiple advertisements on the content page. The birth of JavaScript-based crypto miners offered another solution – instead of burdening the users with flashy ads, a website owner can simply embed a JavaScript within the website html page which mines a cryptocurrency using the visitor's CPU power and generate a respectful revenue. While this tactic sounds effective, to separate it from malicious activities carried out on the user browser unknowingly such as browser hijacking, transparency is required.

It is expected of a website owner to notify its visitors that an alternative process is taking place in order to spare them the inconvenience of online advertisements. Unfortunately, the simplicity of the use of the script, which only required embedding, rather than distribution and infection, led to giant wave of hackers that exploited legitimate, high profile websites to embed a web-based Crypto Miner without the website owner's knowledge.

Unlike website owners, attackers use as much as 90% of the user's CPU power to mine cryptocurrency. Top websites exploited for mining in the past include a Los Angeles Times website and a Jerusalem Post website, as well as 4,000 government websites in the US, UK and Australia.

The success of web-based crypto miners was boosted by two key trends:

1. The sharp rise in the value of many cryptocurrencies. The first cryptocurrency that gained popularity and led to a significant market growth was BitCoin. Its popularity led to the development of many additional digital currencies such as Ethereum, Monero and Litecoin. Monero is often preferred by attackers due to the relatively lights resources required to mine it.
2. The rise in the required resources. As time passed and crypto mining gained popularity, the computational resources needed to mine new crypto coins grew higher. Specialized hardware, or a mass number of personal computers combined became a necessity.

After a long period of Crypto Mining malware, especially web-based scripts, dominating the cyber landscape, it seems safe to say that the golden age of this type of attack is behind us. As 2018 progressed, the prices of BitCoin and along with it

[15] https://thehackernews.com/2017/09/pirate-bay-cryptocurrency-mining.html

most other coins, fell significantly, rendering the process of mining it unprofitable. As always, cyber criminals found another way to leverage the cryptocurrency market for monetization, taking the attack to the next level.

Lately, we have been observing a new vector of attack leveraging cryptocoins - Cryptocurrency exchange attacks. Prominent attack vectors used recently to target Cryptocurrency Exchanges are the following –

1. Distributed Denial of Service (DDoS) attacks, capable of shutting down the entire trading activity of the exchange for a limited time thus preventing transactions, lowering the value of the coins and damaging the reputation of the portal. In June 2018, one of the most prominent cryptocurrency exchanges suffered a DDoS attack that ceased the activity of the exchange for three hours.
2. Phishing attacks – simple yet effective, phishing attacks can be useful in this case as well. Using tailored content, attackers could lure an employee into granting them access to the exchange network, thus enabling information and credential theft.
3. Transaction malleability attacks, in which the attacker alters the transaction ID of a BTC transaction and uses it to carry out a transaction of his wish. If attackers are able to change a transaction ID without invalidating it, they could perform a transaction of their own from the sender's wallet. The sender would think that the transaction has failed, when in fact, it had already taken place before the failure.
4. Online Wallet attacks – wallets that are connected to the internet are often offered by exchange portals for secured storage of private keys of cryptocurrencies. while many of them state they use offline resources to store the keys it is not always the case, making them a tempting target.

Binance Data Breach leads to Theft of 40 million USD

In May 2019, some 40 million USD worth of BitCoins were stolen from one of the most popular coin exchange portals, Binance. The company admitted that 7,000 BitCoins were stolen from its storage, and that the attackers managed to bypass two-factor authentication processes. Binance is considered as the biggest cryptocurrency exchange in the world in terms of trading volume.

Shortly after in June 2019, the Singapore-based cryptocurrency exchange, Bitrue, reported a massive data breach which led to losses of 4.5 million USD from customer funds. The hacker exploited a vulnerability in the company's security procedures to steal private wallet information and to collect coins from approximately 90 wallets.

32 million USD Stolen in a Breach of the Japanese Exchange BitPoint

Just recently one of the biggest cryptocurrency exchange hacks took place as 32 million USD worth of cryptocurrency were stolen from the Japanese exchange BitPoint in July. At least 23 million USD worth of coins were customers funds, and the company admitted that coins were stolen from both its "hot wallets", used for trading, and its "cold"; wallets, which are used for secured storage and should be much less accessible.

Lastly, as of May 2019 ClearSky has been investigating a newly-discovered extensive operation which targets Cryptocurrency exchange portals using quality spear-phishing techniques. The attackers use misspelled domains carrying the names of Google and Amazon services to lure its targets into visiting their pages, as well as well-written and designed Word documents with the logo of the attacked exchange and matching content, or alternatively, some general information about cryptocurrency trading.

The Word files we found were password protected, but the password was attached inside the zip folder in a txt file. Upon execution, the Word file reaches out to a URL shortened via the bit.ly service. Then, after gaining access to machines within the cryptocurrency exchange network, we believe that multiple actions are conducted to steal as much funds as possible from the exchange, causing immense damage to the company.

ClearSky Investigation – Operation CryptoCore: Attack Infrastructure Targeting Crypto Firms

As part of our ongoing investigations we detected in May a password protected word file that references the cryptocurrency exchange HitBtc[16]. We found that it is most likely part of an infrastructure that contains numerous addresses, domains, and sub domains with similar properties:

- All the domains we detected in the infrastructure are disguised as Google services (drive, mail, sheets, docs) and are written with spelling mistakes.
- Most of the Doc files communicate with the URL shortening service bit.ly, most likely in order to try to conceal the communication attempts.
- In the address line, after the TLD this routing always appears: -*. 8080/open?id

At this stage the penetration vector is unknown. When we pivoted the domain and the address it is stored on, we reached other domains and addresses which share identical properties.

As of now analysis of the files did not reveal the attack vector, but we can infer that it is based on a large and dedicated infrastructure. We recommend adding the attached indicators into the organization's monitoring systems. Moreover, since the domains have names that appear legitimate but are actually malicious, we recommend presenting them to employees, and make sure they are mindful of the links they open.

Additional files

In early July we identified new IP addresses attributed to this infrastructure. After carrying out additional investigation, we detected an empty word file sample that communicates to the domain named service[.]amzonnews[.]club, which is hosted on a server with the address 75[.]133[.]9[.]84. The file named "Introduction to the World Blockchain Association.doc", was uploaded to VirusTotal from Brazil on June 26th, and was identified as malicious by 5 antivirus engines.[17]

[16] https://hitbtc.com/
[17] https://www.virustotal.com/gui/file/583cf86894e47a81fa914fdc46fa6587807cf17f9196160625b149d47560f9b0/submissio

The Digital Cold War

The Deterrence theory, which gained prominence during the Cold War, states that an inferior force, with lower destructive capabilities, could deter a more powerful adversary as long as it maintains the ability to protect itself against a surprise attack. It is based on the fear from reprisal, and as such, the deterrent weapon must be ready, but not necessarily used in full force.

In the summer of 2017, a unique malware has hit the industrial safety systems of a petrochemical plant in Saudi Arabia.[18] The malware was designed to manipulate the Triconex Safety Instrumented System (SIS) – by altering the system controllers to a failed safe state the entire industrial system automatically shuts down.

The SIS controllers are the last line of defense against physical disasters in Industrial Control Systems, meant to kick in if danger is detected. Therefore, their proper detection capabilities are a key to the function of the entire system, and if they are not intact, real danger is posed to the facility employees and surrounding. Considering the dangers petrochemical plant poses, makes the malware even more of a milestone in the cyber threat timeline. Dubbed Triton, in late 2018 the malware was attributed to a Russian Government-Owned institution – The Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM).[19]

While the security community had been made aware of the threats posed to Industrial control systems, Triton follows a small number of publicly exposed incidents in which a malicious software successfully infected an Industrial Control System. The most recent one would be Industroyer, which targeted Ukraine's power grid and deprived a part of Kiev of power for an hour. Some believe that the implementation of the malware was a test, in preparation a real need. Industroyer followed the Notorious Stuxnet, that in 2010 damaged Iran's centrifuges in the process of separating nuclear material.

The first half of 2019 demonstrates that The Deterrence theory is now more relevant than ever, with a new weapon in its core – a full-power SCADA attack; the ability to cripple a national infrastructure by sabotaging its core systems, thus preventing its civilians and leaders from accessing vital services and perform, daily functions.

In March 2019, it has been reported that the authors of the Triton malware are now on researching additional targets in North America and other parts of the world.[20] While a big SCADA attack has not been observed, the attack timeline detailed above makes it clear that it is only a matter of time until a radical move in the global political sphere will lead to a precedent. It is now clear that an expanding number of entities, most of them government-backed, are possessing or in the development process of malware capable of affecting such infrastructure.

[18] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
[19] https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html
[20] https://dragos.com/resource/xenotime/

Just like the nuclear deterrence theory, we believe that powerful countries – notably Russia and the United States – are now realizing that possessing such abilities, mainly on the systems used by their adversaries', as a key part of the up-to-date global deterrence equation.

The escalation of the digital cold war

Cyber espionage capabilities have been a key part of silent, under the radar battles between power countries, including the United States and Russia, for quite a few years now. For example, the infamous Stuxnet malware uncovered in 2010 is said to be a part of a joint Operation between The Unites States and Israel against Iran's nuclear program. In 2014, Ukraine suffered a massive cyber-attack targeting its government networks, as well as a cyber attack against Ukrainian Army's Rocket Forces and Artillery. Both of these attacks have been attributed to Russian actors.

Russia

Russia is known for its use of cyber espionage, Denial of Service (DoS) and destruction tools as part of its territorial and political conflicts – the diplomatic row with Estonia in 2007, the Russo-Georgian War in 2008 and the Russian military intervention in Ukraine as of 2014.

There is no doubt that the key turning point in the Russia-United States cyber dispute was the 2016 United States presidential elections. In 2015 an attack against the American Democratic National Committee (NDC) led to the leakage of almost 20,000 private emails.[21] It was shortly followed by additional exfiltration attacks to the Democratic Congressional Campaign Committee (DCCC), and Clinton campaign officials. These acts is affiliated with Russia's Main Intelligence Directorate, commonly known as the GRU. Russian institutions are known for their vast interference in the 2016 elections with the goal of harming the leading democratic candidate, Hilary Clinton, and boosting the president Donald Trump.

The main vector of intervention observed around the elections is undoubtfully disinformation campaigns, mostly referred to as 'fake news'. On the months prior to the elections, Russian companies and activists carried out an immense operation social media campaign meant to distribute their propaganda. The campaigns used thousands of designated fraudulent social media accounts and online advertising space to promote events in support of Trump, radical political groups and Clinton opponents. These accounts were managed by a troll farm disguised under the name The Internet Research Agency (IRA), most likely linked to the Kremlin.

Although the Russian interference actions were widely investigated by the United States Congress and the FBI, similar acts took place again on the 2018 presidential mid-term elections. However, this time, the United Scape Cyber Command responded with an offensive campaign against the IRA.[22] The operation rendered the farm entirely offline during Election Day and is considered one of the most aggressive publicly reported campaigns launched by the Cyber Command.

In late 2018, ClearSky investigators revealed an extensive and well-managed Iranian disinformation infrastructure used by the to distribute modified content in over 28 countries[23]. The Russian disinformation campaign filled an important role in the global cyber landscape, as it raised great awareness to the unprecedented impact of fake news campaigns. In 2019, we can clearly state that the public knowledge of the presence of fake news on all social media channels is as high as it could be.

The Cyber Command's takedown on the IRA marks a milestone in the history of cyber. However, the first half of 2019 marks in ever greater escalation in the use of cyber warfare as part of the United States-Russia tension. For the first time, Trump administration officials reported that US software code was deployed inside Russia's power grid and other targets.[24] While

[21] https://www.wired.com/2016/07/heres-know-russia-dnc-hack/
[22] https://www.theverge.com/2019/2/26/18241600/us-cyber-command-russian-troll-farm-attack-election-day-2018
[23] https://www.clearskysec.com/global-iranian-disinformation-operation/
[24] https://www.independent.co.uk/news/world/americas/us-politics/us-russia-cyber-attacks-trump-power-grid-putin-kremlin-a8960681.html

the operation is meant to display power and warn President Vladimir V. Putin, the Kremlin states that this act means there is a hypothetical possibility of a cyber war.

To conclude, the below examination of the change in the United States-Russia cyber conflict demonstrates that cyber warfare acts, whether committed by hacktivists or nation-sponsored groups, have become an actual possibility, and an integral part of the civilians' everyday lives.

China

China has been implementing aggressive political and economic moves in recent years with the aim of becoming the world's leading power country within the next decade. Three prominent Chinese programs in this regard are the following:

- Made in China 2025 – An aggressive government program that promotes the development to a China as a high-tech power country by developing, manufacturing and purchasing local technologies.[25]
- Belt and Road (aka 'One Belt, One Road') – A government program that promotes the development of road and rail infrastructure across 152 countries in Asia, Europe, Africa, and Latin America. This project has been criticized by many parties around the world who claim corruption and exploitative conditions affecting long-term countries, as well as blatant use of the project to promote Chinese interests around the world at the expense of various countries. For this reason, this program was called Debt-trap diplomacy.
- World Leading Programs in the development and supply of 5th Generation Mobile Internet Technologies - 5G.

In light of these plans, we have seen a spike in Chinese APT attack campaigns targeting the private, political and security sectors worldwide as of 2018. In this context, we must mention the infamous supply chain attack against HP and IBM carried out by APT10, the theft of sensitive British and US government military documents from military suppliers and the theft of advanced commercial developments from technology companies and academic institutions around the world.

In October 2018 a long-term espionage campaign which took place from 2010 to 2015 was unveiled by the Chinese government's intelligence agency - MSS (Ministry of State Security).[26] During the campaign at least 12 aerospace technology companies were hacked. Among other things, intellectual property had been stolen with the aim of assisting Chinese government companies in developing a new jet engine. This incident is one of many industrial espionage activities carried out by Chinese actors in an attempt to gain intellectual property from Western companies to promote Chinese produce.

One of the major events, which is still ongoing, is the confrontation between the US government and the Chinese telecommunications company Huawei. This confrontation includes the arrest of Meng Wangzhuo - CFO and daughter of the company's founder. This happened in tandem with the imposition of trade restrictions with Huawei, which could disrupt the international operations of a company's cellular and computer divisions, and lead to 30 billion USD in losses. In parallel to these events, both countries have declared protective tariffs on hundreds of billions of dollars in import and export. As of mid-July 2019, these restrictions are planned to be removed, but the company's future is still unclear. [27]

It is important to remember that most large Chinese companies have close ties to the CCP (Chinese Communist Party). When it comes to Huawei, founder and CEO of Ren Zhengfei is a party member and is closely related to state president Xi Jinping. Accordingly, every action Huawei does is primarily aimed at promoting China. Although officially Huawei and other Chinese companies such as ZTE are private companies, the US government has defined them as "an arm of the Chinese government".

[25] https://www.forbes.com/sites/marcoannunziata/2018/08/10/seven-steps-to-success-or-failure-for-made-in-china-2025/
[26] https://www.justice.gov/opa/press-release/file/1106491/download
[27] https://gizmodo.com/huawei-still-on-commerce-department-blacklist-reporte-1836359551

In October 2018, Bloomberg Businessweek magazine published an article stating that China has installed spyware on 30 major Western technology companies, among them Amazon and Apple.[28] All companies involved have denied this claim and at the same time no additional evidence has been revealed. Due to the vast dependency of Western companies in manufacturing in China, this concern seems to be pointing to a probable espionage vector. In light of this, in August 2018, the US government banned operational civilians and soldiers from wearing wearable technology, including smart watches, which could collect information such as location, record Audio or take pictures.[29]

Middle East and Gulf Countries

The escalation in the use of cyber warfare tactics by power countries can also be observed in other regions of the world, and is integrated in political conflicts worldwide. An example of this is the crash of a UAE military spy satellite launched by the European Space Agency (ESA). This incident, which occurred last July, is still under investigation. However, preliminary findings suggest possible tampering.

Additionally, Russian military activity in Syria involving GPS jamming has begun to hit the Middle East and Israel airspace over the past year. Intelligence agencies estimate that Russian cyber operations are not aimed at Israel, but still pose a security risk due to its proximity to the conflict area and tensed status with Syria. It should be noted that, as of July 2019, these disruptions only affect civil systems and do not affect Israeli military frequencies operating used by secure and encrypted networks.

Conclusions

To summarize, the escalation of the cyber conflict between the United States, Russia and China may lay the foundations for a future cyberspace war. Whether it is a state-of-the-art technology institute or highly motivated hackers, the beginning of 2019 introduces a rise in the use of cyber warfare tools and an increase in the rate of the references to this arena in the global daily discourse.

[28] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
[29] https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/

Russian and Chinese APT Cyber Activity

Russian APT activities

Law Enforcement Operations - What Doesn't Kill You Makes You Stronger

One of the most notorious APT groups of our time is the FIN7 hacking group, and for a good reason. It is estimated that the actor has managed to collect over a billion USD from companies worldwide, and over 12 million credit card numbers from thousands of businesses. Top countries impacted by the theft operations are the United States, Australia, the United Kingdom and France, and among the hacking group's victims are major companies such as Chipotle Mexican Grill, Arby's. Saks Fifth Avenue and Emerald Queen Casino.

The FIN7 group has been around since at least 2015 and has been conducting large-scale, quality payment card data theft operation. Their monetization technique is based mainly on a prominent card shop. Attacks carried out by the group usually target Point-of-Sale (PoS) systems, however, when a targeted organization uses systems secured with end-to-end or point-to-point encryption layers, the group often attacks the finance department within the organization network.

FIN7's persistence and prominence in the cyber landscape can be credited to their innovative and adaptive nature – the group often alters its attack techniques, such as the file type of the attachments sent as part of phishing campaigns, or the file extension of the files launched afterwards as part of the infection. Their malware campaigns are usually initiated by a tailored phishing email sent to a company employee, which includes an attachment. The email would include business-relation content that would require the recipient to open the attachment in order to receive details about the inquiry. Emails are sometimes accompanied by supporting phone calls.

Another key step taken by the group to ensure the success of their campaigns is the use of digital certificates. By signing their decoy documents with legitimate certificates, the group is able to bypass many security controls. This supports multiple evasion techniques taken by the group, such as changing obfuscation types, AV engines coverages tests and more.

Surprisingly, on August 1st, 2018, the United States District Attorney's Office for the Western District of Washington uncovered that several individuals suspected of being in leadership positions within the FIN7 cybercrime group had been arrested. All three of them - Dmytro Fedorov, 44; Fedir Hladyr, 33 and Andrii Kolpakov, 30, are Ukrainian nationals. They

were charged with 26 felony counts of alleged aggravated identity theft, wire fraud, computer hacking, access device fraud and conspiracy.

Despite the major takedown step taken by the United States authorities against the alleged group leaders, it appears that the group has not ceased action. Researchers reported recently that since the arrest, FIN7 has targeted approximately 130 companies worldwide using spear-phishing campaigns and delivering the GRIFFON malware, a JavaScript backdoor. In this case as well, campaigns operations were able to gain the trust of their victims using well-written, business-related content.

The group runs a seemingly-legitimate operation which includes the of fake companies to hire professionals such as vulnerability researchers and penetration testers. Evidently, their procedures are organized enough to enable them to continue functioning even without their leaders. It has a clear purpose, a successful record and a drive – to generate the greatest revenue, keep avoiding detection and utilize new social engineering tactics, unfamiliar to the business sector employees.

Another notable case demonstrating the persistence of APT groups is revolving around the OilRig group. In March 2019, the actor suffered a great data leak as part of which hacking and espionage tools, as well as C&C components, target lists and strategies. However, no signs of an operation shutdown were observed, and researchers believe that the group will continue acting against targets in the middle east and worldwide, while developing a brand-new toolset.

Both cases teach us in the cyber security community that sometimes, separating the leaders from the group is not enough to stop a powerful cybercrime infrastructure from functioning. Over the past few years, professional APT group such as the Russia-oriented APT28 (Sofacy), the Iran-oriented OilRig and FIN7, have established their presence in the cyber landscape, generating massive damages to businesses and government organizations worldwide. While we expect to see more takedown attempts by state authorities against these groups during 2019, we also believe that these arrests alone are not enough.

Threat groups APT28 and Sandstorm Targeting European Governments

Russia's interference with political procedures worldwide in the cyberspace is on the rise. The first notable incident, which made headline and raised public awareness as for the Russian involvement in the political landscape, was the infamous data leak from the Democratic National Committee prior to the 2016 presidential elections on the United States. The hack, in which almost 20,000 sensitive emails were made public, is attributed to the Sofacy group, also known as APT28 – a group linked to the Russian military intelligence agency GRU. This hack was followed by aggressive fake news campaigns spread throughout the social media, which promoted the Republican candidate, Donald Trump.

Another noteworthy attack targeting a political entity is the NotPetya ransomware attack which took place in June 2017. In this attack, government offices, banks, a city airport and even the power utility of Kiev were severely attacked by a new, fast-spreading type of ransomware later dubbed NotPetya. The malware features were significantly based on the NSA tools leak. The attackers, most likely the Russian government-backed group Sandworm, infected the update servers of a popular software business in Ukraine and propagated via its software updates.[30]

In the first half of 2019, we are witnessing the continuance of this line of action, as both APT28 and Sandworm had targeted European government-related institutions with spear-phishing emails ahead of the European Parliament elections in May 2019. Researchers reported that emails containing links to seemingly-legitimate websites were sent to government personnel across Europe in order to lure them into changing their passwords and thus providing their credentials to the attackers. Similarly to the United States attack, the attacks primarily targeted democratic institutions in Europe, but

[30] https://securelist.com/apt-trends-report-q1-2019/90643/

election campaigns, think tanks and non-profit organizations promoting agendas related to democracy and public policy were also attacked.

Fake Software Update Used in a Turla APT Campaign Against Government Targets

In January this year, ESET investigators tracked a new espionage campaign by Turla, a government-backed Russian group that has been operating since at least 2014 against former USSR countries.[31] As part of the campaign, the group used social engineering to convince its targets to download and run a supposedly legitimate Adobe Flash Player containing a Backdoor. The victims think they are referred to the official Adobe site to download a legitimate update, but in reality the traffic is redirected to the attacker's server and behind the scenes a malicious file is downloaded. According to the report, most of the targets were political factors.

Researchers ruled out the option that Adobe's official servers were hacked and used for malware download. They speculate that MitM (Man in the Middle) attacks were used as part of the attack chain. There are several ways that may constitute Turla's attack vector:

- Local MitM - Using enterprise machines that are already under the Turla's control as an intermediary between the victim machines and the server that stores the malware, by performing ARP Spoofing.
- MitM on the gateway of the attacked organization - Interception of the entire organization's traffic through utilization of the corporate gateway rather than through specific stations.
- MitM at the ISP level - the group's intervention takes place outside of the attacked organization's network. There have been previously reported cases of malware distribution using this attack vector.
- BGP Hijacking attack – redirection of traffic by manipulating the routing table, thus altering the route to the ADOBE official servers so that communication passes through a point that belongs to the group.

Once control of the victim machine is obtained, the collected information is translated to Base64 and sent to a domain under the attacker's control. Collected information includes a username, a list of security software installed on the machine and the routing table. Parallel to the malicious activity, inquiries of legitimate Adobe addresses and domains occur, as a means of disguise. Once the infection process is complete, a legitimate Adobe Flash Player version is downloaded and installed, coming from an unofficial source like Google Drive.

In recent months Turla has begun to develop new advanced malware and attack techniques. According to recent findings from July, the group distributes a new Dropper called Topinambour, which performs further malware downloads. It also features data exfiltration capabilities. Turla implements a number of evasion and defense mechanisms. For example, it develops versions of the malware in several different coding languages (JavaScript, .NET, and PowerShell) – Thus, if one version fails another one is executed.

Financial Institutions Attacked by Russian Attack Groups via Cloud Services

At the end of January, Netskope researchers discovered a wave of attacks aimed at some 42 entities linked to the financial sector and government agencies around the world. The attacker, most likely Cobalt Strike[32], used Google Cloud Platform (GCP) to distribute malware through PDF files that were created using Adobe Acrobat 18.0 and then emailed. The company alerted Google on January.

[31] https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf
[32] https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html

In the first stage of the attack, the victims received malicious emails that contained PDF files that were automatically uploaded to legitimate cloud services (Google Drive, for example). The emails were sent from legitimate and reliable sources to lure the victim to open the email and file. The victims then shared the PDF with other users who received it through the cloud services, and therefore found it reliable. The PDF files contained a link to a Word file called "Doc102018 [.] Doc" which contained macros. When the Word file is run, a message pops up that asks the user to enable editing. After the message is approved, a macro file downloads a file named fr.txt is downloaded from the transef [.] Biz / fr.txt address.

Chinese APT activities

The International Civil Aviation Organization Concealed a Major Cyber Attack by APT27

Just recently it was revealed that during 2016, the International Civil Aviation Organization (ICAO) experienced a cyber attack caused by poor management and negligence in the face of the event[33]. The attackers achieved a foothold in ICAO's network for several months, and by attacking ICAO, the attackers were able to reach a Turkish government website. The attackers planted a malware which targets governments and airlines was in two servers. Researchers discovered security loopholes in the network which were neglected. Four employees from the IT department hid evidence and mishandled the incident.

The incident was discovered in November 2016, when a researcher from Lockheed Martin contacted the information Security officer at ICAO to alert them about two infected severs. The researcher stated in his alert that it was a significant event with a high risk against the aviation sector. The ICAO Information Security Officer (CISO) received the alert and instructed to shut down the infected servers. However, the IT team refused to do so, and ignored the request for a long time. The firm authorized a forensic investigation on the severs only after two weeks.

During the whole time since the discovery of the attack, the IT employees did not cooperate with the officer's instructions, and even took out classified information to their homes. A high-ranking official in the company rejected the recommendations to investigate the IT team's performance, and they were even reemployed. The attackers were able to attack foreign government websites through ICAO because of the security loopholes.

The attackers' identity

The researchers assume that the Chinese attack group APT27 (also known as Emissary Panda) is responsible for the attack. The group is known for espionage and attacks against foreign governments, embassies, and technology and defense organizations. They are also known for watering hole attacks by injecting malicious code into government websites.

- The attackers gained 2000 critical systems passwords like email servers and accounts with high permissions (domain admin and sys admin).
- They could read, send, and delete emails from every user in the organization.
- They obtained personal information about all present and past employees.
- They obtained medical information of anyone who used ICAO's health clinic.
- They stole personal and financial information from anyone who visited the ICAO building, or that was even subscribed to the website.

[33] https://ici.radio-canada.ca/nouvelle/1155312/oaci-onu-virus-hacker-cyberattaque-montreal-organisation-aviation

Norwegian Cloud Service Firm Visma Hacked by Chinese Group APT10

Techerati posted details about an attack by the Chinese attack group APT10, which is a part of the CloudHopper attack campaign[34]. The Norwegian firm Visma, which provides cloud solutions for over 850,000 clients around the world, experienced a breach in their network already in August 2018. According to a report posted by Rapid7 and Recorded Future, the attack was carried out by the Chinese attack group APT10[35]. We express doubts about attributing the attack to this group with full certainty.

The attack was designed to attack cloud services to obtain user's information. The attackers stole the login details from Citrix and LogMeIn (used by Visma employees) about two weeks after the first propagation in the firm's network. They then used these login details to distribute a malware which spread to several computers in the firm's network and enabled access to sensitive information.

The attackers used the attack tool Mimikatz (named pd.exe) in order to steal login details. They made use of scheduled tasks via the Microsoft BITSAdmin utility to transfer files from their C&C to the Visma network. Examination of network logs revealed an employee's credentials were stolen and used to authenticate to the network outside of his normal working hours. Throughout August 2018, the attackers regularly logged in to the Visma network during typical Chinese working hours.

Two weeks after the initial intrusion into the network, APT10 implanted their malware, Tochilus. In order to this, they used a C&C server that communicates with Salsa20 and RC4 encryption. After entering into the system, the attackers reached information on the Visma systems by using WinRAR files which were transferred to a Dropbox account. APT10 has already used Dropbox previously.

This attack method raises concerns amongst many companies in the Western world, since they rely on cloud services. Visma's operations and securities manager Espen Johansen told Reuters that the attack was halted before client networks were breached.

[34] https://techerati.com/news-hub/chinese-state-hackers-attack-norwegian-cloud-computing-firm/
[35] https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf

ClearSky Investigations – Analysis of Iranian Cyber Operations

On March 7, 2019, a malicious email was sent to an employee of an Israeli security company which provides products and services to the military and aerospace industries in Israel. The attack was investigated by us in collaboration with additional security researchers. The investigation led us to conclude that the actor behind the attack is the North Korean APT group Lazarus. Lazarus is a threat group operating under the support and supervision of the North Korean regime. The main goal of the group is financial gain and intellectual property theft – Lazarus APT is constantly trying to steal foreign money to make up for the economic difficulties the country has encountered following the imposition of sanctions by Western countries.

The most prominent attacks associated with Lazarus include the Sony Pictures breach on 2014 and the WannaCry destruction attack on 2017, in which the networks and services of giant companies around the world were shut down due to a ransomware. Affected companies include Honda, the Spanish Telephone Network, the UK's NHS (National Health Service) network and the Russian Ministry of the Interior.

The Attack Chain

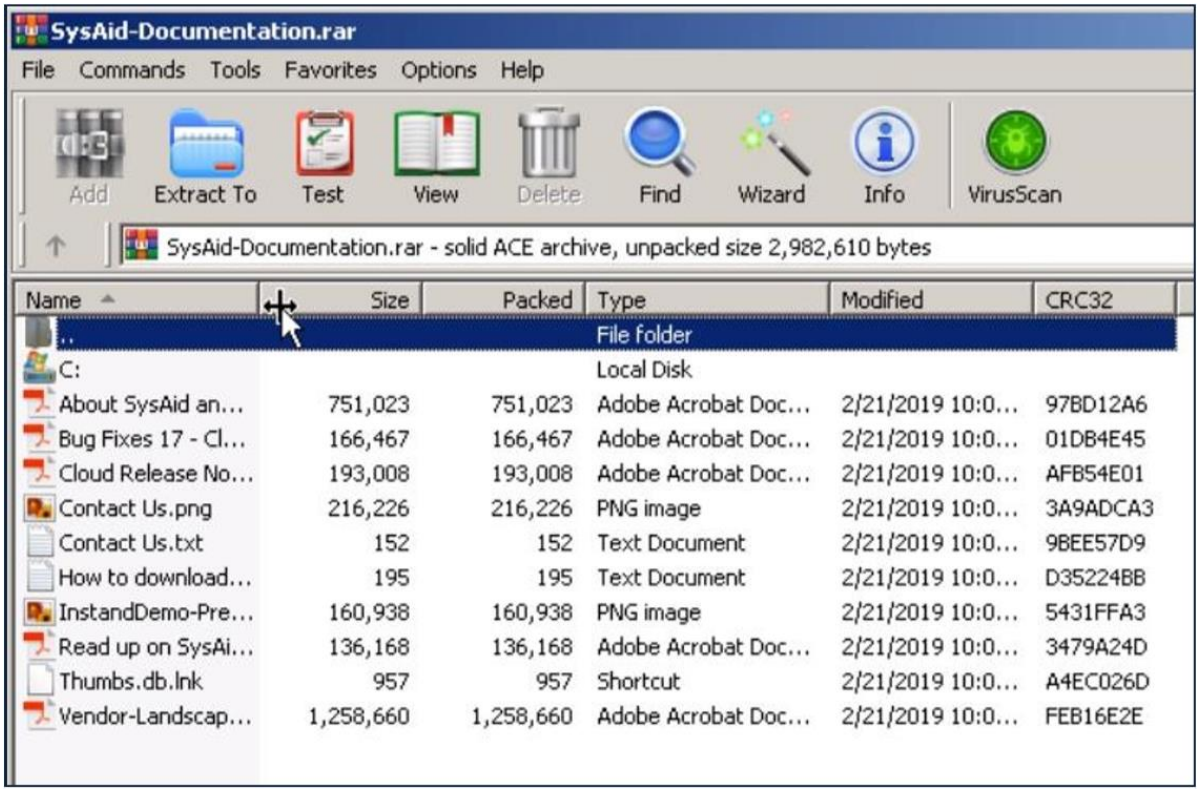
Below is the malicious email sent to the employee:

The message was sent between two employees via organization's internal email system. This meant that the attackers already had gained access to at least one internal email account in the company - and that they were trying to exploit the access he had gained for spreading and infecting computers within the company network. It should be noted that the company's internal network is not connected to its external network, making it even more difficult for an attacker to gain access to the internal system.

Exploiting RARLAB WinRaR – CVE-2018-20250

The email contained the following attachment – SysAid-Documentation.rar (062801F6FDBDA4DD67B77834C62E82A4)

The file exploits the vulnerability assigned CVE-2018-20250[36], which was revealed by Check Point in February 2019. If the archive file is opened using a vulnerable version of WinRaR software, the vulnerability lead to the installation of an executable file (exe) on the machine that could allow an attacker to run a malicious file on a machine using remote access. In the case in question, when the file is opened a Backdoor is installed, which allows the attacker to access the computer.



Malware Analysis

The malware (96986B18A8470F4020EA78DF0B3DB7D4) is a backdoor which functions as a payload on the infected computer. It is a relatively small executable file - 96.5 KB in size. The malware attempts to communicate with a number of C&C servers hardcoded in its code. A malware sample can be found in the following link - https://app.any.run/tasks/64b8f3a9-0c58-4583-8605-78f4faa9ea37/

The following is the list of addresses contacted by the malware to obtain additional commands or to download a second stage malware:

The reaches out to a domain in many cases and to an IP address directly in others. We assess that the attackers did not establish a designated attack infrastructure. Instead, they hacked these addresses and utilized them for the attack. This

[36] https://research.checkpoint.com/extracting-code-execution-from-winrar/

could be a demonstration of the attack method adopted by the group. Using this method, the attackers are spared the need to invest resources in acquiring infrastructure.

The User Agent used by the malware appears to be fake, as it does not match a genuine User Agent - and can therefore be used as an indicator of the malware's malicious traffic:

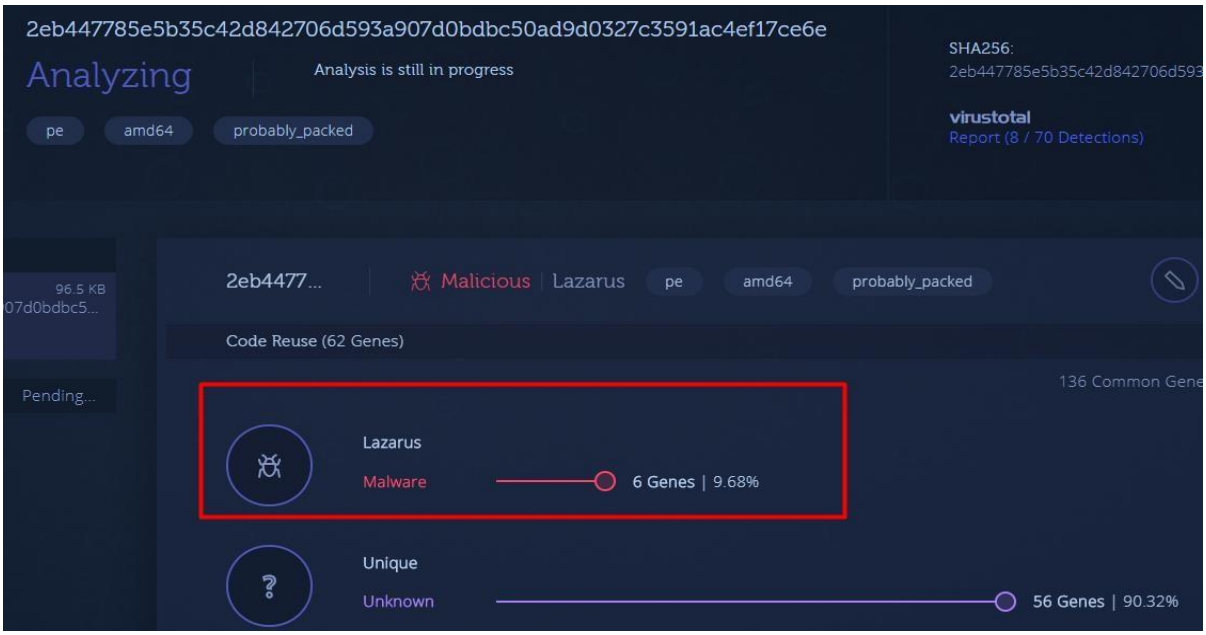
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC&C; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)

Attribution to the Lazarus APT

Based on overlap in code snippets, file structure and file behavior, we believe the malware in question is linked to the Lazarus attack group.

Code Overlap

An examination of the malware in the Intezer system allowed us to detect similarities in the executable code files. The examination revealed a 10% overlap in the code of our malware with a malware known to be used by the Lazarus group.[37]



Intezer also pointed out an overlap between the following two malware samples:

f3bd9e1c01f2145eb475a98c87f94a25

2e17b048c7e317da9024a86d9439c74b

These samples appear in the McAfee report about the Lazarus Group released in December 2018.[38] The report sheds light on an operation dubbed "Operation Sharpshooter" that targeted the security, telecommunications and critical infrastructure sectors worldwide. The campaign took place during October and November 2018 during which 87 organizations from 24 countries were attacked. The purpose of the campaign according to the report is espionage and data theft from the above-mentioned sectors. These attacks were based on the distribution of a maliciously crafted Word

[37] https://analyze.intezer.com/#/analyses/7f80d1ad-a4ea-4eb9-8aea-cac5fec03161

[38] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

file that impersonated a resume, using Dropbox. Although the content was written in English, it is edited in Korean a Word version. After opening the document a Shellcode is run.

Overlap in Meta Data and Behavior

Investigating possible similar malware samples revealed that the malicious file properties are similar and that there are no other similar files. To verify this hypothesis, we performed a VirusTotal search that included some of the file properties and two additional ones: loading the 'ObtainUserAgentString' function, and a file size smaller than one MB. The query results confirmed our hypothesis that the files were uniquely similar, as the query detected only two files - the file reviewed in this report and the file reviewed in the McAfee report.

We detected further similarities in the structure and style of the C&C servers, their location at the end of the executable file, and similar properties surrounding them, as can be seen in the text strings of the malicious files. To the right is the file reviewed in the McAfee report and to the left is the file reviewed in the current report:

```
Microsoft Enhanced Cryptographic Provider v1.0
HTTP/1.0
Accept: text/html
Accept-Language: en-us;q=0.8;q=0.6,en-us;q=0.4,
Content-Type: application/x-www-form-urlencoded
Content-Length:
IDR_RESOURCE
%s..\GuiCache.db
http://www.alahbabgroup.com/bakala/verify.php
http://103.225.168.159/admin/verify.php
http://www.khuyay.org/odin_backup/public/loggof
http://47.91.56.21/verify.php
```

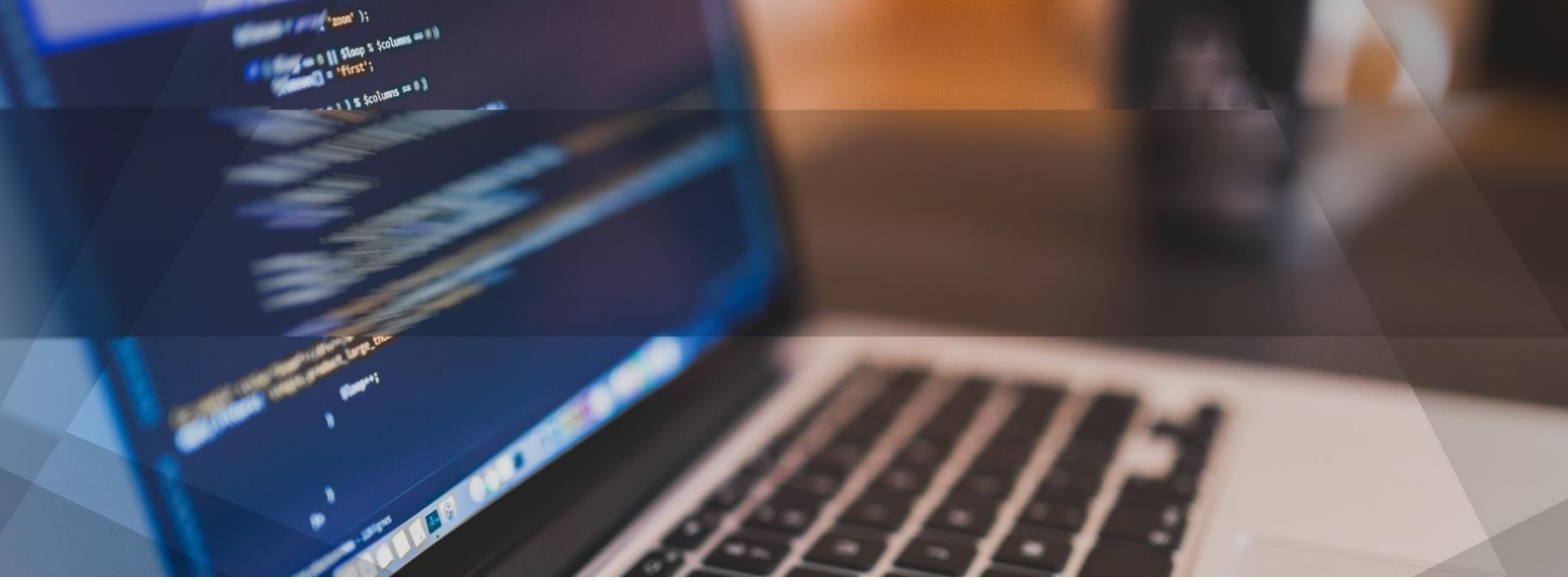
```
Microsoft Enhanced Cryptographic Provider v1.0
Accept: text/html,application/xhtml+xml,application/xml
Accept-Language: en-us;q=0.8;q=0.6,en-us;q=0.4,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length:
Connection: Keep-Alive
Cache-Control: no-cache
%s\*.*
%s\%s\
%s "%s > %s" %s
sZBam?W
C:\Users\WMJI\Desktop\sample.exe
http://34.214.99.20/view_style.php
http://137.74.41.56/board.php
https://www.kingkoil.com.sg/board.php
```

The Lazarus APT

The North Korean group Lazarus (also known as APT38 and Hidden Cobra) is one of the most active APT groups of the last decade. Among its most notable attacks are the 2016 attack on the Bangladesh Central Bank and the attacks against the Bithumb and Coincheck cryptographic exchange portals during 2018.

The group is associated with the North Korean government, and thus possess many resources and uses sophisticated and aggressive methods and self-developed tools. Unlike many other APT groups, Lazarus does not hesitate to carry out destruction operations in order to destroy evidence. Among the group's most famous malware families are PowerRatankba, Hangman and Positron.

While Lazarus attacks many sectors to achieve different goals, most of its attacks aimed at the financial sector are carried out by the subgroup Bluenoroff. Based only on the publicly exposed incidents, the extent of the theft attempts exceeds a billion and a half USD. According to a Group-IB analysis, Lazarus had stolen at least 571 million USD between January 2017 and October 2018, on 14 attacks.



Cyber-attacks Targeting Israel in the First Half of 2019

Smart Kangaroo - Phishing Campaign Targeted at Financial Institutions around the World

Background

Since March 2019, a group operating a sophisticated phishing infrastructure has been targeting banking clients in the Middle East and worldwide. We assess hundreds of thousands of USD worth of various currencies were stolen from several bank accounts. Our initial findings led us to believe that the campaign primarily targets Israeli users. However, in recent months the attacks against financial institutes in Israel have declined. Instead, the attacks have shifted to well-known firms in the media and financial sectors.

The name of the campaign "Clever Kangaroo" stems from the fact that the attackers are able to transfer their entire phishing infrastructure to new IP addresses in a short time span. In addition, they are able to bypass the two-factor authentication mechanism (an SMS message from the bank to the client). We detected hundreds of domain names and dozens of IP addresses most likely connected to the attacker's infrastructure. Most of the domain names and phishing pages that the attackers created are disguised as financial organizations.

The Targets

We believe that the attack group is a skilled international criminal group from Eastern Europe, possibly Russia, that recruited "money mules". These mules carry out money laundering operations for the group, often without knowing that they are taking part in illegal activity.

During April 2019, the campaign focused on phishing attempts against Israeli banks. However, recently the group has expanded its scope and begun targeting international companies from the financial and telecommunication sectors, among them PayPal, Vodaphone and Scotiabank.

Properties

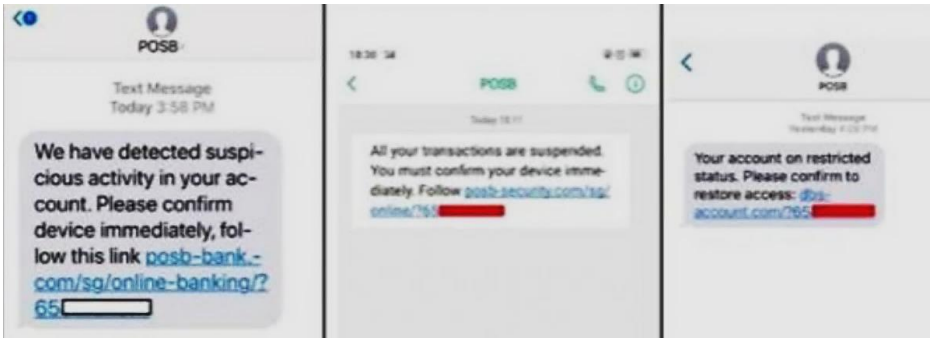
Throughout the course of our investigation, we were able to identify key characteristics of the campaign:

- Utilizing fake hosting and internet services disguised as Amazon, Akamai, Google and more.
- Disguising IP addresses of the attack infrastructure as to known internet services, media and porn websites.
- Obfuscating the attack infrastructure with Fast Flux - a DNS technique used by mainly by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. Thus, the servers' IP addresses are constantly replaced so they can sustain counterattacks by the victims.

- Setting up the infrastructure in Russia – hundreds of the registered domains use identical Nameserver servers – ns1[.]parens[.]ru, ns2[.]parens[.]ru – and approximately 70 domains were registered with NameSilo.
- Registering domains that resemble the targeted company's names (misspelled or phrased differently) and building a fake website based on the company's current portal and branding, all in a short time span.
- Generic domain names containing relevant keywords and targeting a broader audience. Below here is a mapping of the terms used by the attackers and their popularity within the domains registered by the attackers:

Domain Keyword	Number of Domains using the Word
online	**350**
bank	**200**
verification	**90**
login	**90**
account	**60**
secure	**50**
protect	**30**
validation	**20**

- The live fake websites were scanned several times via URLScan[.]io. This was done first in either parking mode or redirection mode to Bing. After adding fraudulent content they were scanned again.
- A collection of key IP addresses have been used throughout the campaign:
    - 124[.]156[.]115[.]52
    - 47[.]254[.]128[.]246
    - 5[.]189[.]224[.]208
    - 47[.]254[.]129[.]11
    - 185[.]244[.]150[.]0/24 (A range that was used often – note that the entire range was not used).
- Propagation via SMS – the most common distribution vector of the phishing websites was via SMS messages. In addition, fake websites were built so that they would look like the mobile platform of some of the targeted banks. Below here are a few examples:

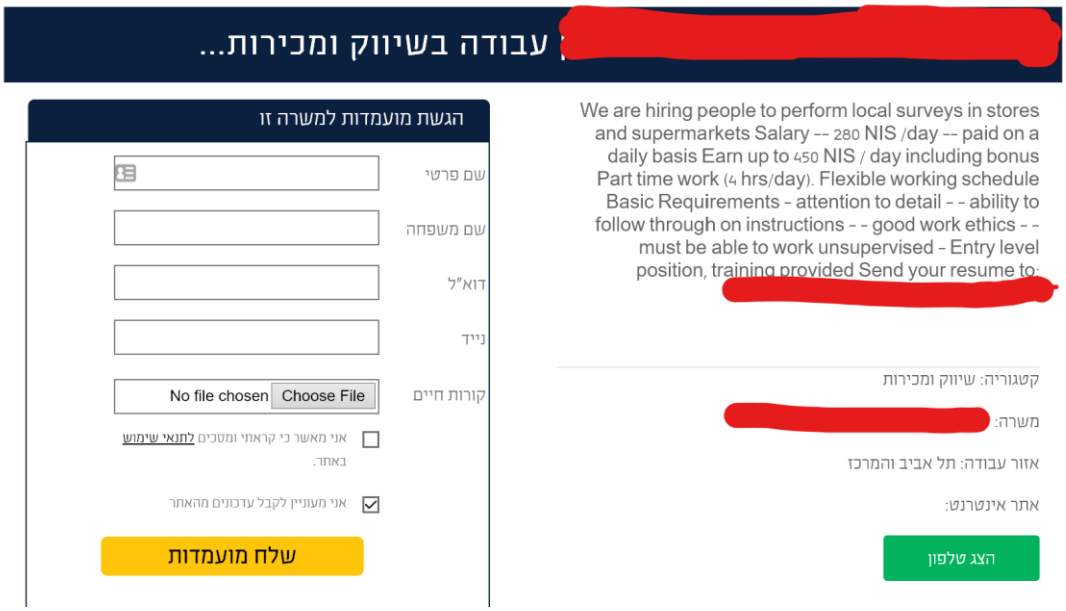


- Bypassing the OTP technology via SMS message – Research by some of the victims shed light on the attack method:
    - When the client inputs his login details in his bank portal, the attacker connects to the bank website.

- He then makes a financial transaction that is usually followed by an OTP message from the bank.
- Afterwards the victim receives another phishing message to his phone with a link for inputting the OTP code that he got from the bank.
- The attacker completes the transaction after receiving the legitimate code.

- Money Mules – The money was transferred to citizens who were persuaded to make financial transactions from their accounts. Most of them did not know where the money came from and that they were part of a fraud campaign. They were recruited with 'wanted ads' in English that they saw on employee recruiting websites, without knowing that the employer was actually a cybercrime gang. We recommend investigating the receivers of the financial transactions in order to check for similar methods of operation.

  Below here is a Money Mules recruiting ad:



A report about money mule recruitment has been spotted already in January:

> On January 4, 2019, I saw a part time employment ad on gumtree for a flexible admin job which requires just surveying the supermarkets within 2km of your house residence. i was to be paid $28/hr, with a maximum commitment of 20 hours/ week. and so given that i lack the time but was in need of money, i applied.
>
> I first got into contact with "arnold smith" who claims to be a human resource manager then got into contact with "erika andersen", the order support manager once i was "accepted". i also got into contact with "christian markovic" who claimed to be the hr director, asking for my bank details where you want the salary to be transferred.
>
> I was four days into doing the "order reports" when **they asked me to register in an e-currency website**. that's when i started doubting their legitimacy, and started to search for derby f&b. to my horror, this company has been scamming people from different parts of the world, targeting people to be their money mules.

Outline of the Attacks and SMS Verification Bypass Attempts by the Group

First case – Attacking the Verification Process of Financial Transactions

The normal verification process for a financial transaction is as follows:

1. The client logins from the mobile app or from the computer on the bank's website.

2. He accesses the financial transaction section from the interface.
3. He requests to carry out a transaction.
4. The bank's computers send the client a verification message via SMS.
5. The client inputs the verification code and the transaction is carried out.

Attack Process

Stage	Actor	Action	Result
1	attacker	Builds an attack infrastructure including websites disguised as the banks he wants to attack.	Fake website infrastructure.
2	attacker	Sends SMS message to potential clients with a link to the fake website	An SMS message is received in the client's cellphone.
3	client	Believes the message and presses the link of the SMS message.	A fake website appears on the client's phone.
4	client	Decides it is a fake website.	Exits the website. End of attempt.
4	client	Fills in his login details.	The account details are sent to the attacker.
5	attacker	Logs in to the bank through a computer or mobile device. He accesses the financial transaction section and fills in the transaction details.	A device verification request is sent to the bank.
6	bank	Carries out the transaction verification process.	Sends an SMS message with a verification code to the device which sent the request.
7	client	Receives an SMS from the bank	Reads the code.
8	attacker	Shows the client a form for inputting the code in the fake website.	Waits for the code from the client.
9	client	Inputs the code he received via SMS into the attacker's input form.	The verification code is sent to the attacker.
10	attacker	Receives the verification code from the client.	Inputs the verification details into the bank, in order to carry out the transaction.
11	bank	Receives the verification details from the attacker.	Carries out the transaction for the attacker.
12	attacker	Concludes the data receiving process from the client	Presents a conclusion screen to the client.

Second case – Attacking the Verification Process of Financial Transactions

Banks used to offer an option to register a device so that a verification code will not be required to carry out banking operations, including financial transactions. Note that this feature was eventually cancelled to prevent attacks.

The attackers exploited this feature by planting a cookie in the client's device after authentication of a mobile device or computer, in order not to prevent the bank from sending a verification code for financial transactions. The normal registration process is as follows:

1. The client logs in on a mobile app or on the computer.

2. She accesses the registration request on the interface.
3. The bank's computers send a verification code via SMS.
4. The client verifies the device, it is registered and henceforth can carry out transactions without authentication.

Attack Process

Stage	Actor	Action	Result
1	attacker	Builds attack infrastructure including websites disguised as the banks he wishes to attack.	Fake website infrastructure.
2	attacker	Sends SMS messages to potential clients with a link to the fake website.	An SMS message in the client's cellphone.
3	client	Presses the SMS message link.	She is redirected to a fake website of the bank.
4	client	Determines that it is a fake website.	Leaves the website.
4	client	Fills in her account details.	The account details are sent to the attacker.
5	attacker	Logs in from a different device into the bank's website, and requests to register his device.	A verification request is sent to the bank.
6	bank	The bank carries out the device registration process.	Sends am SMS message with a verification code to the device that requested registration.
7	Client	Receives an SMS message from the bank.	Reads the code.
8	attacker	Shows the client a form for inputting the code, in the fake website.	Waits for the code from the client.
9	client	Inputs the verification code she received via SMS, into the attacker's form.	The verification code is sent to the attacker.
10	attacker	Receives the verification code from the client.	Uses the code for the bank's registration process.
11	bank	Receives the verification code from the attacker	Registers the attacker's device.
12	attacker	Concludes the data receiving process from the client.	Shows a task conclusion screen to the client.
13	attacker	In some later time, logs in to the bank and carries out a transaction without needing verification code.	Money is transferred from the client's account.

Preventive Banking Measures

- SMS messages sent from the bank to the clients detail their exact purpose and are never generic.
- The option to register a device was cancelled. Each financial transaction is followed by a specific SMS message with an explanation about the transaction.
- The verification mechanism on the bank is explained in detail on the bank's portal, as well as a warning against phishing attacks.
- A more conservative limit for financial transactions without verification.

- Each client has a main cellphone number for verification purposes. To prevent changing it easily an SMS message is sent to the original number. The message explains that a change of number request has been received and warns the client before further verification.
- Research and investigation efforts meant to detect the infrastructure and attackers.

OpIsrael and OpJerusalem 2019 –Anti-Israeli Hacktivism OUT, Targeted Operations IN

Continuing the tendencies of the last years, the latest anti-Israel activism campaign was characterized by lowering of quality and reach of the activities. Organizers of the campaign have failed, this year especially, to gain momentum, and so the operation came to an end without any significant activities. Despite the social networks being full of publications calling for activists to attack Israel, very few of those activists have conducted actual attacks.

The only anti-Israeli hacktivist effort worthy of any notice this year has been operation OpJerusalem – an attack conducted on March the 2nd and enfolded the targeting of hundreds of Israeli internet sites for the purpose of infecting them with ransomware and showing defacement messages. Among the affected and defaced sites were "ynet", "Calcalist", and several other prominent sites.

The defacement message came after the attackers were able to gain control over the DNS registry of sites using a third-party accessibility addon and redirected the viewers to a malicious site containing a pro-Palestinian message and a ransomware. These affected sites load a JavaScript library from an address of a third-party service called "Nagish Beklik", which adds accessibility options for people with special needs in terms of vision, hearing, or mobility. From a check we have conducted, there were 1600 Israeli sites which use this addon.

The primary intrusion vector had been, apparently, a phishing email against the sites' owners, through which the attackers were able to get the credentials for the site containing the DNS registries and change them. The attackers have performed DNS Hijacking – gaining access to the manager of DNS entries of nagish.co.il. They have done so through gaining access to the Nameserver manager of the registrar, a company named "Box". The attackers have changed the IP address of one of the subdomains to point to their own, malicious IP address.

Both redirects to the subdomains of the "Nagish" site were changed: js.nagich[.]co.il and yad2-js.nagich[.]co.il. As a result, the attackers were able to serve the sites a different, malicious JavaScript instead of the original accessibility.js. The attackers have also produced an SSL certificate, which allowed them to serve the file without HTTPS alerts from the site they have prepared.

The malicious code was written to check the operational system of the computer, and if it's not Windows – the defacement message "Jerusalem is the capital of Palestine #OpJerusalem" is shown. Otherwise, a message prompting the user to update the Flash program would appear.

Clicking on "Update" will result in downloading a file hosted on another server under the attackers' control. The file does not run automatically, but rather waits for the user to run it after downloading. It is important to notice, that the system-checking script did not work during the analysis.

OpJerusalem 2019 Results

Thousands of internet users received a pop-up message declaring that Jerusalem is the capital of Palestine. However, due to a malfunction in the infection code, no actual damage to the was caused. In our estimation, if the script had worked, tens of hundreds of users would have been infected with ransomware. At this point, it is unclear who is behind the incident

and whether these are activists. Investigator Yuval Adam (@yuvadm) thinks that the actor behind the operation is @LulzSec[39], but @ZHacker claims it was @Th3Falcon.[40]

'Nagish' OpJerusalem Investigation

The company published an investigation into the incident. In the investigation, the security manager stated that after identifying the change of records in the box.co.il storage services, the company did the following:

1. The DNS records were soon updated to the correct IP addresses. It should be noted that a certain period of time is required between the update and its actual release and update on the DNS servers, both in Israel and around the world.
2. The box and the login information for the DNS records user interface has been replaced with the help if the BOX technical service.
3. Change of DNS servers and 2-step verification (2FA) of the management account.

https://twitter.com/yuvadm/status/1101887294242476033 [39]
https://twitter.com/ZHacker13/statuses/1102585591517118469 [40]

Iranian Global Cyber Operations

A Review of Recent Events – Nuclear Enrichment and Cyber Activities

In July 2019, the International Atomic Energy Agency (IAEA) confirmed that Iran has breached the limit of its enriched uranium stockpile set in the 2015 nuclear deal. This confirmation followed the statement published by Iran Foreign Minister, Mohammad Javad Zarif. This violation of the deal, as well as an explicit warning by European co-signatories, follows an escalation of the economic sanctions by the United States which was set on last May by President Donald Trump, after the latter has decided to quit the nuclear deal and urged its alley countries worldwide to cease the purchase of Iranian oil.

Earlier, in June, the United States carried out a high-profile attack on Iranian assets tied to the Revolutionary Guard Corps' missile launch systems. This move was initiated following a retaliatory military move that was called off but was originally set as a reaction to Iran's attack of an American RQ-4A Global Hawk surveillance drone that flew over southern Iran.

Alongside the deterioration of Iran's geo-political status in the international arena, the country has expanded its cyber activities targeting western entities – notably United States and Israeli targets – as well as continued its ongoing aggressive attacks against its usual targets, Saudi Arabia, the United Arab Emirates and Iranian minorities and anti-regime groups. Clearly, Iran is constantly translating its political activities and the global moves of the western countries against her to cyber-attacks. Thus, in the past few months the campaigns carried out by Iranian APT groups are becoming more and more aggressive and unconcealed.

A prominent example of the nature of the Iranian activities is the profile of APT33, also known as Elfin. The group has been actively targeting organizations in the research, chemical, engineering, manufacturing, finance and other sectors as of early 2016. Its prime targets are located in Saudi Arabia and the United States. Some 18 American organizations were attacked by APT33 in the past three years, including several Fortune 500 companies as well as healthcare providers and organizations targeted for the purpose of carrying out supply chain attacks.

It appears that despite the constant efforts, organizations and groups in the targeted countries put up a decent fight – throughout the past few months highly sensitive information about the activities of government-backed groups was leaked, exposing abilities, strategies, and attack tools. The main medium for this leak was a telegram channel, as well as GitHub. The first leak uncovered hacking tools, espionage tools, WebShells and target list of APT34, also Known as OilRig. APT34 has been attacking worldwide targets with an emphasis on the Middle-East. Another group that suffered from the leaks is the MuddyWater APT. The leaked information included previously unknown C&C servers used by the group, as well as attack tools that are offered for sale on underground forums.

To summarize, in the first half of 2019 there has been considerable escalation in the Iranian activity profile, from all aspects. Politically, the country is responding to the United States sanctions escalation with several bold moves, including

enlarging the enriched Uranium stockpile above the limit set in the nuclear deal, drop down of an American surveillance drone and most likely, sabotaging oil tanks on four trade ships in the Persian Gulf. Nevertheless, western governments and organizations are responding with full power, successfully sabotaging Iranian activities on a timely basis. These powerful reactions include the American cyberattack against the missile launch systems of the Revolutionary Guard Corps. The constant leaks of Iranian attack infrastructure and naturally, the extensive, in depth research of Iranian APT groups carried out by the security community.

The Citrix Hack

On March 8th, Citrix, a software company which provides multiple computing services, issued a statement that on March 6th it had received an alert from the FBI intelligence agency that the company's systems had been hacked by "international cyber-attackers"[41] using a Password Spraying attack – a Brute Force technique that leverages week passwords and examines them against a large number of accounts in the attacked organization.[42] It is important to note that the extent of the breach is still unclear and at this stage the nature of the documents and information stolen has not been confirmed. However, it is estimated that financial information and sensitive identification information (such as SSNs) relating to employees, suppliers and customers were stolen.

Following the incident, the security company Resecurity has claimed that it has uncovered findings linking the attack to Iranian entities that have previously attacked government organizations and energy companies around the world. According to them, the stolen database was 6 to 10 GB in size, and included email communications, files, business documents and internal corporate documents.

While the security community remained baffled with Resecurity's publication, on March 11, the company updated its reporting and provided a number of indicators - 3 IP addresses in Iran and 7 IP addresses from Canada, USA, Germany and France.

Iranian APT33 Exploitation of Outlook Vulnerability

On July 3rd, FireEye issued an update alert to an APT33 campaign from December 2018. The recent alert provides additional findings further supporting the attribution of the campaign to the group.[43] In this campaign the group executes attacks by exploiting an old Outlook vulnerability that was first reported in 2017 (CVE-2017-11774).[44]

According to the recent FireEye report, the campaign continued its activity throughout June and July 2019, and targeted governmental and federal organizations, financial firms, academic establishments, and media companies in the US. As a reminder in our follow up investigation we detected an overlap between APT33's attacks and another Iranian group – OilRig.

[41] https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/
[42] https://resources.infosecinstitute.com/password-spraying/
[43] https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
[44] https://www.gov.il/BlobFolder/reports/apt33/he/OUTLOOK-CERT-IL-W-967.pdf

Sea Turtle – DNS Record Hijacking Campaign Against Government Organizations in the Middle East and North Africa

Talos exposed a new DNS record hijacking campaign named Sea Turtle[45]. We recently posted a breaking alert on a new attack tool and C&C server by OilRig. There are connections and overlaps between the Talos indicators and the servers used by OilRig, which could indicate that OilRig are responsible for the attack.

Main targets: military, defense, and intelligence organizations, governmental departments and offices including foreign, energy and critical infrastructure departments.

Secondary targets leveraged to compromise the main targets – telecom companies, ISPs and DNS registers, and IT companies.

Most of the targets were located in the Middle East and North Africa. The attackers obtain initial access to the targets' DNS record management, and then changed the addresses under their control. By doing this, they were able to intercept traffic and act as a MITM (Man in the middle). Consequently, they could gather login information that passes from the end user to the targets' servers through the malicious server. Moreover, the attackers exploited several known vulnerabilities for initial penetration and/or propagation in the target's network.

[45] https://blog.talosintelligence.com/2019/04/seaturtle.html

ClearSky Investigations – Analysis of Iranian Cyber Operations

Iranian Nation-State APT Groups - Confidential Documents Leak

Analysis of Targets, Plans, and Attack Vectors

Over the past few weeks, Iranian APT groups have suffered several significant data leaks. After analyzing and investigating the documents we conclude that they are authentic. Consequently, the loss of data causes considerable harm these groups and their ongoing cyber operations.

Most of the leaks are posted on Telegram channels that were created specifically for this purpose. The identity of the actor behind the leak is currently unknown, however based on the scope and the quality of the exposed documents it appears that this is the work of professionals. We estimate that the leak will hamstring the groups' upcoming operations and minimize the risk posed by their attacks in the near future.

The documents were released to the public via three main Telegram groups:

- **Lab Dookhtegam pseudonym** ("The people whose lips are stitched and sealed" – translation from Persian) – this channel featured attack tools attributed to the OilRig group, as well as a WebShell that was inserted into the Technion, tools used for DNS attacks and more.
- **Green Leakers** – this channel was used to leak attack tools attributed to the MuddyWater group. The group's name and its symbol are identified with the "green movement", which led the protests in Iran after the Presidential elections in 2009. These protests were heavily repressed by the revolutionary guards (IRGC)
- **Black Box** – a long existing channel, unlike the above-mentioned ones. On May 5th, dozens of confidential documents classified as 'Secret' (the second highest classification rank) concerning Iranian APT groups' activity were posted on this channel.

Among the leaked data are documents by the Iranian Ministry of Intelligence that uncover information about a group called "Rana". At this stage, we cannot attribute the group to any known Iranian actor. Activities conducted by the group, according to the exposed documents, include Iranian citizens monitoring, both in Iran and abroad. The documents also reveal victim lists, cyber-attack strategies, alleged areas of access, employee list and screenshots from internal espionage system portals. A document related to the Islamic Revolutionary Guard Corps (IRGC) reveals details about the development of a malware aimed at attacking SCADA systems.

Iranian Ministry of Intelligence Documents

Rana team

Documents about the "Rana" group, classified as 'Secret', appear to have been written by a hacking and penetration team within the Iranian Ministry of Intelligence's cyber operations department.

A yearly report summarizing the year of 1394 (March 2015 – March 2016) was partially leaked. The report reveals a strategic data exfiltration operation targeting airline companies. Based on the report, we believe that hacking attempts against airline companies were indeed carried out. The operation is meant to allow monitoring of important Iranian personnel, as according to the report, such people use international airline services.

The information that should be collected as part of the operation includes the following data types:

1. Flight information, such as airline routes that might be under foreign surveillance, passenger identification and scenarios and detection of passengers that might have boarded a flight in disguise, for the purpose of arriving to an Enemy State.
2. Aircrew information, including personal credentials and the number of professionals in specific flights.
3. Information about high ranking professionals in a specific airline.
4. Equipment information, including suppliers, number of devices used in a specific flight, plane number and type and computer equipment.

Another report for the year of 1395 (in this case, only March 2016 – August 2016) enlists several successful espionage projects that targeted airline databases. Affected organizations include the Israeli airline "Israir", a Qatar-based airline and a Saudi Arabian insurance company. The databases of the Turkish police department and Emirates Roads and Transport Authority were examined.

3. تحقیق و پژوهش (R&D)

1-11 جلسه با کارکنان فرودگاه مهرآباد

- آشنایی با سیستم های GDS و CRS و روال کار آن‌ها
- آشنایی با زیرساخت نرم‌افزاری و بستر ارتباطی هواپیمایی‌های ایران
- آشنایی با روند پرواز یک مسافر (چک-این و کارت پرواز و غیره)

1-12 مباحث مربوط به داده‌کاوی

- مطالعه در مورد مفاهیم پایگاه‌داده‌ای ODS, MDS, DataMart, DataWarehouse
- آشنایی با ابزارهای مصورسازی داده مثل Tableau, Wrangler, Gephi

1-13 مباحث مربوط به Oracle

- Function, Stored Procedure
- توابع Lead, Lag, Partition
- مبحث Cursor (کار با خروجی یک کوئری)
- کار با SQL Loader برای وارد کردن سریع داده‌ها (txt, csv, ...) به پایگاه داده

1-14 مباحث مربوط به SQL Server

- نوشتن تابع معادل Listagg اوراکل در SQL Server (کاربرد این تابع: لیست کردن اطلاعات یک موجودیت مثل ش پاس‌های یک فرد)
- جمع‌آوری، ویرایش و تحویل کوئری‌های بررسی محتوای پایگاه داده‌های SQL Server برای تسهیل کار گروه هک

The preliminary research for these attacks included meetings with airline employees of 'Mehrabad' airport in Tehran, attack vector collection, asset mapping and database Query Language research, covering Oracle and SQL.

Amongst the documents there was also an image which, according to the leakers, proves an attempt to conceal currency procurement – perhaps due to the sanctions on Iran – via a VMware server.

Targets

Another leaked document provides information about attack campaigns meant to hack Israeli insurance companies, including multiple top firms – Ayalon, Altshuler Shaham, Clal, Menorah, Herel, Migdal, Phoenix, Direct Insurance and more. Nevertheless, the status of these attacks remains unclear. Further hacking targets are Israeli hotel reservation portals, for the purpose of credit card data theft. One successful hack lead to the theft of 86,000 credit card credentials. Among the government sector, the Israeli Ministry of Agriculture was attacked.

The leaked documents revealed Iranian attack plans against multiple additional targets worldwide, for example, governmental institutes in Kuwait. The goal of the attack was to obtain access to a Kuwaiti email service and leverage it for a data theft operation against the Ministry of Foreign Affairs. A strategic report from the first half of 1396 (March – August

2017) describes activity carried out against Kuwait. According to a report from 2017, two teams were in charge of the attack operation – the Hacking team and the Social Engineering team.

The Hacking team's work precedes that of the social engineering team. In the attack against the Kuwaiti ministry, the team begun with penetration tests on the ministry's systems. They then mapped the network and infrastructure and collected IP addresses, the domains, the websites and applications. They found out that they could obtain the highest level of control of the targeted servers. The hacking team also obtained access to the ministry's employee database in order to send spam messages to everyone within the ministry and validate the emails using Mail Tracker.

The Social Engineering team's responsibilities include mainly phishing and spear-phishing operations. As part of this scope, the team sent phishing emails to a hospital called 'Atam Ananya' and the Qatari oil company. The team also carries our spear-phishing attack. Thus, the team communicated directly personnel related to the Ministry of Foreign Affairs in Kuwait. According to the documentation of the attack, it was successful.

Iran Revoltionary Guard Corps (IRGC) Documents

A document carrying the IRGC's logo contains a details about a plan named Project 910, which revolved around the development of a malware intended to damage SCADA systems. It is a botnet that features spyware capabilities, such as remote connection. As of the time of writing, February 2016, the project did not achieve its goals despite its high budget.

MuddyWater APT Attack Infrastructure Targeting Turkish and Kurdish Organizations Exposed

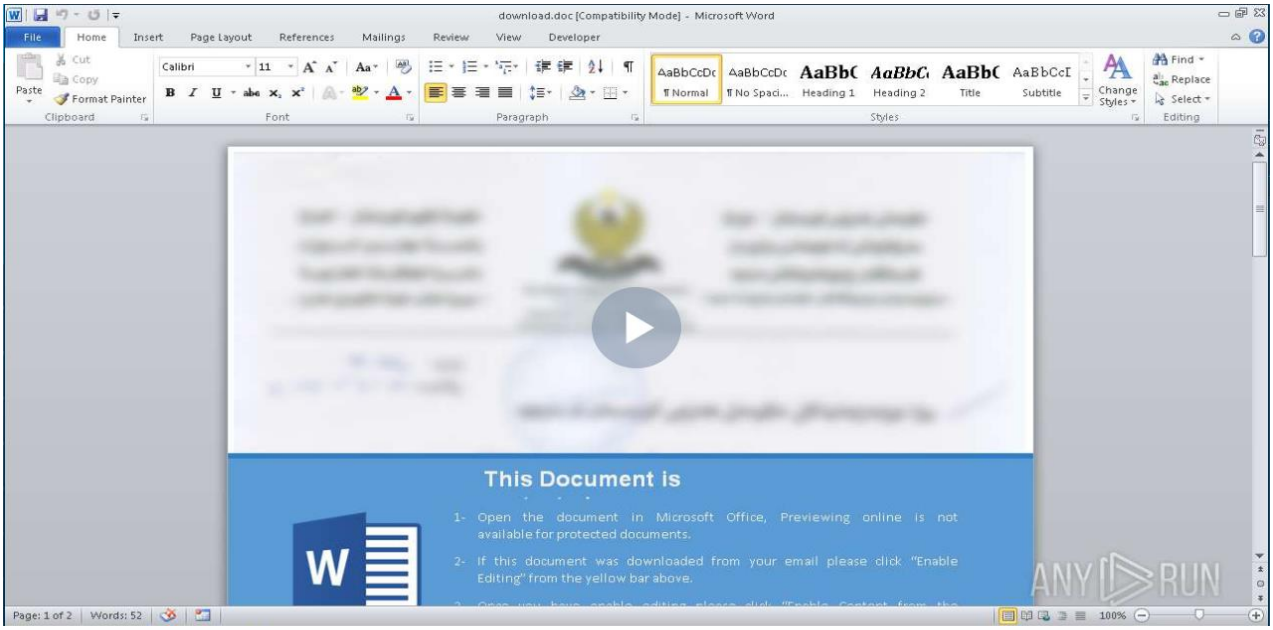
As part of our ongoing monitoring of the Iranian attack groups, in April 2019 we found documents we linked to previous infrastructure of the Iranian APT group MuddyWater. In previous research, we detected two domains that were hacked by the group (one of them Israeli) and used to store malicious code snippet of the POWERSTATS malware affiliated with the group. For more information on the outline of the attack, please visit the ClearSky blog.[46]

Unlike the previous attack vector, we did not identify the use of hacked servers' infrastructure in which the malicious code snippet was stored, but a malware that comes with a built-in snippet. In addition to the bait file of the first attack vector, we found five additional files that function the same but contain no content. We estimate that the attackers performed malware tests to determine whether the document was classified as malicious by the various Anti-Virus engines.

[46] https://www.clearskysec.com/muddywater-operations-in-lebanon-and-oman/

Attack Techniques and Targets

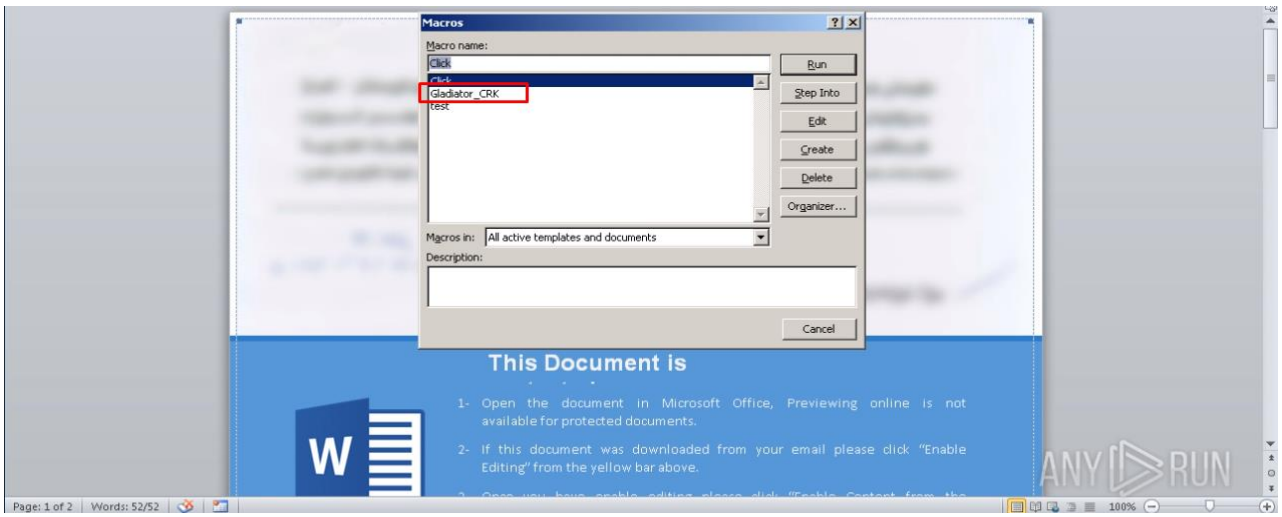
Most of the victims of the current wave of attacks are part of Kurdish groups (such as the Komala Organization - a Kurdish-Iranian party in Iraq) and various organizations in Turkey affiliated with the security sector and the Turkish army. The initial distribution vector is distribution by an email containing a malicious Office document. Below are screenshots from decoy documents we obtained.

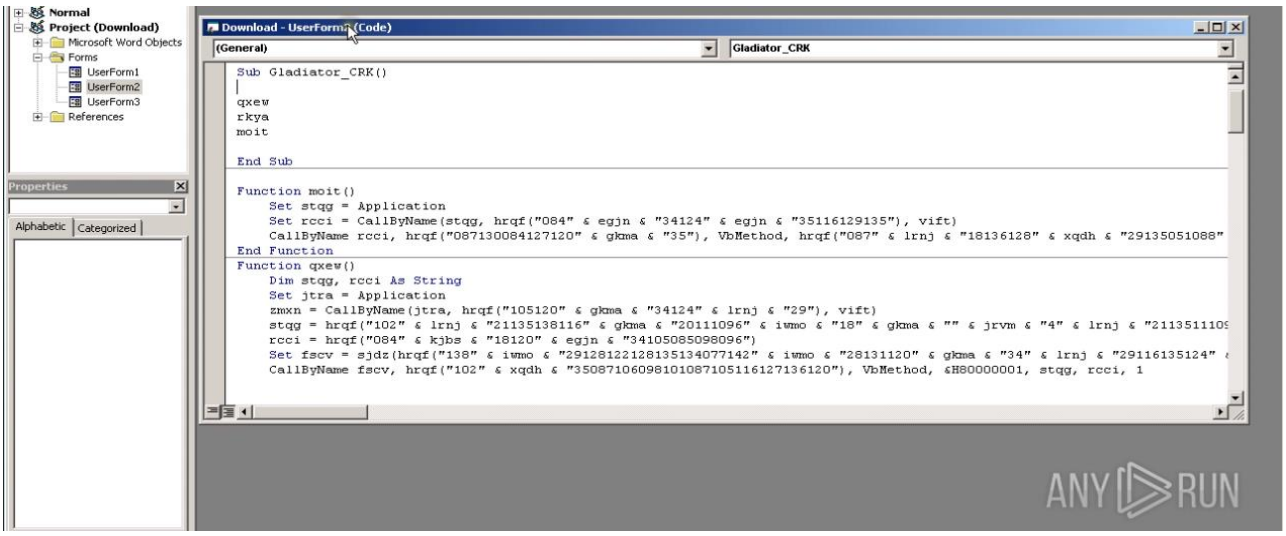


The document contains a blurry image of the Kurdistan Regional Government:

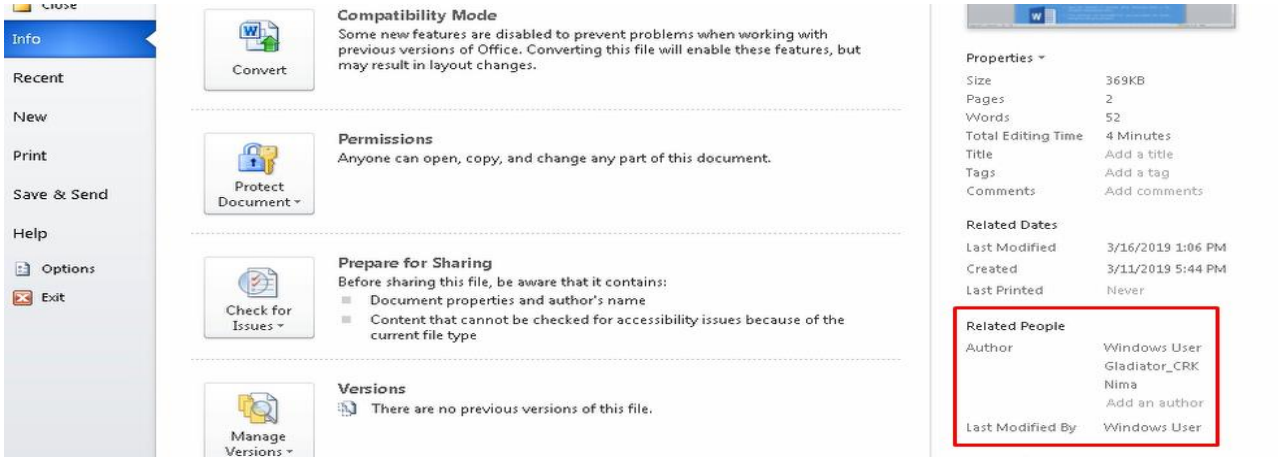
First Attack Vector

As you can see, the first decoy document contains a blurry image disguised as an official Kurdistan government document. The attacker lures the victim into clicking the Enable Editing or Enable Content and thus running a malicious macro command embedded in the Office Word file.





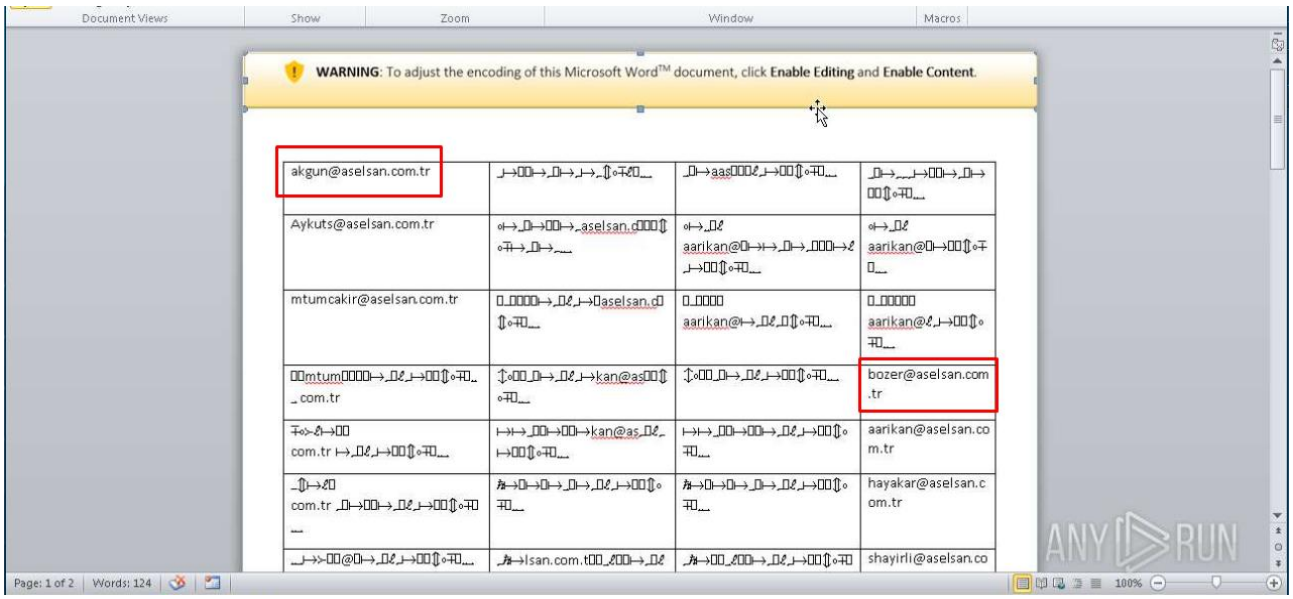
This Macro is called Gladiator_CRK. The attackers used this name in the OLE data as well under the name of the file editor.

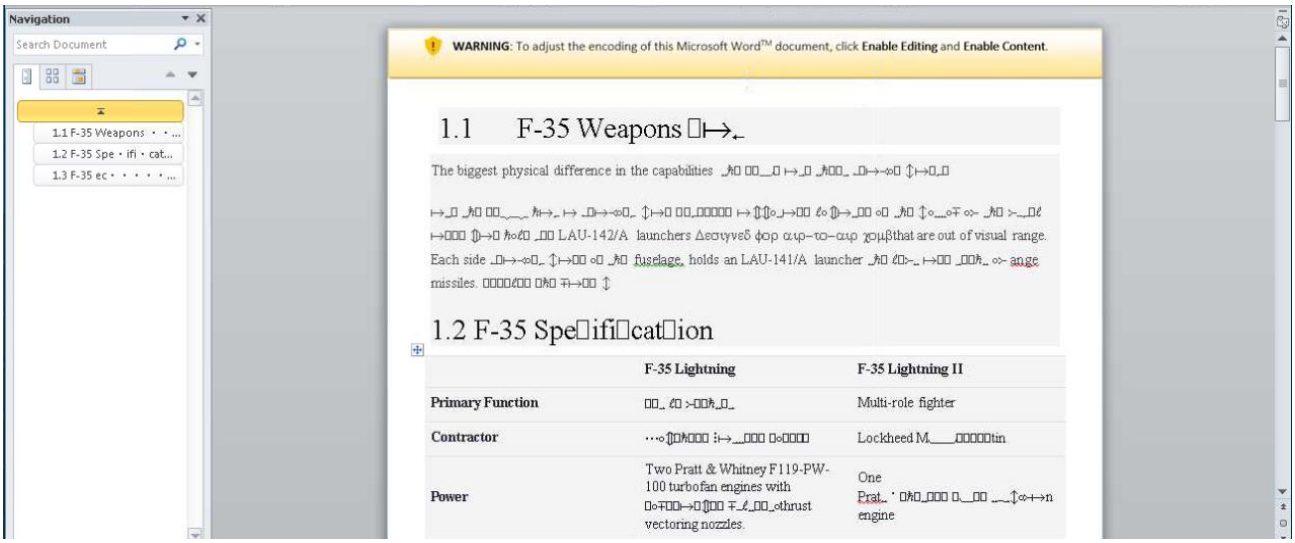


We pivoted the name, and it returned several documents that perform partial actions of the malware, most of them without any impersonating content. These files may have been uploaded to VirusTotal as a test to see if they are caught by the Anti-Virus engines. It should be noted that all of the empty files were uploaded to VirusTotal from Germany, while the malicious decoy document was uploaded from Iraq - this strengthens our assessment that files uploaded from Germany are tests.

Like previous cases, this Macro also uses an embedded com object in the macro code that allows the Excel process to run and run various commands under it. After running the malicious Macro, Registry entries are changed in order for the malicious code to run even after booting the infected station, thus ensuring persistency. In addition, two files were created in the Temp folder which contained the code snippets that extract the POWERSTATS malware, similar to the previous attack vectors. The PowerShell uses Windows Script Host (WScript.exe) to extract a VBE code from the first image file (icon.ico) and is encoded in VBScript. This code runs a JavaScript code in the file which is embedded in the second file (picture.jpg) and encoded in base64.

Unlike the previous files, we did not identify any additional servers used to download the above malware and they were created automatically.





Second Attack Vector

In this vector, we found that after the victim allowed the Macro to run, an encrypted txt file called Win32ApiSyncLog.txt was created on the computer in which the backdoor was encoded in base64. In addition, a file called Win32ApiSync.bat (Batch type) - which contains the script that executes the code snippet - was compiled.[47] This script creates a scheduled process on your computer (schtasks) which creates, reads, and extracts the contents of the Win32ApiSync file every hour. Despite the request to enable content in the document, no malicious macro command is installed (unlike the first file).

This may explain why, unlike the previous file, a PowerShell was not installed on the computer via the excel process. The OLE data shows that the document was recently edited by a man named Babak Amiri. In this case, too, we found several other documents under this name, but they also did not contain a Macro. These documents share identical properties:

[47] https://www.hybrid-analysis.com/sample/bef9051bb6e85d94c4cfc4e03359b31584be027e87758483e3b1e65d389483e6?environmentId=120
https://twitter.com/h4ckak/status/1108290593862475776

File information

Comments | ITW | Submissions | Analyses | Content | Details | Identification

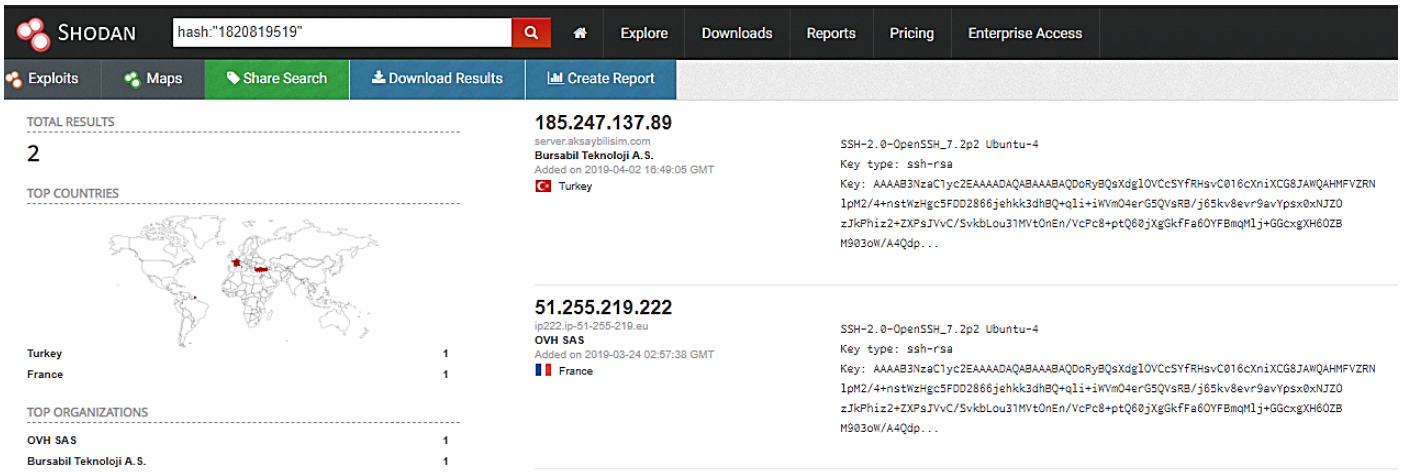
MD5	5c6148619abb10bb3789dcfb32f759a6
SHA-1	9732cf8c9e84e992d8856537dc5988371bb73f7c
SHA-256	bef9051bb6e85d94c4cfc4e03359b31584be027e87758483e3b1e65d389483e6
ssdeep	12288:3zwjL9+sC3QFiiQuBpKMPkHqD6jv2/wGhSnUdksu:30MsC3QFiiQuBpKMPuBkxksu
Size	716.5 ק"ב (bytes 733696)
Type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Template: Normal.dotm, Last Saved By: Babak Amiri, Revision Number: 244, Name of Creating Application: Microsoft Office Word, Total Editing Time: 12:41:00, Create Time/Date: Sun Feb 17 06:17:00 2019, Last Saved Time/Date: Wed Apr 03 18:51:00 2019, Number of Pages: 3, Number of Words: 304, Number of Characters: 1739, Security: 0
TrID	(Microsoft Word document (54.2% (Microsoft Word document (old ver.) (32.2% (Generic OLE2 / Multistream Compound File (13.5%

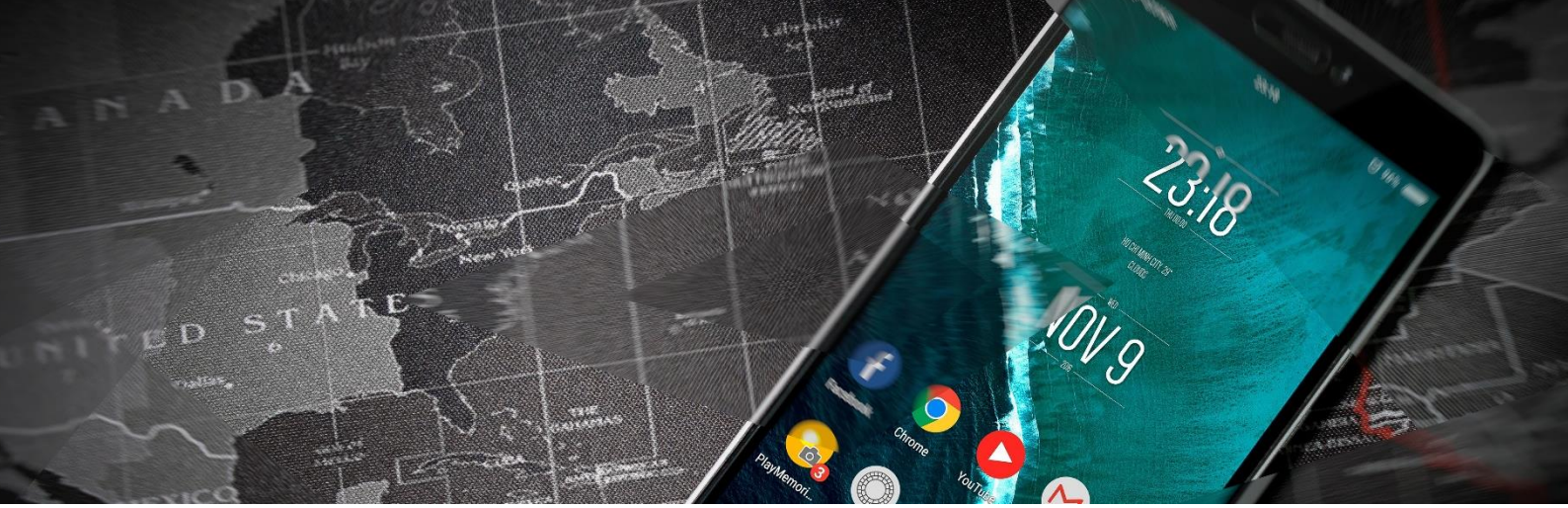
File information

Comments | ITW | Submissions | Analyses | Content | Details | Identification

MD5	8a7b2167c14a0158b3e9a43453a3e8f3
SHA-1	a1fa4ca930448d7660cd042c9c8d7e66fc7948f8
SHA-256	0c15fee57399462b192f4f35de3b37417afa519fda429540503c1f6e9a7b88c4
ssdeep	wSi8iS8px8SMDter0ZQko7RKDKMZX+8ozVN0jBS7JnoctjhNS:5q3yy0Z9eRMZ6z7pJnVNS:384
Size	40.0 ק"ב (bytes 40960)
Type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: Gladiator_CRK, Template: Normal.dotm, Last Saved By: Windows User, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Sat Mar 16 12:13:00 2019, Last Saved Time/Date: Sat Mar 16 12:15:00 2019, Number of Pages: 1, Number of Words: 0, Number of Characters: 0, Security: 0
TrID	(Microsoft Word document (54.2% (Microsoft Word document (old ver.) (32.2% (Generic OLE2 / Multistream Compound File (13.5%

Via further searches we performed we identified that in previous attacks the use of the Routing 46.105.84 [.] 146: 443 / WordOffice.jpg was noted for downloading images containing the malicious code snippet. Here are the two servers that were identified in our Shodan scan as having the same characteristics and are probably part of the same infrastructure:





Timeline – Events and Attacks in 2019 H1

Notes	Sector	Country	Attack Vector	Target
January				
The ticket order platform was hacked, resulting in the theft of 5 million passenger records, later offered for sale.	Transportation	China	Hacking and Data Leak	**China Railway**[48]
Credentials of over 3,000 passengers were stolen, and the company website was shut down.	Transportation	Ireland	Hacking and Data Leak	**Luas Trams**[49]
Two major attacks in the past two years, leading to client data theft.	Manufacturing	United States	Hacking and Infection	**OXO International**[50]
Election systems and computer network hacked.	Government	Ukraine	Hacking	**Servers and computers of election staff in Ukraine**[51]
IT systems were taken down. Among the company's clients are French Engie and Iridium Satellite.	Engineering	France	Hacking	**Altran Technologies**[52]
Financial information of clients was stolen in 2018.	Finances	United States	Hacking	**Discover Financial Services**[53]
500MB database of sensitive data was stolen.	Mining	Brazil	Hacking and Data Leak	**Vale**[54]
IT systems were hacked, manufacturing wasn't impacted.	Aviation	France	Hacking	**Airbus**[55]
Attacked by the Iranian group Chafer APT.	Government	Multiple Countries	Espionage	**Foreign diplomatic entities based in Iran**[56]

[48] https://technode.com/2019/01/02/beijing-police-data-leak-5-million/
[49] https://www.irishtimes.com/news/ireland/irish-news/over-3-000-luas-user-records-may-have-been-compromised-in-cyber-attack-1.3746674
[50] https://www.zdnet.com/article/oxo-international-discloses-data-breach-customer-data-over-two-years-impacted/
[51] https://www.reuters.com/article/us-ukraine-cyber-exclusive-idUSKCN1PJ1KX
[52] https://www.reuters.com/article/us-altran-tech-cyber/frances-altran-tech-hit-by-cyber-attack-idUSKCN1PM0IJ
[53] https://www.bleepingcomputer.com/news/security/discover-card-users-affected-by-data-breach-new-credit-cards-issued/
[54] https://www.databreaches.net/vale-e-hackeada-e-documentos-mostram-como-empresa-lida-com-acidentes-vale-is-hacked-documents-show-how-company-handles-accidents/
[55] https://www.reuters.com/article/us-airbus-cyber/airbus-reports-breach-into-its-systems-after-cyber-attack-idUSKCN1PO2TQ
[56] https://securelist.com/chafer-used-remexi-malware/89538/

Seven branches and the company's website were attacked.	Healthcare	United States	Phishing	**Valley Professional Community Health Center**[57]
February				
Banking activity ceased after attackers transferred funds out of the country.	Finances	Malta	Hacking	**Bank of Valetta**
30,000 medical records were exposed.	Healthcare	United States	Hacking	**Memorial Hospital**
100,000 customer records were exposed.	Real Estate	Australia	Hacking and Data Leak	**LandMark White**
400,000 medical records may be exposed after a ransomware attack.	Healthcare	United States	Ransomware	**Columbia Surgical Specialists of Spokane**
Some 7.7 million USD in cryptocurrency were stolen, due to a human error.	Finances	Singapore	Hacking	**EOS Cryptocurrency**
Hacking groups LulzSecITA and Anonymous Italia leaked information of seven agricultural companies as part of #OpGreenRights campaign.	Agriculture	Italy	Data Leak	**Italian Agricultural Corporations/Organizations**[58]
Attacked by South American APT-C-36 group.	Government, Finances and Energy	Colombia	Phishing and Malware Infection	**Colombian Government Institutions and Corporations**[59]
Attacked by the South Korean group Lazarus (Hidden Cobra).	Multiple Sectors	Russia	Ongoing Attack Campaign	**Russian-based companies**[60]
Attacked by the Russian group APT28 (Sofacy).	Politics	Multiple European Countries	Ongoing Attack Campaign	**Democratic institutions in Europe**
Company email, website and phone were taken down.	Automotive	Australia	Malware	**Toyota Australia**[61]
15,000 medical records were encrypted.	Healthcare	Australia	Hacking Ransomware	**Cabrini Hospital**[62]
March				
Attacked by the Chinese espionage group APT40.	Security, Engineering and Transportation	United States	Espionage and Ransomware	**Major organizations in engineering, transportation and defense**[63]
13 million USD stolen.	Fintech	South Korea	Financial Theft	**Bithumb**
Toyota subsidiaries hacked and 3 million client records were leaked.	Transportation	Multiple Countries	Hacking and Data Leak	**Toyota**[64]
Surrey Police office hit by ransomware.	Public	Great Britain	Ransomware	**UK Police Federation** [65]
Admin systems were offered for sale on the dark net.	Transportation	China	Hacking	**Chinese railway company**[66]

[57] https://www.databreaches.net/in-thousands-of-patients-information-compromised-in-data-breach/
[58] https://roguemedialabs.com/2019/02/19/anonymous-italia-lulzsecita-release-joint-leak-of-7-agricultural-corporations-organizations-across-italy/
[59] https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/
[60] https://www.bleepingcomputer.com/news/security/north-korean-apt-lazarus-targets-russian-entities-with-keymarble-backdoor/
[61] https://www.tripwire.com/state-of-security/featured/toyota-australia-cyber-attack-heart-hospital-ransomware/
[62] https://www.theage.com.au/national/victoria/crime-syndicate-hacks-15-000-medical-files-at-cabrini-hospital-demands-ransom-20190220-p50z3c.html
[63] https://www.zdnet.com/article/chinese-hackers-use-phishing-emails-to-target-engineering-transport-and-defence-companies/
[64] https://www.bleepingcomputer.com/news/security/toyota-security-breach-exposes-personal-info-of-31-million-clients/
[65] https://techcrunch.com/2019/03/21/police-federation-ransomware/
[66] https://www.hackread.com/dark-web-hacker-selling-admin-access-to-a-chinese-railway-company/

Over 90 websites defaced.	Government	India	Website Defacement	**Indian Government Websites**[67]
Attacked by the Iranian group Chafer APT.	Government	Turkey	נוזקה	**Turkish government entity**[68]
Attackers maintained internal access for six months.	Computing	United States	Hacking	**Citrix**[69]
Infected by the Gandcrab ransomware.	Government	China	Ransomware	**People's Government of Yiling District**
Japan banking users attacked by sophisticated malware.	Finances	Japan	Malware	**Banking Customers in Japan** [70]
Attackers sold access to the company's publishing systems, and enabled code manipulation.	Publishing	United States	Supply Chain Attack	**Sizmek Inc.**[71]
Private customer data stolen.	Retail	New Zealand	Hacking	**Kathmandu Holdings**[72]
Attacked by ransomware twice in the past two years.	Energy	United States	Ransomware	**Fort Collins Loveland Water District and South Fort Collins Sanitation District**[73]
Attacked by the LockerGoga ransomware, manufacturing network was damaged.	Manufacturing	Norway	Ransomware	**Norsk Hydro**[74]
Attacked by the LockerGoga ransomware, manufacturing network was damaged.	Chemical	United States	Ransomware	**Hexion**[75]
Suffered from a targeted attack campaign for three years.	Government	Saudi Arabia	Ongoing Phishing Campaign	**Saudi Government Agencies**[76]
Attacked by the Vietnamese group APT32.	Multiple Sectors	Multiple Asian Countries	Ongoing Attack Campaign	**Various targets in Asia**[77]
350,000 email accounts and sensitive data were exposed.	Government	United States	Hacking	**Oregon Department of Human Services (DHS)**[78]
Attacked by the Russian group APT28.	Government	Multiple European Countries	Espionage	**European governments**[79]
Attacked by an Indian APT group as part of the 'Lucky Elephant' campaign.	Government	Multiple Asian Countries	Espionage	**Government entities in Pakistan, Bangladesh, Sri Lanka, Maldives, Myanmar, and Nepal**[80]
Manufacturing network was infected by malware via a software update.	Computing	Taiwan	Hacking and Malware Infection	**ASUS**[81]
Over a million USD in cryptocurrency stolen.	Finances	Singapore	Financial Theft	**DragonEx** [82]

[67] https://www.hindustantimes.com/india-news/indo-pak-tensions-play-out-in-cyberspace-websites-hit/story-0qj6riwp9ETU6mKQrsjbCN.html
[68] https://securityaffairs.co/wordpress/82004/breaking-news/chafer-apt-python-backdoor.html
[69] https://www.darkreading.com/application-security/citrix-hacked-by-international-cybercriminals/d/d-id/1334122
[70] https://www.zdnet.com/article/this-banking-malware-just-returned-with-new-sneaky-tricks-to-steal-you-data/
[71] https://krebsonsecurity.com/2019/03/ad-network-sizmek-probes-account-breach/
[72] https://www.zdnet.com/article/kathmandu-urgently-investigating-incident-potentially-exposing-customer-info/
[73] https://www.databreaches.net/cyberattacker-demands-ransom-from-northern-colorado-utility/
[74] https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/
[75] https://www.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers
[76] https://threatpost.com/phishing-campaign-saudi-gov/142998/
[77] https://www.zdnet.com/article/oceanlotus-revamps-public-exploit-code-to-abuse-microsoft-office-software/
[78] https://www.bleepingcomputer.com/news/security/2-million-emails-of-350k-clients-possibly-exposed-in-oregon-dhs-data-breach/
[79] https://www.cnbc.com/2019/03/21/russian-hackers-target-european-governments-ahead-of-election-fireeye.html
[80] https://securityaffairs.co/wordpress/82963/hacking/lucky-elephant-campaign.html
[81] https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers
[82] https://www.zdnet.com/article/cryptocurrency-platforms-dragonex-and-coinbene-disclose-hacks/

Over 45 million USD in cryptocurrency stolen.	Finances	China	Financial Theft	**CoinBene**[83]
Over 21 million USD in cryptocurrency stolen.	Finances	South Korea	Financial Theft	**Bithumb**
April				
8,000 client data records stolen.	Transportation	Japan	Hacking and Data Leak	**Kyushu Railway Co.**
11,000 client data records leaked.	Public	United States	Hacking and Data Leak	**Minnesota Department of Human Services**[84]
1.3 million personal records accessible due to a flaw.	Academy	United States	Hacking	**Georgia Tech**[85]
Email system hacked and funds were stolen.	Public	United States	Hacking and Fraud	**Saint Ambrose Catholic Parish**[86]
Severely attacked, operations were damaged for over two weeks.	Retail	United States	Ransomware	**Arizona Beverages**[87]
Attacked by the Wicked Panda APT with WINNTI malware.	Medical	Germany	Malware	**Bayer AG**[88]
Thailand factories were partially shut down.	Medical	Japan and Thailand	נזוקת כריית מטבעות קריפטוגרפיים	**Hoya Corporation**[89]
The official elections portal was attacked.	Government	Finland	DDoS	**Finland Election Result Service (vaalit.fi)**[90]
The company website was defaced twice within several hours.	Energy	Bangladesh	Website Defacement	**Petrobangla Oil, Gas and Mineral Corporation**[91]
The company was hacked, and ransom was demanded.	Transportation	Russia	Hacking and Ransomware	**largest transport company in the Republic of Bashkortostan Bashauto**[92]
Attacked by the Gustuff Android malware.	Finances	Australia	Mobile Malware	**Australian financial institutions**[93]
Attacked by Russian attackers using the Triton SCADA malware.	Energy	Unknown	Destructive Malware	**Undisclosed Critical Infrastructure**[94]
The defense sector was heavily targeted.	Defence	Latvia	Hacking and Disinformation Campaign	**Lithuanian Ministry of Defense**[95]
Company systems hacked and leveraged for further attacks.	IT	India	Supply Chain Attack	**Wipro**[96]
May				
Access to 500,000 customer records was obtained.	Retail	Japan	Credential Stuffing	**UNIQLO Japan**[97]

[83] https://www.zdnet.com/article/cryptocurrency-platforms-dragonex-and-coinbene-disclose-hacks/
[84] https://securityaffairs.co/wordpress/83609/data-breach/minnesota-department-of-human-services-breach.html
[85] https://www.bleepingcomputer.com/news/security/georgia-tech-data-breach-exposes-info-for-13-million-people/
[86] https://www.bleepingcomputer.com/news/security/175-million-stolen-by-crooks-in-church-bec-attack/
[87] https://techcrunch.com/2019/04/02/arizona-beverages-ransomware/
[88] https://www.reuters.com/article/us-bayer-cyber-idUSKCN1RG0NN
[89] https://www.japantimes.co.jp/news/2019/04/06/business/corporate-business/hoya-hit-cyberattack-february-disrupting-thai-factory-operations/#.XL6SvaaEbxg
[90] http://www.helsinkitimes.fi/finland/finland-news/domestic/16333-dos-attack-against-election-results-portal-under-investigation-in-finland.html
[91] https://www.databreaches.net/petrobangla-website-hacked-again/
[92] https://www.ehackingnews.com/2019/04/hackers-broke-into-database-bashauto.html
[93] https://www.darkreading.com/vulnerabilities---threats/new-android-malware-adds-persistence-targets-australian-banking-customers/d/d-id/1334394
[94] https://arstechnica.com/information-technology/2019/04/mysterious-safety-tampering-malware-infects-a-2nd-critical-infrastructure-site/
[95] https://securityaffairs.co/wordpress/83813/cyber-warfare-2/attack-hit-lithuanian-defense.html
[96] https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/
[97] https://www.bleepingcomputer.com/news/security/hackers-access-over-461-000-accounts-in-uniqlo-data-breach/

Funds were stolen from sellers' accounts.	Commerce	United States	Hacking	**Amazon**[98]
4,000 blood donor data was obtained.	Healthcare	Singapore	Hacking	**Singapore Red Cross**[99]
139 million user data was leaked by a hacker called GnosticPlayers.	Computing	Australia	Hacking and Data Leak	**Canva**[100]
Company website hacked and several systems, including payment, were shut down.	Energy	India	Hacking	**Telangana State Southern Power Distribution Company Ltd (TSSPDCL)**[101]
The company's systems were hacked and numerous services, such as email, were disrupted.	Construction	Austria	Hacking	**Porr AG**[102]
Numerous systems, none of them critical, were shut down by the RobbinHood Ransomware.	Municipality	United States	Ransomware	**City of Baltimore**[103]
Over 40.7 million USD in BitCoin stolen from the largest crypto exchange in the world.	Fintech	Multiple Countries	Hacking	**Binance**[104]
Some 130 companies were attacked by the FIN7 group using the Griffon malware.	Multiple Sectors	Multiple Countries	Ongoing Attack Campaign	**130 companies worldwide**[105]
Attacked by the Russian group Fxmsp.	Information Security	Multiple Countries	Targeted Attack Campaign	**Trend Micro, Symantec and McAfee**[106]
Payment data of 1,100 subscribers stolen.	Computing	United States	Hacking and Data Leak	**WIRED**[107]
Sensitive employee data was stolen.	Sports	United States	Hacking and Data Leak	**Pacers Sports & Entertainment (PSE)**[108]
Over 25,000 patient records impacted.	Healthcare	United States	Ransomware	**South-eastern Council on Alcoholism and Drug Dependence, Inc. ("SCADD")**[109]
Attacked by the North Korean group APT37.	Government, Military and Media	South Korea	Targeted Attack Campaign	**Government, defence, military, and media organizations in South Korea**[110]
Internal systems were hacked.	Computing	United States	Hacking	**Stack Overflow**[111]
Several systems were damaged, no impact on security or flight control systems.	Transportation	United States	Ransomware	**Louisville Regional Airport Authority (LRAA)**[112]

[98] https://www.bloomberg.com/news/articles/2019-05-08/amazon-hit-by-extensive-fraud-as-hackers-siphoned-merchant-funds
[99] https://www.databreaches.net/singapore-red-cross-website-hacked-more-than-4000-blood-donors-info-compromised/
[100] https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/
[101] https://www.thehindubusinessline.com/info-tech/ransomware-attack-on-ap-telangana-power-utility-sites/article27027361.ece
[102] https://porr-group.com/en/investor-relations/announcement-events/ad-hoc-announcement/ad-hoc-details/news/cyber-angriff-bei-der-porr/
[103] https://arstechnica.com/information-technology/2019/05/baltimore-city-government-hit-by-robbinhood-ransomware/
[104] https://www.coindesk.com/hackers-steal-40-7-million-in-bitcoin-from-crypto-exchange-binance
[105] https://www.infosecurity-magazine.com/news/fin7-apt-targets-130-orgs-after-1-1/
[106] https://www.bleepingcomputer.com/news/security/fxmsp-chat-logs-reveal-the-hacked-antivirus-vendors-avs-respond/
[107] https://www.databreaches.net/conde-nast-notifies-1100-wired-subscribers-after-subscriber-page-vendor-breach/
[108] https://www.zdnet.com/article/indiana-pacers-disclose-security-breach/
[109] https://www.databreaches.net/25148-patients-served-by-southeastern-council-on-alcoholism-and-drug-dependence-notified-of-ransomware-incident/
[110] https://securityaffairs.co/wordpress/85469/apt/scarcruft-apt-bluetooth-harvester.html
[111] https://www.bleepingcomputer.com/news/security/hackers-accessed-stack-overflows-production-systems/
[112] https://www.scmagazine.com/home/security-news/louisville-regional-airport-authority-grounded-by-ransomware-attack/

Databases were hacked and used for phishing and supply chain attacks.	Computing	United States	Supply Chain Attack	**Computacenter UK Ltd**[113]
Attacked by the Russian group TA505 with the Amadey botnet.	Finances	Chile	Targeted Attack Campaign	**Financial institutions in Chile**[114]
June				
Sensitive operational documents were leaked and exposed.	Cyber-attack	Iran	Doxing	**AP34**[115]
200,000 student and staff records were stolen.	Academy	Australia	Hacking and Data Leak	**Australian National University**[116]
Sensitive information was stolen.	Government	The European Union	Hacking and Data Leak	**European Union's embassy in Moscow**[117]
Systems were infected by the Globeimposter 2.0 ransomware.	Nonprofit Organization	United States	Ransomware	**Auburn Food Bank**[118]
10 million USD in Ripple (XRP) were stolen.	Fintech	Great Britain	Financial Theft	**GateHub cryptocurrency wallet service**[119]
Networks were infected by a multi-purpose backdoor.	Government	Russian-speaking Countries	Malware	**Russian-speaking government entities in Central Asia**[120]
Attacked by the PLATINUM APT group.	Government and Military	Multiple Asian Countries	Ongoing Attack Campaign	**Diplomatic, government and military entities in South and Southeast Asian countries**[121]
Attacked by the Scattered Canary threat group.	Governmental Organizations	United States	BTC Attack	**U.S companies and government institutions**[122]
The traffic of several Cellular carriers was taken over by a hacker for a few hours.	Telecommunications	Multiple European Countries	Cellular Internet Interception	**Multiple carriers in Europe**

[113] https://www.theregister.co.uk/2019/05/23/computacenter_staff_security_clearance_application_mailbox_breached/
[114] https://www.infosecurity-magazine.com/news/ta505-suspected-in-chilean-malware/
[115] https://www.bleepingcomputer.com/news/security/new-email-hacking-tool-from-oilrig-apt-group-leaked-online/
[116] https://www.smh.com.au/politics/federal/anu-says-sophisticated-operator-stole-data-in-cyber-breach-20190604-p51ua9.html
[117] https://www.scmagazineuk.com/russia-accused-hacking-eu-embassy-moscow/article/1587122
[118] https://www.bleepingcomputer.com/news/security/food-bank-hit-by-ransomware-needs-your-charity-to-rebuild/
[119] https://securityaffairs.co/wordpress/86769/hacking/gatehub-cyber-heist.html
[120] https://www.scmagazine.com/home/security-news/malware/new-hawkball-backdoor-attacks-government-sector-in-central-asia/
[121] https://securelist.com/platinum-is-back/91135/
[122] https://threatpost.com/newly-identified-bec-cybergang-targets-u-s-enterprise-victims/145195/

Email: info@clearskysec.com
Website: clearskysec.com

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.