

January
2018



Cyber Intelligence Report 2017

Preface

Major cyber trends in 2017

The most significant attacks this year were executed by organized cybercrime groups and nation-state actors

Over the last two years, the cyberspace has become a prominent medium for fighting between countries. Amongst the major global cyber actors, Russia is both the most significant nation-state actor and the habitat for cybercrime groups, who stole in the past year billions of dollars using ransomware and spear phishing targeted attacks. **Accordingly, we have declared Russia as 2017's "Cyber Queen".**

Cyber-attacks targeting democratic processes and public perception

This year we have observed cyber-attacks that have been executed with the end goal of undermining democratic processes and blatantly trying to change the political status quo by spreading misinformation designed to alter public opinion, as well as sabotaging elections and public opinion polls. This has been achieved by various means including the creation of thousands of fake social media profiles. Examples of this are evidenced by the propagation of fake news in the Ukraine; attempting to alter election results in the US and France; and aiming to influence the outcome of the Brexit referendum in the UK.

The crash of the "Eggshell Security" paradigm

The model, which is primarily based on the idea of implementing comprehensive outer security measures while keeping the inner "core" exposed, resulted in billions of dollars of losses to companies in 2017. The ramification of this paradigm is that in recent years inter-organizational security systems were neglected. The current state is that many organizations allocate considerable amounts of resources to their outer security layer at the expense of inner security systems. This imbalance enables attackers to easily spread across various systems once they penetrate an organization. Moreover, this paradigm is increasingly becoming less effective against hybrid attack vectors that uses multiple techniques to ensure a successful attack.

Attacks such as NotPetya and WannaCry, have demonstrated and emphasized that this paradigm is outdated and no longer adequately effective.

The year of Enterprise-cyber-attacks – widescale successful destructive attacks against large companies

One of the most prominent trends in 2017 is large destructive attacks against prominent multi-national corporations. This is the first year we have seen widescale destructive attacks against private firms. Tens of thousands of computers and corporate core systems were corrupted due to cyber-attacks. Billions of dollars of damages, as well as months of disrupted operation have illustrated this threat to the managerial echelon of companies across the world.

Cyber-attacks exploiting supply chain

In 2017 there was a significant increase of successful attacks that exploited supply chain (i.e. third-party service provider) in order to compromise their targets. Often these attacks are executed in conjunction with the exploitation of vulnerabilities in OS and communication protocols vulnerabilities.

Instantaneous exploitation of 1-day vulnerabilities

Another significant trend relates to the growing speed with which attackers are exploiting 0-day and developing new attack tools following the publication of corporate reports. Events of 2017 have illustrated that for an attacker to execute a significant attack, he no longer needs to invest time and effort in uncovering unknown vulnerabilities,

but merely needs to monitor channels of information that report newly discovered weaknesses. The attacker is then in a position to leverage the gap between the vulnerability being discovered, and the organization updating their systems with the relevant security update; which may take several weeks and even months. The WannaCry event is an example of such an attack.

Proliferation of attack tools - wide scale propagation and instantaneous use of tools shared online

In a similar fashion to the exploitation of 1-day vulnerabilities, there is also a proliferation of attack tools. A notable example can be seen by the rapid proliferation of the leaked NSA attack tools that quickly got adopted by threat agent from North Korea, Russia, China and other countries.

The financial sector (banks) have become a central target for sophisticated attackers (both criminal and nation-state actors)

Core banking systems such as SWIFT and ATM networks have become a favorable target for cyber attackers. Primary targets have been banks located in Eastern Europe and East Asia, with successful attacks resulting in the theft of hundreds of millions of dollars.

Cryptocurrency markets and wallets have become a prominent target for cybercriminals

As cryptocurrencies are rising in acceptance and becoming more widely used, hackers and cybercrime actors have increasingly turned their attention towards them. This year between several dozen to several hundreds of millions of crypto coins have been stolen through various scams and attacks.

Most prominent cyber actors

Following our 2016 assessment, it appears that the most significant attackers in 2017 are Russian actors who can be categorized as follows:

1. **Nation-state threat agents** - Groups such as APT28 that have executed high profile attacks, most notably against Ukraine and the US. The Russian government has continued to blatantly and readily use cyber weapons this year. This was done in numerous ways, ranging from attacks against the Ukraine's infrastructure, from attempts to influence certain countries' political process in order to undermine the global geopolitical status quo.
2. **Cybercrime groups** – The most prominent group is Carbanak which attacked SWIFT and ATM systems.

In accordance with our 2016 end of year assessment, as of early December, large Russian cybercrime groups (such as Carbanak), **have not spear targeted Israeli companies in 2017.**

Most significant attacks in 2017

1. Petya/NotPetya – destructive cyber-attack against Ukraine: This was one of the largest and most destructive cyber-attacks which took place in late June, wiping thousands of computers, and disrupting the operation of numerous companies in the Ukraine as well as countries that conduct business with Ukraine.

As of December 2017, this was the single most costly cyber-attack of the year. Based on reports from affected companies, it is estimated that the total sum of damages reached around US\$1.2 billion.

2. WannaCry – global destructive cyber-attack: On Friday May 12th, WannaCry attack instigated an unprecedented global event, infecting and damaging over 230,000 computers across 150 countries within a single day.

3. Equifax breach: In early September the consumer credit rating agency Equifax Inc. reported that it fell victim to a large scale cyber-attack resulting in over 143 million records of individuals and companies being compromised. Most of the stolen data pertains to US, UK and Canadian citizen.

Equifax is one of the three largest American credit agencies, with extensive operations around the world. It aggregates and manages sensitive databases, including credit ratings of about 800 million citizens and companies.

4. Nation-state attack tools and documents leak: The CIA documents leak, in conjunction with the NSA 0-day vulnerabilities and attack tools leak have resulted in the expedited development of new and more sophisticated attack vectors and tools.

The weaponization of the leaks were leveraged by numerous actors from across the cyber landscape (hacktivists, criminals, nation-state threat agents, and terror organizations).

5. Russian intervention with the US and other countries' elections and democratic processes, including Brexit

Claims were made regarding the propagation by Russian actors, of sensitive and/or false information to influence and disrupt the democratic process in various countries. As part of this agenda, the malicious use of various social platforms such as Facebook and Twitter were noted attempts to undermine Western and pro-Western countries' political status quo.

Most prominent attack vectors in 2017

1. Attacks exploiting the supply chain: Breaching a third-party service provider in order to execute an attack on a company that uses its services or products. In the NotPetya campaign a legitimate accounting software was exploited to distribute malware to thousands of companies and organizations (including governmental organizations) in Ukraine.

2. Exploitation of native vulnerabilities with OS and communication protocols: This vector grew this year due to, amongst other reasons, a series of nation-state attack tool leaks. This threat increased after November 9th, when the source code of HIVE, the CIA's malware management software, was leaked by WikiLeaks.

3. Ransomware extortion attacks: Throughout 2017, hundreds of business, NGOs, governmental organizations and private individual fell victim to ransomware attacks.

4. BEC scams (Business Email Compromise) – attacks based on impersonating executives: This type of scam is relatively easy to execute with one of the most common scenarios being that the attacker impersonates a director in the company and requests from the target (often someone in a financial department) to immediately and covertly wire transfer money for reasons such as an urgent and secretive, yet highly important business deal. According to an FBI report, companies in the US have lost over US\$5 billion to such attacks over the last two years.

5. Wide scale DDoS attacks, some of which executed by IoT botnets: This year has registered a significant increase in the frequency of global DDoS attacks, which have nearly doubled over the previous year, increasing 91% since January 2017.

This is due in part to the exponential growth of IoT (the Internet of Things), i.e. "smart" devices such as household appliances with online capabilities that are susceptible to being infected by Botnets such as the Mirai Botnet. Moreover, the market for DDoS-for-hire services is continually growing, enabling any malicious actor to execute massive DDoS attacks regardless of their technical capabilities.

Predictions for 2018

Growing exploitation of the supply chain for various attack vectors

The largest attacks this year have illustrated to all active threat agents operating today that this vector is highly effective, yet not fully exploited, and thus can be used to considerably expanded by the scale of attacks, as well as the success rate. In our assessment, this vector will be extensively used next year.

Increased attempts of attacks against the financial sector

Throughout 2016-2017 numerous attacks were executed against the SWIFT system, ATM systems, and other core banking/accounting systems. This trend is expected to grow in 2018 alongside new attacks against additional core banking systems.

Proliferation of attack tools

The timeframe between the moment an exploit code is made public and its use as an attack tool by malicious actors around the world is continuously becoming shorter. For example, the use of NSA's tools by North Korea - This trend is expected to continue into 2018.

Increased awareness of data leaks following the implementation of the GDPR

On May 25th, 2018, the GDPR (General Data Protection Regulation) will be instated. One of the most important clauses of this regulation is that organizations will be required to report any database breach within 72 hours or be penalized with heavy fines. Accordingly, despite the probable initial difficulties in adapting, going forward we expect to see more transparency from European organizations regarding malicious activity.

As for Israel

In our assessment, in 2018 we expect to see increased activity of multi-national criminal actors within the Israeli cyberspace. We also expect that concurrently additional criminal groups will enter the Israeli cyberspace. Furthermore, we will likely see anti-Israeli nation-state threat actors adopting new attack vectors, although with a notably lower operational capability than criminal actors.

Recommendations for 2018

1. Relocating additional resources for inter-organizational security systems: With recent developments in hybrid attack vectors, the outer security shell can no longer be prioritized over the internal security framework. Accordingly, organizations and companies must transition to a more holistic security model that can effectively cope with the accelerated evolution of attack methods that we have witnessed over the last couple of years.

2. Segmenting networks and taking core systems offline

3. Creating an emergency backup system that could allow a company to operate up to three months after being hit by a destructive cyber-attack.

4. Minimizing the time-gap between the time security patches are released and when they are installed: Examine how to rapidly implement a policy to install security patches, despite the potential risk of disruption to an organization's normal operation. It is advised to define a timeframe that is both realistic and agreed upon by the relevant parties within the organization.

5. Raising employee awareness to new attack vectors: Most notably about social engineering techniques and significant campaigns.

Table of Contents

PREFACE	2
MAJOR CYBER TRENDS IN 2017	2
MOST PROMINENT CYBER ACTORS	3
MOST SIGNIFICANT ATTACKS IN 2017	3
MOST PROMINENT ATTACK VECTORS IN 2017	4
PREDICTIONS FOR 2018	5
RECOMMENDATIONS FOR 2018	5
TABLE OF CONTENTS	6
SIGNIFICANT TRENDS AND ATTACKS IN 2017	9
MAJOR TRENDS IN 2017	9
MAIN ATTACK TOOLS/VECTORS IN 2017	11
2017 CYBER EVENT SUMMARY TABLE – INCLUDING THE ATTACK VECTOR AND SCOPE OF DAMAGE	13
MALICIOUS ACTIVITY TRENDS IN 2017	16
MOST ATTACKED SYSTEMS IN 2017	16
MOST COMMON RANSOMWARE FAMILIES - 2017	16
MOBILE THREATS – TRENDS IN 2017	17
DDoS ATTACKS	17
MOST SIGNIFICANT ATTACKS IN 2017	18
PETYA/NOTPETYA – WIDESCALE DESTRUCTIVE CYBER ATTACK	18
INVESTIGATION OF THE EVENT	20
IMPLICATIONS	20
ANOTHER UKRAINIAN ACCOUNTING SOFTWARE PROVIDER WAS HACKED	20
WANNACRY – GLOBAL DESTRUCTIVE MALWARE ATTACK	21
INSIGHTS	21
ADDITIONAL FINDINGS STRENGTHEN THE LINK BETWEEN NORTH KOREA AND WANNACRY	24
MONITORING WANNACRY DISCUSSIONS ON RUSSIAN CYBERCRIME FORUMS	24
EQUIFAX BREACH	25
WHAT WAS STOLEN FROM EQUIFAX'S DATABASES	25
WHO ARE THE ATTACKERS	26
IMPERSONATION ATTEMPTS OF THE ATTACKERS FOLLOWING THE PUBLIC REVEAL OF THE BREACH	26
THE INVESTIGATION	27
THE STOLEN DATA SENSITIVITY	27
POSSIBLE ATTACKERS COURSE OF ACTION	27
BREACH TIMELINE	27
ATTACK TIMELINE	28
ATTACK VECTOR	28

ASSISTANCE FOR INDIVIDUALS AND COMPANIES THAT WERE POSSIBLY AFFECTED	28
CLASS ACTION LAWSUIT AGAINST EQUIFAX	29
OUR INSIGHT FROM THIS AND SIMILAR EVENTS	30
RECONSTRUCTING THE ATTACK	30
PARADISE PAPERS – LEAK EXPOSES TAX EVASIONS OF TRILLIONS OF DOLLARS	31
ATTACK VECTOR	31
CONNECTIONS TO ISRAEL	31
TIMELINE	31
EXPOSED ENTITIES	32
SIGNIFICANT RANSOMWARE ATTACKS	32
A RANSOMWARE ATTACK SHUT DOWN 70% OF DC POLICE SURVEILLANCE CAMERAS	32
SOUTH KOREAN WEB HOSTING FIRM PAYS A RANSOM OF ONE MILLION USD	33
RANSOMWARE ATTACKS AGAINST HOSPITALS AND HEALTHCARE ORGANIZATIONS	33
RANSOMWARE ACTIVITY IN ISRAEL	35
FRAUDULENT RANSOMWARE ATTACKS	35
NATION-STATE ATTACK TOOLS AND DOCUMENTS LEAKS	35
NSA LEAKS	35
CIA DOCUMENT LEAK VAULT7 AND VAULT 8	36
ATTACK AGAINST THE SWIFT GLOBAL BANKING SYSTEM	38
THE NORTH KOREAN ACTIVITY AGAINST THE GLOBAL FINANCIAL SECTOR	38
60\$ MILLION STOLEN FROM FAR EASTERN TAIWANESE BANK VIA SWIFT	40
HACKERS STOLE 4.5 MILLION DOLLARS FROM A BANK IN NEPAL BY HACKING ITS SWIFT SERVER	41
HACKERS ATTEMPTED TO STEAL A MILLION DOLLARS FROM A RUSSIAN STATE BANK	41
BEC ATTACKS	41
COMMON BEC SCENARIOS	42
RUSSIAN INTERVENTION WITH U.S. POLITICS AND PRESEDENTIAL ELECTION	43
ATTACK VECTOR	43
DESTRUCTIVE MALWARE ATTACKS AGAINST SAUDI ARABIA	44
DARKNET MARKET ACTIVITY DURING 2017	46
LEADING DARKNET MARKETS TAKEN-DOWN BY LAW ENFORCEMENT	46
SUSPICIOUS ACTIVITY REGARDING A LARGE DARKNET MARKET, AND THE SHUT-DOWN OF ANOTHER MAJOR MARKET BY RUSSIAN AUTHORITIES	47
TOP DARKNET MARKETS SHUT-DOWN, POSSIBLY DUE TO ANOTHER LAW ENFORCEMENT AGENCY OPERATION	48
CRYPTOCURRENCY PLATFORM ENIGMA COMPROMISED; OVER HALF A MILLION DOLLARS IN ETHEREUM STOLEN FROM USERS	49
RUSSIAN APT DRAGONFLY ATTACKS TARGETING CRITICAL INFRASTRUCTURE SECTORS	49
SHADOWPAD – CHINESE ATTACKS ON BANKS AND CRITICAL INFRASTRUCTURES VIA MALICIOUS SOFTWARE UPDATES	50
SWEDEN'S TRANSPORT AGENCY EXPOSED SENSITIVE DATA OF NEARLY ALL ITS CITIZENS BACK IN 2015	51
OUTLOOK WEB ACCESS BASED ATTACKS, MAINLY IN OFFICE 365 ENVIRONMENT	51
AN OVERVIEW OF THE DELOITTE HACK	52
 SIGNIFICANT ATTACKS AGAINST ISRAEL IN 2017	 53
 PERSISTENT IRANIAN ATTACKS AGAINST ISRAELI TARGETS	 53
JANUARY 01.17	53

FEBRUARY 02.17	54
MARCH 03.17	54
APRIL 04.17	54
MAY 05.17	55
JUNE 06.17	56
JULY 07.17	56
AUGUST 08.17	56
SEPTEMBER 09.17	57
OCTOBER 10.17	58
NOVEMBER 11.17	59
A SUMMARY TABLE OF THE IRANIAN THREAT AGENT OILRIG'S ATTACKS AGAINST ISRAELI IT COMPANIES	60
TENS OF THOUSANDS OF MALICIOUS EMAILS CONTAINING LOCKY AND TRICKBOT MALWARES SENT TO MULTIPLE ORGANIZATIONS IN ISRAEL	62
POPULAR ISRAELI INSTAGRAM ACCOUNTS COMPROMISED BY AN ARAB HACKER.....	62
TWO ISRAELI NEWS SITES DEFACED BY TURKISH HACKTIVISTS IN COMMEMORATION OF THE BALFOUR DECLARATION'S 100 YEAR ANNIVERSARY	63
PHISHING EMAILS IMPERSONATING 013 NETVISION'S EMAIL SERVICE E-BOX.....	63
A PHISHING ATTACK AGAINST THE ISRAELI MINISTRY OF ECONOMY.....	64
EMAIL ATTACKS (LIKELY GENERIC) AGAINST ISRAELI COMPANIES AND INDIVIDUALS.....	65
HAMAS ATTACK CAMPAIGN TARGETED ISRAELI SOLDIERS VIA FAKE FACEBOOK ACCOUNTS.....	67
FAKE SOCIAL MEDIA ACCOUNTS AND ANDROID APP STORE	67
BEC ATTACKS AGAINST ISRAELI COMPANIES	70
FIRST INCIDENT: ISRAEL POLICE JOINTLY WITH INTERNATIONAL LAW AGENCIES SHUT DOWN AN ISRAEL-BASED FINANCIAL CRIMINAL GROUP (CASE 278)	70
SECOND INCIDENT: TARGETED SPEAR BEC ATTACK AGAINST AN ISRAELI COMPANY	70
CONTINUED SPEARED BEC ATTEMPTS AGAINST ISRAELI COMPANIES	72
OPISRAEL 2017 – THE FAILURE OF ANTI-ISRAELI HACKTIVISTS.....	72
OPERATIONAL INSIGHTS FROM THE CAMPAIGN	73
SIGNIFICANT HACKS AND DATA LEAKS	73
DAFACEMENTS	74
DDOS ATTACKS	74
NOTABLE GROUPS AND INDIVIDUALS	75
ACTIVITY OF ISRAELI HACKERS	75
OPISRAELFREEJULY - ATTEMPTS TO RE-ENGAGE OPISRAEL CAMPAIGN	76
<u>TIMELINE – CYBER EVENTS AND ATTACKS 2017</u>	<u>77</u>

Significant Trends and Attacks in 2017

Major trends in 2017

Trends	Details and comments
Loss of effectiveness of the "Eggshell Security" methodology	In recent years, many organizations have invested considerable resources in hardening their outer security shell, while neglecting their inner-organizational security systems. This discrepancy is exploited in numerous ways by malicious actors. For example, the growing use of hybrid attack vectors that increase attackers' chances of breaching a target and then laterally move within its systems with relative ease.
Growing exploitation of the supply chain for various attack vectors	breaching a third-party service provider to execute an attack on a company that uses its services or products. In the NotPetya campaign a legitimate accounting software was exploited to distribute malware to thousands of companies, completely shutting down or destroying their computer systems. In Israel we identified an Iranian threat agent that breached numerous companies via their IT provider.
Exploitation of native vulnerabilities with OS and communication protocols	In the two most devastating campaigns (NotPetya and WannaCry) that took place during first half of 2017, the attackers used native vulnerabilities in Microsoft OS and communication protocols. In the second half, we have identified a continuation of this trend; notably the exploit of vulnerabilities leaked by ShadowBrokers. Further, in September attackers exploited vulnerability CVE-2017-5638 to breach the credit rating company Equifax.
Growing use of hybrid attack vectors	Combining several attack techniques, such as exploitation of supply chains together with exploitation of vulnerabilities. This year we saw a growing trend of brute-force attacks against organizational RDPs, followed by infection of systems with ransomware. However, it should be noted that this attacks vector has been identified in the wild almost exclusively against large companies and organizations.
Proliferation of attack tools	The timeframe from the moment an attack tool is made public and its use by malicious actors around the world is constantly becoming shorter. For example, the use of NSA's tool by North Korea - This trend is expected to continue in 2018.

Trends	Details and comments
1-Day attack	Using publicly known vulnerabilities. Attackers no longer must invest considerable time and resource to find unknown vulnerabilities, instead they follow public reports and exploit vulnerabilities between the time they are revealed, and the time companies update their security systems to resolve it.
Increase of wide -scale destructive attacks	Unlike attacks that have the goals of ransom or gathering intel, destructive attacks are executed with the intent of causing as much harm as possible to the target. This year was unprecedented with such attacks executed by nation-state attackers.

Main attack tools/vectors in 2017

Attack tools/vectors		
Ransomware/wiper malware	Over the last year we saw a dramatic increase in both proliferation and sophistication of ransomware attacks. Further, this year several major events happened in which attackers distributed wiper malware that masqueraded as ransomware with the aim of prolonging the attacks.	
Emails containing malicious attachments or redirect users to malicious sites	Spear phishing malicious emails or widespread malicious emails sent via botnets were used in a variety of phishing attacks such as BEC, malicious spam, or as a means of penetrating organizational systems. For example, in Q1 of 2017 alone, Kaspersky lab detected ¹ over 51 million malicious emails. In order to bypass security and email filtration systems, malicious actors began incorporating in their attacks social engineering techniques ² , For example, the Russian cybercrime group Carbanak contact business by phone and convince the representatives under various pretenses to open malicious attachments, thus insuring that they are compromised.	Most common files attachments used in email attacks
		.doc
		.exe
		.scr
		.xls
		.bin
		.js
		.class
		.ace
DDE – macro-less execution of malicious code in Office documents	In recent months a macro-less code execution method began receiving attention ³ . This method is based on a native Windows function named DDE (Dynamic Data Exchange). However, as Microsoft sees it as a native feature rather than a vulnerability, and have not released a security patch for it. When opening a document that exploits this method, the user is presented with two notifications which he must approve in order for the code to run. However, note that the attacker can modify some of the wording on the second notification to make it appear less suspicious. This is not a new method; however it is actively being used in the wild. Talos ⁴ has reported that this method was used in attacks impersonating the US SEC (Securities and Exchange Commission), presumably by the cybercrime group FIN7. Recently it was reported ⁵ that nation-state threat agents such as APT28 (aka Fancy Bear), are using this vulnerability. This attack vector is one of the reasons Office became the second most attacked software in 2017, At October 23 rd , Microsoft published a guideline on how to mitigate this issue ⁶ . Beside the recommendations to manually change Office values and Registry keys to disable the DDE fields and OLE links automatic, Microsoft advised users to install	.xml
		.rtf

¹ <https://securelist.com/spam-and-phishing-in-q1-2017/78221/>

² <https://www.malwarebytes.com/pdf/labs/Cybercrime-Tactics-and-Techniques-Q1-2017.pdf>

³ <https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/>

⁴ <http://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html?m=1>

⁵ <https://thehackernews.com/2017/11/apt28-office-dde-malware.html>

⁶ <https://technet.microsoft.com/en-us/library/security/4053440.aspx>

Attack tools/vectors	
	Windows 10 Fall Creator Update. This update enhances Windows Defender Exploit Guard's security capabilities by blocking DDE based malwares ⁷ .
Waterhole attacks	<p>The attacker creates a fraudulent site or abuse a legitimate site that is usually often visited by the target. In many cases the attacker lures the target to the site by using different methods such as phishing emails, spear phishing, etc. Once accessed the site usually serves malicious payload such as exploit code or malware.</p> <p>In cases of spear targeted attack, the attacker creates custom content to his target and his interests. Illustrating the magnitude of this attack vector, between Q1 and Q3 of 2017 Kaspersky identified over 72 million unique sites with malicious content⁸. Malicious actors have even started creating websites that imitate web browsers' warning of malicious sites.</p> <p>These types of sites most often download a malware or redirect the users to various fraudulent services that tricks them into providing sensitive information such as login credentials or credit cards details.</p> <p>Another common technique is creating a website with a minor almost invisible change in their URL. For example, early this year malicious actors registered the domain google[.]com that impersonates Google.com (the little G is in fact a Latin character). This method is growing and nowadays entire domains are registered with various languages that have similar character to English, thus increasing the difficulty of identifying a fake URL.</p> <p>Earlier this year we identified Iranian campaigns that used the same method to compromise computers of Israeli users.</p>
SQL Injection	An attacker exploits a website or application by escaping the SQL syntax in the application and can then execute code on the remote machine, this is typically achieved using login form or user controlled input which has not been properly sanitized. This year this vector grew by 62% compared to the same time last year ⁹ .
Malicious Android Apps	<p>Propagation of malicious apps via unofficial and fake App stores.</p> <p>Infecting users who reach waterhole attacks by exploiting a vulnerability to download and install an App (commonly with older android versions).</p> <p>Luring victims to download and install external APK files. For example, malicious versions of the Pokémon Go game, as the game was not released worldwide, many were tempted to install versions that malicious actors published online by various channels such as social networks.</p>

⁷ <https://blogs.technet.microsoft.com/mmpc/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/>

⁸ <https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/>

⁹ <https://www.akamai.com/uk/en/about/news/press/2017-press/akamai-releases-third-quarter-2017-state-of-the-internet-security-report.jsp>

Attack tools/vectors	
DDoS attacks executed with IoT botnets	This year we saw a 91% increase of DDoS attacks ¹⁰ . This is due in part to the exponential growth of the IoT (Internet of Things) market. i.e. "smart devices" that got infected by botnets such as Mirai.
RDoS (Ransom Denial of service) Extorting companies with threats of DDoS attacks	In the last quarter we noticed a dramatic increase of RDoS attacks in which malicious actors threaten companies with DDoS attacks unless they paid a ransom. For example, in June seven South Korean banks were extorted by the Armada Collective group for the sum of \$315,000 dollars. These types of attacks are becoming more and more prevalent as DDoS-for-hire services are getting more commonly and easily available.
Leveraging compromised accounts and cloud based systems (e.g. Dropbox, 365 and Gmail) to gain access to sensitive systems	leveraging cloud services to gain access to companies and organizations.

2017 Cyber event summary table – including the attack vector and scope of damage

Campaign	Target	Date	Attacker	Scope of damage	Attack vector
NotPetya	Ukraine	July	The attack is attributed to Russian Nation-State actors	Critical damage inflicted on about 2,000 Ukrainian and foreign companies operating in Ukraine. Some of the largest companies that were affected are: Maersk, Merck, FedEx	Propagation of a destructive malware impersonating a ransomware via an accounting software update
WannaCry	Global	April	The attack is attributed to North Korea	Thousands of computers of both individuals and companies/organizations were permanently corrupted.	Unprecedented global ransomware/destructive attack
Equifax	USA	September	Likely a Chinese Nation-State actor	Data pertaining to 143 Million individuals and companies was stolen.	Exploitation of OS and communication protocols' vulnerabilities – CVE-2017-5638

¹⁰ <http://info.corero.com/DDoS-Trends-Report.html>

Campaign	Target	Date	Attacker	Scope of damage	Attack vector
NSA attack tools leak	USA	August 2016 - ongoing	Hacker group - Shadowbrokers	Following the leak, a new set of cyber threat has evolved.	The NSA's attack tools were publicly leaked online.
Attacks against the banking system SWIFT	Global	2016 - ongoing	The attack is attributed to the North Korean group Lazarus	Hundreds of millions of dollars were stolen from various banks around the world. Theft potential of billions of dollars in the future.	Multiple vectors such as malware with sophisticated obfuscation capabilities – used to steal funds and issue fraudulent letters of credit.
Russian actors involvement in US and additional countries Elections (Brexit included)	USA and several other countries	Early 2017 - ongoing	Russian Nation-State actors	Undermining the political status-quo of western and pro-western countries.	Dissemination of sensitive/false information for sabotaging political process, wide scale usage of social platforms such as Facebook and Twitter.
Paradise Papers	Global	October	Unknown	The leaked documents exposed tax evasions of trillions of dollars. Sensitive financial documents were exposed, pertaining to numerous highly influential individuals from around the world including business people, politicians and even royalty.	As of writing this report, the breach vector was not revealed.
destructive attacks executed against Saudi Arabia	Saudi Arabia	- 2016 ongoing	The attack is attributed to Iranian Nation-State actors	Numerous Saudi organizations and companies were affected by this destructive attack.	The attack's goals appear to be espionage and disruption.
Ransomware and BEC (Business Email Compromise) attacks	Global	Ongoing	Various criminal actors	Hundreds of millions of dollars stolen from companies and organization from every sector.	Compromising computers via malicious emails attached with malware; luring victims to waterhole sites, hacking emails accounts which are used to send fraudulent emails.

Campaign	Target	Date	Attacker	Scope of damage	Attack vector
Spear targeted ransomware attack against public/private hospitals and additional healthcare providers	Global	Ongoing	Various criminal actors	Millions of dollars stolen, shutdown of vital healthcare operations	Core hospital systems infected and encrypted by ransomware.

Malicious activity trends in 2017

2017 registered a dramatic increase in malware activity, both with regard to proliferation and sophistication. This year Kaspersky¹¹ Lab has detected over 198 million malware samples¹² in Q3 alone. Concurrently, in Q3 2017 almost 400 million malware incidents were detected by Comodo¹³.

Furthermore, we have seen growing evidence¹⁴ this year that ransomware has become a highly profitable and organized “industry”. This complies with our 2016 end of year review in which we identified ransomware as being the most significant cyber threat of 2017.

Most attacked systems in 2017

In the second half of 2017, Microsoft Office became the second most attacks software, with 22.80% of all attacks (an increase from 10.26% in H1 2017); overtaking Android OS that now accounts for 22.71% of the attacked systems. This shift is due in part to the growing trend of DDE attacks that rely on Macro-less execution of malicious code via a native Office function.

Software	Percentage of the attacks
Browsers	35.00
Microsoft Office	22.80
Android OS	22.71
Java	7.62
Adobe Flash	5.48
PDF software	1.39

Most common ransomware families - 2017

Malware family	Percentage of the attacks
WannaCry	16.78
Crypton	14.41
Purgen/Globelmposter	6.90
Locky	6.78
Cerber	4.30
Cryrar/ACCFDFA	3.99
Shade	2.69
Spora	1.87
(generic verdict)	1.77
(generic verdict)	1.27

¹¹ <https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/>

¹² Defined by them as - unique malicious and potentially unwanted objects.

¹³ https://www.comodo.com/ctrlquarterlyreport/q3/Comodo_Q3Report_111417_HR.pdf#_ga=2.41741931.834119800.1510771011-900913835.1510771011

¹⁴ <http://www.securityweek.com/ransomware-booming-industry-continues-evolve>

Mobile threats – trends in 2017

Although the most significant cyber platforms are still computer systems, one of the fastest growing trends in 2017 was mobile devices malware attacks, with a sharp increase in both their occurrences and sophistication.

In Q3 of 2017, Kaspersky researchers detected over 1.5 million malicious installation packages – an increase of 20% from the previous quarter. Below are the most common mobile malwares identified in 2017:

Name	Percentage of attacked users
DangerousObject.Multi. Generic	67.14
Trojan.AndroidOS.Hiddad.an	7.52
Trojan.AndroidOS.Boogr.gsh	4.56
Backdoor.AndroidOS. Ztorg.c	2.96
Trojan.AndroidOS. Sivu.c	2.91
Backdoor.AndroidOS. Ztorg.a	2.59
Trojan.AndroidOS. Hiddad.v	2.20
Trojan-Dropper.AndroidOS. Hqwar.i	2.09
Trojan.AndroidOS.Hiddad.pac	2.05
Trojan.AndroidOS.Triada.pac	1.98
Trojan.AndroidOS. Iop.c	1.87
Trojan-Banker.AndroidOS. Svpeng.q	1.68
Trojan.AndroidOS.Ztorg.ag	1.63
Trojan.AndroidOS. Ztorg.aa	1.57
Trojan.AndroidOS. Agent.eb	1.57
Trojan.AndroidOS.Agent.bw	1.53
Trojan.AndroidOS. Loki.d	1.48
Trojan.AndroidOS. Ztorg.ak	1.47
Trojan-Downloader.AndroidOS.Agent.bf	1.41
Trojan-Dropper.AndroidOS.Agent.cv	1.29

DDoS attacks

This year we saw a significant increase in the frequency of global DDoS attacks. Over the last year, DDoS attacks nearly doubled, increasing 91% since January¹⁵. This is due in part to the exponential growth of IoT (Internet of Things), i.e. "smart" devices that have online capabilities that are infected by Botnets such as Mirai. Moreover, the market of DDoS-for-hire services is continually growing, enabling any malicious actor to execute massive DDoS attacks regardless of their technical capabilities.

However, two of the largest botnets were shut down this year. The first, named Kelihos, was shut down in April after Spanish authorities arrested the individual behind it, a Russian hacker named Peter Levashov¹⁶. The second, WireX, was taken down in August by coalition of tech firms¹⁷. Further, in December three hackers were arrested and were charged for allegedly creating and distributing Mirai botnet¹⁸.

¹⁵ <https://www.infosecurity-magazine.com/news/ddos-attacks-nearly-double-since/>

¹⁶ <https://www.technologyreview.com/s/604138/the-fbi-shut-down-a-huge-botnet-but-there-are-plenty-more-left/>

¹⁷ https://www.theregister.co.uk/2017/08/28/tech_firms_take_down_wirex_android_botnet/

¹⁸ <https://thehackernews.com/2017/12/hacker-ddos-mirai-botnet.html>

Most Significant Attacks in 2017

Petya/NotPetya – widescale destructive cyber attack

On June 27th, one of the largest and most destructive cyber-attacks took place, wiping thousands of computers, disrupting the operation of numerous companies in Ukraine and additional countries that conduct business with Ukraine. The dissemination vector for the malware was via a software update of a legitimate yet compromised third party provider. This attack vector, by the time of this attack was not observed in such magnitude.

The attack appears to be executed by Russian threat agents with the goal of inflicting as much harm as possible to companies and organizations in Ukraine. Below is a review of the attack.

The date of the attack

The attack took place the night prior to a Ukrainian holiday and vacation day – “constitution day”. The time was probably selected in order to inflict the most damage by insuring that there is little to no staff present to alert or mitigate the attack.

Main attack vector

Similarly to WannaCry, **the attack vector was not via email. Instead, the malware was disseminated via a weaponized software patch issued by a compromised program updater.** This is the first time this type of vector was seen in the wild in a large-scale attack.

The malicious software update was for an accounting software named MeDoc. This is a legitimate and highly popular software in Ukraine used for accounting, issuing digital invoices and reporting taxes. Further, there are indications that concurrently the attackers also executed a secondary infection vector via waterhole attacks by infecting a popular Ukrainian news site.

Post infection dissemination vector

After the malware compromised a computer it continues to spread within the company's internal networks by using the following two vectors:

First – stealing credentials from infected computers that have access to different computers’ admin\$ share. Note that malware propagated with this vector can also compromise up-to-date computers and servers that have the latest security patches.

Second – exploitation of the SMB v1 protocol vulnerability, same as WannaCry. Dissemination via this vector could only compromise computers that did not have the necessary security patches.

The malware and its objectives

This is a destructive malware and not a ransomware. i.e. the attackers did not seek financial gain, rather they aimed to wipe/corrupt the infected computer’s hard-drive, to cause as much possible harm. The malware encrypts the system’s files and then corrupts the hard-drive by erasing the MBR. As a result, even if the hard-drive is restored, the files cannot be recovered. Our assessment is that the strategic objective of the attack was retribution against Ukraine, in addition to creating deterrence.

Targets

The malware was used against companies and organization in Ukraine, In total it seems that about 2,000 companies and organizations were affected; amongst them, governmental offices, banks, corporations, as well as small to medium business. Further, as many international companies who operate in/with Ukraine also use MeDoc they too have sustained considerable damages. Amongst them are Maersk (the world largest shipping company), and TNT, who struggled for a long time to bring their operations back to normal. In one case, a U.S. security firm reported that a U.S based company operating in Ukraine (presumably TNT) had about 5,000 of their computers destroyed.

The attacker

According to the method of operation, and previous attacks, it seems almost certain as a Russian attack. However, it should be noted that as of yet, there is no forensic evidence to support this claim. Kaspersky lab has identified certain similarities between the code that was used against the Ukrainian power-grid infrastructure and the malware that was used in NotPetya. Furthermore, the Ukrainian secret service has issued an official statement blaming the attack on Russian special services¹⁹.

How to better prepare for future attacks

In the days following the attack, we spoke to multiple Information & Cyber Security Directors regarding the event and its ramification; below are our insights and conclusions:

1. Currently organizations do not have a viable way to inspect, and if needed, to block malicious software updates from legitimate sources. Accordingly, a similar attack against companies in Israel would have also caused considerable damage. As a result, it is imperative that we examine methods of monitoring software updates.
2. It is vital to maintain an organizational security baseline, with a key emphasis on – segmentation, implementation of strict authorization management, maintaining offline and comprehensive backup.
3. Information from this attack was reported sporadically, some of it was unclear, and often contained mistakes. As a result, organizations had to deal with the attack and decide the course of action while having only fragmented and inaccurate information. By improving the information pipeline, organization may receive more credible and accurate info, which in turn will enable them to implement better contingency plans to mitigate attacks (this is where Cyber Security services, Anti-Virus alerts and CERT alerts come in to play).
4. Companies that have offices in other countries around the world, must prepare for the possibility of promptly disconnecting compromised branch offices from the organizational network during an attack. However, it should be noted that if the attack vector contains a “time bomb” component, disconnecting the offices upon identification of the attack might still be too late, as seen with Maersk and TNT case.
5. Attack tools and vectors are continually evolving and creating new threats. Over the last four years the main attack vector was via email, and many organizations have been able to develop relatively effective defense mechanisms against it. However, these recent attacks exploit new vulnerabilities that necessitate organizations to reevaluate their defenses and develop new security measures.

¹⁹ <https://ssu.gov.ua/ua/news/1/category/2/view/3660#sthash.eXmK8lpy.Kg8ZGUD4.dpbs>

Investigation of the event

About a week after the NotPetya attack (aka Diskcoder / ExPetr / PetrWrap), the cyber security firm Talos²⁰ and ESET published investigative reports revealing new finding regarding the attack. Below is a review of the findings.

The attack began earlier than initial findings indicated. The malware was disseminated in April 2017 and not in late June

The initial infection vector was via a backdoor that was installed on the Ukrainian accounting software MeDoc. The attacker hacked their update server and altered the software to contain the backdoor. The first malicious version was issued to all the software's users during April 2017.

The wiper malware

The malware is a variant of Petya, a ransomware used by various criminal actors unrelated to the attacks against Ukraine. The attacker modified Petya's binary code to masquerade it as a typical ransomware – presumably to create confusion and disrupt counter actions.

Unlike criminal ransomware attacks that have financial gain objectives, in this attack, despite the fact that it encrypted data and demanded a ransom for recovery, the attacker had no intention of providing a decryption key, nor did he create adequate means to do so.

The backdoor's C2 server was MeDoc's updater server

The backdoor module did not use any external servers as C2. Instead the attackers reconfigured MeDoc's update servers to channel traffic to a different server under their control. By doing so, the traffic appeared legitimate, while the communication and data exfiltration was sent **over web cookies** which made it harder to trace.

Implications

Both the targeted organizations' security teams and security firms failed to identify the malware over a long period

Despite the fact that malware was disseminated to thousands of organizations back in April, and was used maliciously during that time²¹, it was not identified until it began its destructive activity.

There are no IOCs that could have indicated the malware traffic and block it.

Similarly to WannaCry and APT10's operations that target the supply chain, currently it is impossible identify, monitor and block malware traffic sent via legitimate channels by using malicious IPs and domains IOCs.

Another Ukrainian accounting software provider was hacked

In August, another attack in the same vein of NotPetya was feared after the Ukrainian accounting software “Crystal Finance Millennium” (CFM) had their web servers hacked²² and used to host malware. However, unlike NotPetya, the attacker did not compromise the CFM server, which is used to distribute software updates.

²⁰ <http://blog.talosintelligence.com/2017/07/the-medoc-connection.html?m=1>

²¹ <https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/>

²² <https://www.bleepingcomputer.com/news/security/ukraine-fears-second-ransomware-outbreak-as-another-accounting-firm-got-hacked/>

Additionally, the breach was identified several days prior to the Ukrainian Independence Day. This was a highly suspicious day as NotPetya also happened a day before a national holiday – the Ukrainian constitution day. However, according to the investigation, it appears that this attack was in fact generic and unrelated. As of early December, no similar attacks to NotPetya were executed against Ukraine.

WannaCry – global destructive malware attack

On Friday May 12th, WannaCry attack instigated an unprecedented global event, infecting and damaging over 230,000 computers across 150 countries within a single day. The malware, which was based on a vulnerability identified by the NSA and exposed by WikiLeaks, targeted Windows OS, including XP and 7. Many large private and governmental organizations that did not properly update their systems with the necessary security patches were affected.

Prior to the attack, Microsoft and numerous other software vendors issued security updates, however due to the underlining difficulties organizations and companies face to rapidly implement them concurrently to the evolution of the malware, it continued inflicting harm even several weeks after the event began.

For example, on May 19th, Honda had to shut down operation with one of their Japanese plants after its systems were infected by WannaCry malware²³. Several days later, on June 22nd, it was reported²⁴ that 55 Traffic Lights and Speed Cameras in Australia were taken down after an employee used an infected USB drive.

On October 20th, the US healthcare network FirstHealth was a hit several days earlier by a new WannaCry variant, shutting down and disrupting its operation for several days. However, FirstHealth's statement²⁵ emphasized that the attack was detected quickly and the malware did not spread to any vital systems, and that no patient information has been compromised.

Insights

1. The timeframe to prevent damage to the organization from the moment it has been alerted of the threat, has dramatically shortened

On the morning of Friday May 12th, the malware began spreading. Around midday various sources began reporting that UK NHS hospitals fell victim to a cyber-attack. Around 15:30 they issued a statement acknowledging that 16 NHS organizations were affected.

This statement, alongside other reports of similar attacks against a Spanish Telecommunication company, as well as alerts issued by the Spanish and British CERTs, indicated that this was indeed a unique and significant event. In turn, these led to a wide scale and global coverage of the unfolding events.

Within several hours it became clear to all cyber security organizations around the world that this is unique event. Further, it was apparent that this attack exploited Windows OS's SMB vulnerability. Most companies and organizations around the world began receiving alerts on the matter starting Friday May 12th around midday.

²³ <http://news.softpedia.com/news/honda-shuts-down-car-production-plant-due-to-wannacry-infection-516583.shtml>

²⁴ <http://news.softpedia.com/news/wannacry-virus-takes-down-traffic-lights-and-speed-cameras-in-australia-516614.shtml>

²⁵ <https://www.firsthealth.org/lifestyle/news-events/2017/10/network-downtime>

Other than official reports, there were numerous social media reports directly from victims and employees of various affected organizations. One notable source for real time reports regarding unusual events is Twitter; as was in this situation, during which many users Tweeted about major disruptions to their organizations' computer systems.

Insight 1

The timeframe between the identification and classification of the event as severe by various organizations (security companies, CERT, etc.), and alerting on the matter was several hours. However, many of the alerts and instructions on how to mitigate the attack, were ineffective. A large organization is incapable of updating all its systems in the necessary timeframe of several hours. A fundamental issue that keeps challenging organizations is their inability to quickly execute major changes to their systems, such as shutting down networks, servers and suspending the organizations operation.

2. No security company or cyber researcher can fully contain and respond to major global cyber event.

Even after thousands of security researchers have investigated the event, there are still many unanswered questions. As a result, companies and organizations are unable to adequately prepare themselves for a future event. Below are several of the most notable questions:

- a. **The initial attack vector has yet to be verified.** The fact that the initial attack vector hasn't been confirmed at this point, illustrates the shortcomings of cyber security eco-system. During the initial hours of the event it was reported that the attack vector was via emails attached with malware. These reports were proven wrong, and as of yet, no sample of such malicious email was identified. The current working assumption is that the attackers scanned certain IP ranges, identified computers with SMB vulnerabilities, and directly infected targeted address. Post infection, these computers became agent that further disseminated the malware. However, it should be noted that there is no evidence to support this theory. For the purpose of this discussion, it is possible that the initial infection vector was via an unknown vulnerability exploitation, which enabled the attackers to breach targeted organizations and infect them with the malware.
- b. **Who are the attackers and why did the malware have a Kill-Switch functionality?** The standing theory attributes the attack to North Korea (due similarities in the code to the Swift malware), however the reason for an "off button" remains unanswered.
- c. **Why the attacker did not implement a more sophisticated mechanism to collect the ransom money, and why did he not provide decryption keys.** The fact that the system for victims to transfer ransom payments was lacking (for example there were only three Bitcoin wallets), and the decryption mechanism were not activated (i.e. victims who paid the ransom did not receive decryption key), raises a lot of questions. Did the attacker not care about the money, or did he lack adequate capabilities which resulted in critical malware errors.

Insight 2

Organizations and companies are/will be required to operate in conditions of partial/complete uncertainty during these types of events. Organizations will find it difficult to handle the flow of reports during these types of events. Currently security firms do not have the capability to fully contain such an event within the timeframe that is needed to provide adequate real-time assistance for these organizations. The process of investigating, analyzing and exposing cyber-attacks is often lengthy and limited. In recent years the most prominent attack vector, in regard to organizations, was based on malicious emails and phishing. The willingness of organizations and companies to adapt to new vectors is fairly limited, and demands a reevaluation of the situation

3. Organizations' recovery time from this type of event is lengthy.

Many of the affected organizations took a long time to return to normal operational. Organizations' ability to recover following a major cyber-attack is slow and "painful". This is due to numerous reasons, chiefly the need to continue providing service to their customers throughout the attack, as well as the recovery period. The demand for IT departments to both operate compromised systems, while also cleaning them and bringing them back to normal operation, is nearly an impossible task.

Insight 3

A fast recovery for an organization/company from a debilitating event is impossible. Recovery is a complex process that entails numerous challenges, such as working while having a very limited understanding of the situation. This should be emphasized to all personal and echelons of management. Practicing and preparing for various scenarios will assist in shortening the response time, however it does not guaranty rapid recovery.

4. A basic level of info-security is crucial.

Achieving an organizational security baseline is fundamental. Most of the affected organizations were unable in fulfil the basic info-sec requirements needed to limit the scope of such cyberattacks. Three core pillars are critical to mitigate such attacks and listed below, although it should be noted that most of the organizations we work with are fully aware of them:

- a. **Installing security updates:** making sure that all your organization's computer systems (workstations, servers, routers, switches, software, etc.) and/or computer based systems, have the most current security patches. However, behind this statement there is a near impossible challenge. In our assessment large organizations' capability to ensure that every one of its servers are continually updated with security patches is practically unachievable. considering workstations the situation is better, as most organizations update their workstations within a timeframe of up to two months. This is compared to their server update schedule of two months to a year, and even several years for non-Microsoft based systems. Systems that cannot be updated with security patches should be removed from the network and segmented.
- b. **Compartmentalizing and segmenting the organization's network** to significantly minimize malware ability to disseminate within the organization's system. Further, the network segmentation and separation to different environments and components must implement principles of least privileged (PoLP; aka principle of least authority). i.e. promoting minimal user profile privileges on systems, based on users' job requirements.
- c. **Insuring that the system is backed up and is set up in a manner that allows quick recovery.** Creating a robust backup that on one hand is capable of surviving unharmed from a cyber-attack, and on the other hand will allow for a rapid recovery process following a debilitating attack that shuts down most of the organization's computer systems.

Insight 4

Old school "Eggshell security" methodology is becoming less relevant and efficient. Accordingly, organizations that continue using it are in harm's way. Implementing a comprehensive outer security system, while using less robust/forgoing internal security systems is no longer sufficient against new threats. In our assessment, in the near future we will see more and more attacks that target organizations that continue to maintain a strong outer security system, while neglecting to harden their internal security systems.

Additional findings strengthen the link between North Korea and WannaCry

In late May Symantec published a report²⁶ further supporting WannaCry's link to the North Korean threat agent Lazarus. This attribution is largely based on analysis of previous WannaCry versions that were used in targeted spear attacks throughout February, March and April 2017. With the exception of the penetration vector, previous versions are almost identical to the May variant. The attribution to the Lazarus group is primarily based on similarities of the code, overlap of infrastructures and similar method of operation.

February WannaCry variant

The first known WannaCry variant was identified on February 10th, when a single organization was infected with the ransomware, which spread within two minutes to around 100 workstations. The attackers achieved this by using several tools. Two notable ones are - a variant of Mimikatz (mks.exe), used to steal network passwords; the other, hptasks.exe, was then used to copy and execute WannaCry to other network computers, using the passwords stolen by mks.exe.

Of the five other tools that were identified on the attacked network, three were linked to Lazarus (two are variants of Destover - a tool used in the Sony Pictures attacks. The third is - Volgmer, a malware that was used by Lazarus in attacks against South Korean targets).

March – April WannaCry variant

From March 27th, at least five organizations around the world were infected by a new WannaCry variant. The penetration vector in these cases was deploying WannaCry via two different backdoors Trojans - Alphanc and Bravonc; both of which have been previously linked to Lazarus. Alphanc shares a considerable amount of code with another malware from the Destover sub-family that was used in the Sony Pictures attacks; while Bravonc communicates with a the same C2 server used by a sample of Destover, a known Lazarus tool.

WannaCry also shares custom SSL implementation and some code with a backdoor Trojan named Contopee, which has previously been linked to Lazarus. Moreover, WannaCry has the same obfuscation code as the Fakepude malware, which too was previously been linked to Lazarus.

Monitoring WannaCry discussions on Russian Cybercrime forums

WannaCry created heated discussions amongst cybercrime communities, primarily revolving around two main issues; the first is attribution and objectives of the attack, and the second is the ramifications of the attack on other cybercrime operations.

Regarding attack attribution and objectives, there seems that there is an agreement amongst the cybercrime communities that the objective of this attack was not financial, but rather political. Although most of the reports attributed the attack to the North Korean threat agent Lazarus, amongst the Russian cybercrime community **it is believed that United States is behind the attack**. This is based on the fact that Russia and China were hit the hardest. It should be noted that another possible explanation for this is that a large percent of the operating systems (as well as software) used in these countries are pirated, thus preventing them from installing Microsoft's security patches.

²⁶ <https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group>

On one of the most prominent cybercrime forums, various members called to stop selling and buying ransomware on the forum, due to the harm ransomware attacks have on other cybercrime operations.

These, according to the thread's OP and commenters are:

1. Ransomware attacks raise awareness to malware. Consequently, companies and organizations improve their cyber defense.
2. Ransomware attacks also raise info-security awareness amongst average users.
3. Due to ransomware attacks, it is becoming increasingly harder to use various attack vectors based on JS, DOC and Macros, as more and more organizations began blocking them.
4. They make it harder to distribute malware via spam.
5. Many compromised servers change their passwords.

Although there was a lot of support for this initiative, including from various notable and prominent criminal actors, there was also an adamant opposition by other users. As of writing this report it seems that this initiative did not succeed.

Equifax Breach



On September 7th the consumer credit rating agency Equifax Inc. reported that it fell victim to a large scale cyber-attack resulting in over 143 million records of individuals and companies being compromised. Most of the stolen data pertains to U.S., UK and Canadian citizen.

Equifax is one of the three largest American credit agencies, with extensive operations around the world. It aggregates and manages sensitive databases, including credit ratings of about 800 million citizens and companies.

What was stolen from Equifax's databases

From the company's statements and reports, it appears that three databases were compromised:

The first database, and most significant database contains 143 million records comprised primarily by the following data:

- SSN - Social Security Numbers
- Full names
- Dates of birth
- Addresses
- Driver's licenses numbers
- Credit ratings

The second database contains sensitive credit documents of about 200,000 entities. As of writing of the report, details regarding the content of these documents has not been revealed.

The third database contains records and details of about 209,000 companies, Equifax clients, including their credit information.

These records, and in particular those from the first DB (especially the SSN numbers), could be exploited for numerous malicious purposes such as theft of money, identify theft, executing fraudulent online transactions etc.

Equifax has noted in their statement²⁷ that it has found no evidence of unauthorized activity on its core consumer or commercial credit reporting databases.

Who are the attackers

As of writing this report, and in light that none of Equifax databases have been offered for sale on Darknet markets, it is becoming more likely that behind that attack was a presumably Chinese nation-state threat agent. Many of the attack tools used were Chinese, and as reported by Bloomberg²⁸, inside sources informed with the investigation claim that the attack was executed by two different groups.

This is similar to the method of operation implemented by the Iranians against Saudi Arabia and possibly Israel – one group does the preliminary groundwork by identifying the vulnerabilities and mapping possible attack vectors and targets, while the second group infiltrates the target's network and covertly exfiltrates the data.

First group – conducted preliminary reconnaissance identifying the Equifax servers' vulnerability. Also executed the initial breach.

Second group – exploited the vulnerability identified by the first group to laterally move within Equifax's network while exfiltrating large amounts of data. The attackers gathered any piece of valuable data they came across, however they also focused on several individuals; presumably people of notable value and interest to them.

Impersonation attempts of the attackers following the public reveal of the breach

Shortly after the attack became public, a ransom demand was posted on a Darknet for the sum of 600 bitcoins by a previously unknown group that goes by the handle "PastHole Hacking Team". The ultimatum that they gave was to pay the ransom by 15.09 or all they will publicly leak all of the data. Two days later it was revealed that this demand was fraudulent and this group was not behind the attack.

Several days later, new information about the breach was revealed, this time supposedly by the real attackers²⁹, who allegedly exposed the entirety of Equifax's website management system, as well as significant amount of new data regarding the attack that appear genuine.

However, the samples of the supposedly stolen records that provided by them, appear to be fake. Nevertheless, we cannot rule out that these are indeed that attackers, however in order to verify this, they are demanding an initial sum of 4 Bitcoins. If needed we can provide additional information regarding means of communication with these actors.

²⁷ <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

²⁸ <https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros>

²⁹ <http://spuz.me/blog/zine/3Qu1F4x.html>

The investigation

According to Equifax³⁰, on August 2, 2017, the cybersecurity firm Mandiant was contracted to assist in conducting a comprehensive forensic investigation. Mandiant, which is owned by FireEye, has been routinely linked to the investigation of nation-state attacks.

The stolen data sensitivity

In the United States, a Social Security Number (SSN) is a nine-digit number issued to US citizens, that is not meant to be disclosed. US citizens are advised not to expose them as they are used as a primary means of identification for numerous sensitive services, including government services³¹, such as tax reports and returns.

Possible attackers course of action

As of now, the attackers have not publicly exposed the stolen data. Their course of action will be dictated by their goals as well as by how Equifax and the U.S. government will respond. The attackers have several options:

- **To try and extort Equifax:** As was mentioned, there was one such fraudulent attempt (likely in order to make an easy profit while humiliating Equifax). Nevertheless, this option is still viable.
- **Sell the stolen data on Darknet markets:** The average asking price for a single SSN record on the darknet is \$1. According the potential for profit is of over \$100 million.
- **Use the data:** In order to execute various malicious actions, from stealing phone numbers and tax frauds.
- **Publicly leak the U.S citizens data:** This disrupting the capabilities of U.S. government agencies to identify citizens who require services.
- **If behind the attack is indeed a nation-state attacker:** They may cross-reference the data with data stolen from previous large breaches, such as Anthem and OPM, in order to create a comprehensive intelligence map of US citizens, including government and Department of Defense employees.

Breach timeline

November 2016? - According to an alert from Visa, the timeframe for the breach began around November 2016, however this claim has not been corroborated by other sources³².

May – July 2017 - Most of the information that was revealed so far, indicates that this was the timeframe for the breach and data exfiltration.

July 29, 2017 - The company identified the breach. It is unknown if they discovered it themselves or were notified about it from an external source (possibly the FBI).

September 2017 – Equifax publicly announced the breach. It is possible that the delay between the discovery of the breach and the reporting of it was due to instructions from law enforcement agencies with the purpose of assisting the investigation.

³⁰ <https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832>

³¹ <http://www.eweek.com/security/identity-verification-becomes-trickier-in-wake-of-equifax-breach>

³² <http://uk.businessinsider.com/visa-and-mastercard-alert-consumers-about-equifax-data-breach-2017-9?r=US&IR=T>

Attack timeline

March 6th 2017 - Apache posted a security notification regarding a vulnerability CVE-2017-5638, describing how it could be used to steal data from any company using their software. Apache also provided a security patch for the vulnerability. Equifax only installed this patch after the discovery of the breach.

March 7th 2017 - The information regarding the vulnerability was posted on the Chinese security website freebuf.com, on the same day that the exploit code was introduced into Metasploit, a popular penetration software.

March 10th 2017- Hackers scanned the internet for vulnerable computer systems and identified Equifax's Atlanta server.

From March 10th until late July 2017- The second group installed over 30 web shells, notably China Chopper³³, each on a different web address. This enabled them to continue operating in case some were discovered. The FBI issued a TLP: Amber alert with the files' IoC.

Attack vector

According to initial assessments, Equifax was breached via a critical vulnerability³⁴ CVE-2017-9805 (rated 7.5/10) with the Apache Struts Web Framework, that enables remote execution of code. This open source system is used by thousands of companies in the US to develop Java-based Web applications.

However, on 13th September 2017, Equifax publicly stated that the attackers in fact exploited vulnerability CVE-2017-5638 to breach their systems. On 15th September, the attackers posted screenshots of Equifax's website management system, while boasting how easy it was to access it, as Equifax used very simple passwords.

The security firm Contrast Security³⁵, were the first to suggest that CVE-2017-5638 was the vulnerability that was exploited. This vulnerability, which was first discovered by Cisco's Talos Team in early May 2017³⁶, enables attackers to execute HTTP requests to Sturt Apache servers prior to authentication.

According to the researcher's assessment, this vulnerability was used to interrogate the database in order to exfiltrate data. They claim that this vulnerability seemed much more likely because it is easier to exploit, much better known, and also better fits the timeline. Nevertheless, much is still unknown, accordingly, the possibility that a 0-Day-Exploit was used concurrently with vulnerability CVE-2017-5638 cannot be ruled out.

Moreover, Apache stated that it appears that Equifax did not apply patches for flaws discovered in 2017³⁷. Note that this Apache platform is also used in the products of companies such as Oracle and Cisco. As such it should be checked whether the systems of these companies have been updated with security patches.

Assistance for individuals and companies that were possibly affected

Equifax is offering every citizen a tool to check if their records have been compromised³⁸. However, it appears that this tool is not working properly and provides unreliable results. For example, when it was launched CNET tried

³³ <https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html>

³⁴ <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9805>

³⁵ <https://www.contrastsecurity.com/security-influencers/a-week-of-web-application-hacks-and-vulnerabilities>

³⁶ <http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html>

³⁷ <https://threatpost.com/apache-foundation-refutes-involvement-in-equifax-breach/127910/>

³⁸ <https://trustedidpremier.com/eligibility/eligibility.html>

this tool with fake names and SSNs and was told that their records have not been compromised³⁹. In other cases, Twitter users have reported⁴⁰ to receive the opposite results when inputting false data.

Moreover, this tool was raised concerns on many security issues. Most notably was the fact that it was hosted on the stock WordPress platform, which is a cause for concern when considering the sensitivity of the data that is requested to be provided by the users. Furthermore, it was reported that initially the domain was not registered to Equifax's name (although this was later changed).

when the site was launched, one of its pages was displaying, prior to being taken down, the administrator's username⁴¹. For these reasons, in addition to issues with the site's SSL certificates, Cisco's DNS service provider OpenDNS, flagged the site as suspicious as phishing⁴².

These problems are not limited to this site. It was reported that concurrently, Equifax's main website was displaying debug codes. While this is not a critical security issue, it is something that should never happen on any production server, and may indicate the grave distress that Equifax was and possibly still in.

Another option that Equifax is offering its clients is a free monitoring service that tracks their accounts for any suspicious activity. It should be noted that initially it was reported that according to the service's "term of use", clients who sign up waived their rights to sue Equifax. However, later it was revealed that this arbitration clause, even if Equifax would have wished to enforce it, is not legal in such events as this⁴³. Equifax later removed this clause from the terms of use.

Following the revelation of the breach, Equifax announced on 11.09 that it is changing the PIN generator for clients who wish to enact a security freeze for their accounts. The new system now generates random numbers rather than the sequential ones that were issued up to that point⁴⁴. The old numbers were essentially date-time stamps, and could potentially be brute-forced to unlock a credit report for malicious purposes such as identity theft⁴⁵.

In light of these developments, many U.S. citizens opted to enact a security freeze on their accounts, however Equifax was not adequately prepared, on 13.09 their systems crashed for about an hour around 17:00 EST.

Class action lawsuit against Equifax

Following the attack, many citizens affected by the breach have filed a class actions lawsuit claim against Equifax⁴⁶. The company does have an insurance policy against cyber breaches for the sum of about \$100 million to \$150 million, however it is likely inadequate to cover the losses⁴⁷. If they win the lawsuit, Equifax will have to pay reparations of hundreds of millions and possibly billions of dollars, which in turn may cause it to go bankrupt. one of the class lawsuits is seeking as much as \$70 billion in damages.

Since exposure of the breach the company's stocks have crashed 35% to a low of \$92 (as of 15th September) compared to \$142.72, a day prior to the reporting. shortly after the breach was discovered by the company, three

³⁹ <https://www.cnet.com/how-to/psa-equifaxs-hack-checker-is-a-hot-mess/>

⁴⁰ <https://twitter.com/GUHoyas777/status/906340885042003968>

⁴¹ <https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/>

⁴² <https://www.bleepingcomputer.com/news/security/highly-sensitive-details-of-143-million-users-stolen-in-equifax-hack/>

⁴³ <https://www.cnet.com/news/equifax-breach-hacked/>

⁴⁴ <https://twitter.com/webster/status/907242378829889537/photo/1>

⁴⁵ <https://arstechnica.com/information-technology/2017/09/equifax-moves-to-fix-weak-pins-for-security-freeze-on-consumer-credit-reports/>

⁴⁶ <https://www.bloomberg.com/news/articles/2017-09-08/equifax-sued-over-massive-hack-in-multibillion-dollar-lawsuit>

⁴⁷ <https://www.bloomberg.com/news/articles/2017-09-09/equifax-s-insurance-said-likely-to-be-inadequate-against-breach>

of its senior directors sold stocks options in the sum of about \$2 million, several weeks before the breach was publicly announced⁴⁸.

In subsequent months, stock prices have rallied, and stabilized at around US\$110. Nevertheless, the company's profits dropped by 27% like-for-like on the previous year ⁴⁹ as of late November. Additionally, reparations in the form of free monitoring to affected Equifax clients has cost the company about US\$5 million to date and is expected to reach up to US\$110 million according to company sources.

Our insight from this and similar events

The "safe" timeframe that companies hold to update a security patch, notably with regards to online systems, has been reduced to 24 hours. In our assessment, many of the large organizations and companies hacks that took place over the last year, were based on 1-day vulnerabilities.

These are almost as effective as 0-day vulnerabilities, as it takes most companies and organizations a relative long time to install security patches. Further, they do not require from the attackers' much resources to identify them.

- As of December 4th the attackers have not publicly leaked the stolen data.
- There is still much that is unknown; notably the identity of the attacker and the vector of the attack.
- The event has not yet ended. The first ransom demand was fake; however, it is still likely that the real attacker will surface and demand a ransom. If the data is publicly leaked, many U.S. citizens as well as Equifax will be gravely affected.
- in case of a nation-state attacker (such as North Korea, Russia or China), the U.S. authorities have a wide range of tools to use against such attacker in order to prevent them from publicly exposing the data. However, it is also possible that a nation-state actor such as North Korea would hold the data hostage as an insurance against an attack by the states.
- Patching the Apache framework vulnerabilities is a challenge and time-consuming task. It is used by many hardware and software companies' applications. As such, Oracle and Cisco both issued alerts on the matter. It is possible that other companies are using this framework in their products. Accordingly, it is advised to verify and address this issue.

Reconstructing the attack

One of the challenges a hacked company faces is retracing the attackers' operation and braking down their attack vector. Nevertheless, Equifax apparently was able to almost fully reconstruct every step of the attack, as prior to the attack it implemented an open source monitoring tool⁵⁰ named "Moloch", which kept a record of the company's network's internal communications and data traffic.

We recommend examining implementation of the tool within your organization.

⁴⁸ <http://uk.businessinsider.com/equifax-executives-sold-shares-after-the-company-learned-of-a-massive-hack-2017-9?r=US&IR=T>

⁴⁹ <https://investor.equifax.com/news-and-events/news/2017/11-09-2017-211550295>

⁵⁰ <https://github.com/aol/moloch>

Paradise Papers – leak exposes tax evasions of trillions of dollars

On November 5th (aka Guy Fawkes day⁵¹), 13.4 million financial documents and records for assets in the sum of \$10 Trillion were leaked⁵². The leak was reported by ICIJ (International Consortium of Investigative Journalists); a fully independent organization, comprised by hundreds of investigative journalists from around the world, who work to expose corruption.

Attack vector

The computers of the Appleby law firm were hacked. After the documents were exposed, they issued an official response blaming "professional hackers", who covered their tracks. Further, according to the firm, a forensic investigation conducted by a "leading international Cyber & Threats team" found no conclusive evidence that any data was exfiltrated from their systems. They also claim that that this was not an inside job, and that the attackers were not assisted by anyone from within the firm.

Connections to Israel

As of writing this report, the full list of documents has not been released. Accordingly, the full scale of the Israeli stakeholder exposure cannot be determined yet. According to the Israeli journalist Uri Blau⁵³, who a member of ICIJ, the word "Israel" appears in over 20,000 documents. Some of which are related to referrals of Israeli companies to the law firm.

The Israelis who are exposed at this point are – Idan Ofer that allegedly purchased a private jet via offshore tax-exempt company, the mining tycoon Dan Gertler who according to Ha'artz⁵⁴, "appears in 120 documents regarding his relationship with Glencore, a company that uses Appleby's Bermuda branch for much of its business".

Timeline

In October 2017, Appleby law firm's computer network was hacked, and over 13 million documents related to tax evasions were exfiltrated.

About two weeks before the documents were exposed (20.10), an anonymous post⁵⁵ was posted on the Panama Reddit thread with the headline "Do not give up. More is coming.", claiming that a major leak, similar to the Panama



⁵¹ On November 5th, 1605, a group of anarchists, headed by an individual named Guy Fox, attempted to bomb the Palace of Westminster (the meeting place of the House of Commons and the House of Lords), and kill the king and members of parliament, thus destabilizing the government. This failed plan, named "the gunpowder plot", inspired the novel "V for Vendetta". The novel and the 2006 movie adaptation made Guy Fawkes to one of the most prominent symbols for anarchism. Later, the Guy Fawkes image was adopted by Anonymous, who commemorate him on every November 5th by executing various "operations".

https://en.wikipedia.org/wiki/Guy_Fawkes

<https://pastebin.com/Qz8vZW8h>

⁵² <https://www.standard.co.uk/news/world/what-are-the-paradise-papers-and-who-has-been-named-in-the-leaked-documents-a3677066.html>

⁵³ <https://www.themarket.com/allnews/1.4568967>

⁵⁴ <https://www.haaretz.com/israel-news/1.821229>

⁵⁵ <https://qz.com/1120925/paradise-papers-reddit-user-hinted-at-data-leak-16-days-before-news-broke/>

Paper is about to go public. The post was signed with "Paradise"⁵⁶.

The Paradise Papers documents were sent anonymously, at an unreported date, to the German newspaper Süddeutsche Zeitung. This is the largest newspaper in Germany, who published in 2016 the Panama Papers.

After receiving the document, Süddeutsche Zeitung sent them to ICIJ for examination. On November 5th ICIJ uploaded to its website some of the documents⁵⁷.

Exposed entities

The exposed documents detail over 120,000 individuals and organizations from around the world. The list includes past and present head of states, members of parliament, prominent business people, artists, athletes, major companies, etc. Amongst them are notable individuals such as Queen Elizabeth II, President of Colombia Juan Manuel Santos, and U.S. Secretary of State Rex Tillerson.

The complete list has not yet been released, however large portions of it are available online⁵⁸. Further, all of the head of states directly involved were exposed. ICIJ has on its site a platform that allows to review the available documents.

Significant ransomware attacks

A ransomware attack shut down 70% of DC Police surveillance cameras

On January 12th, a ransomware attack affected 70 percent of the public surveillance cameras employed by Washington D.C. The attack took place only eight days prior to the inauguration of U.S. president Donald Trump. It was discovered after DC police noticed that four of their camera sites were not functioning properly, and that they could not access video from their DVRs.

The investigation further revealed that in total 123 of 187 network video recorders were compromised by two ransomware variants. Consequently, the affected CCTV cameras were unable to record public surveillance footage between January 12th and 15th. However, D.C.'s Chief Technology Officer, told The Washington Post that their system was design to prevent ransomware from propagating onto other networks, and as a result there was no access from these devices into their environment. Further, the police department stated that no ransom was paid, and the system was restored to full functionality.

As of writing this report, both the attacker and the penetration vector are unknown. However, it is presumed that the infection was enabled because the camera sites were connected to public Internet for remote access⁵⁹.

In early March, it was reported that two suspects, a British man and Swedish woman were arrested in London in relations to the attack⁶⁰. In late December it was reported⁶¹ that two Romanians were arrested in Bucharest, and now face charges of conspiracy to commit wire fraud and conspiracy to commit various forms of computer fraud.

⁵⁶ https://www.reddit.com/r/PanamaPapers/comments/77n6ix/do_not_give_up_more_is_coming/

⁵⁷ These are available via the following link - <https://www.icij.org/investigations/paradise-papers>

⁵⁸ https://en.wikipedia.org/wiki/List_of_people_and_companies_named_in_the_Paradise_Papers

⁵⁹ <https://www.grahamcluley.com/ransomware-attack-impacted-70-washington-dc-police-surveillance-cameras/>
<https://arstechnica.com/security/2017/01/dc-police-surveillance-cameras-were-infected-with-ransomware-before-inauguration/>

⁶⁰ <http://thehill.com/policy/cybersecurity/317762-uk-arrests-two-in-conjunction-with-dc-camera-ransomware>

⁶¹ <https://thehackernews.com/2017/12/police-camera-hacking.html>

South Korean web hosting firm pays a ransom of one million USD

The South Korean company Nayana paid \$1 million ransom after it fell victim to a ransomware attack encrypting 153 of the company's Linux servers, hosting 3,400 websites. This sum was paid after a negotiation with the attacker who originally demanded four times the amount⁶².

Ransomware attacks against hospitals and healthcare organizations

Continuing on from 2016, 2017 bore witness to a significant increase in ransomware attacks against healthcare organizations. Due to the critical nature of hospitals and healthcare providers, and the extensive and possibly immediate damage that can take place if systems are shut down, these organizations are invariably forced to pay the ransom. Below are several notable attacks from the last year.

Ransomware attacks against UK NHS hospitals

UK's National Health Service (NHS), fell victim to several significant attacks over the last year, most notable was WannaCry, in which it was one of the first to report being hit; however, this was only the latest of a series of attacks against its hospitals.

In November 2016, they reported that the operation of three of its hospitals were impacted following a Globe2 ransomware attack⁶³. About two months later, on January 13, it was reported that six London hospitals operated by "Barts Health NHS Trust" were attacked by a Trojan, which forced the hospitals to partly shut down their IT systems, the malware penetration vector is yet unknown.

Initially it was reported as ransomware attack, however the trust stated that this is not the case, and that they were infected by a Trojan that had not previously been seen. According to them, "whilst it had the potential to do significant damage to computer network files, our measures to contain the virus were successful". Additionally, the trust's stockperson emphasized that at no point patient medical records were compromised, and that medical services for patients were not affected.

Ransomware attack against NHS Lanarkshire hospitals

On August 18th, several Scottish hospitals that are part of NHS Lanarkshire, were infected by a sophisticated variant of the Bit Paymer ransomware⁶⁴. The attack shut down the systems of the hospitals, which were badly hit several months prior during the WannaCry attack. The recent penetration vector was via brute force attacks on exposed RDP endpoints⁶⁵. After gaining access to one of the systems, the attackers laterally moved on the compromised network and manually installed the malware on additional stations.

As of writing this report, there is no way to decrypt files that were encrypted by this ransomware. It should be noted that ransomware attacks that use Bit Paymer often demand remarkably large ransoms. In this attack, the attacker demanded 53 Bitcoins (roughly \$230,000 equivalent when the attack took place).

Widescale ransomware attack targeting ECMC hospital shuts down its computer network

In early April, the NY hospital ECMC (Erie County Medical Center) fell victim to a cyber-attack. Its computer systems were infected by a ransomware that encrypted most of its hard-drives. According to the hospital, following the

⁶² <https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/>

⁶³ <http://www.zdnet.com/article/trojan-malware-blamed-for-cyberattack-at-barts-health-nhs-hospitals/>

⁶⁴ <https://www.bleepingcomputer.com/news/security/bit-paymer-ransomware-hits-scottish-hospitals/>

⁶⁵ <http://www.healthcareitnews.com/news/wannacry-victim-nhs-lanarkshire-hit-new-ransomware-strain>

discovery of the attack (apparently after receiving the ransom notice), its IT team shut down the entirety of the hospital's computer network in order to contain and prevent a spread of the infection. Although the hospital did not disclose the exact details of the type of attack they experienced, it seems that it was a ransomware that was sent to them via email alongside a social engineering attack.

However, the hospital's spokesperson noted that there are no indications that any of the hospital's patient medical records were compromised⁶⁶. Following this event, the hospital scaled down its operation, and instructed its staff to use pen and paper to conduct records, having no access to their patient and operation's registry systems, website and email services.

According to the reports, and despite the hospital's efforts to understate the scale of the attack, it seems that attack impacted all the hospital's networks. Consequently, the hospital was forced fully restore all the compromised systems, taking over a month to return to normal operation.

2017 is on Track to outpace 2016 in regard to healthcare data breaches

According to a report by the healthcare data security company Protenus⁶⁷, 2017 is outpacing 2016 in regard to attacks against healthcare providers, with over a breach or ransomware infection a day. In H1 of 2017 alone, 233 breaches were reported to the HHS (US Department of Health & Human Services), with 41% of them caused by internal factors, be it human error, technical error or malicious action.

Moreover, it should be stated that it appears that the actual scale of attacks is considerably larger than the official numbers indicate, as many events are under-reported or even unreported. For example, this year thousands of databases from all sectors were stolen or corrupted in attacks described as "ransacking", however only a fraction of those incidents was reported to the HHS.

It seems that many companies and organizations chose not to report ransom attacks, regardless if the ransom was paid, believing that the data was only deleted without considering that the attackers copied it with the intent of selling it.

On average, based on date from the reported incidents, it currently takes healthcare organizations 325.6 days (median - 53 days) to discover a breach. The reason for the drastic difference between the mean and median is due to the extreme range of this data. According to the report, some entities discovered a breach immediately, while other incidents went undiscovered for years.

Based on data from reported incidents, it took healthcare organizations on average 57 days from the time a breach was detected until it was reported (median – 57). This is significant improvement over previous years, and now complies with the HHS' mandated 60-day reporting window. This was due in part to the fact that the HHS began fining organizations that failed to do so.

⁶⁶ <http://buffalonews.com/2017/04/21/ecmc-hit-cyberattack-continues-massive-task-restoring-computer-functions/>

⁶⁷

https://www.protenus.com/hubfs/Breach_Barometer/2017/Mid%20Year%20Review/2017%20Protenus%20Breach%20Barometer%20Mid%20Year%20Review.pdf?utm_campaign=Breach+Barometer&utm_medium=email&_hsenc=p2ANqtz-_ih8kwB15UPZBdGIha4KFI9963vuXgyt9ufyzVIDT98z1Da1LbyUNK-HkVnC1bBQMvmxn0rq3hjP3qPDedeqvX68P_Vg&_hsmi=54901109&utm_content=54901109&utm_source=hs_email&hsCtaTracking=6a0222c0-31dd-468e-a6e2-8c2538a8fea0%7C4be65339-88e0-4f55-a1a2-fadffbeb8c03

Ransomware activity in Israel

In early March, we were alerted regarding a malicious email impersonated an Israeli financial organization, and containing a malware⁶⁸, later identified as Stampado⁶⁹. This ransomware is available on Darknet markets for about \$40 USD⁷⁰. However, it should be noted that Stampado has a public decryptor that enables user to decrypt their system for free⁷¹.

The email messages were sent from a mailer service, hosted on a hacked web server located outside of Israel. The email was written with broken English (this indicates that the attacker does not speak Hebrew, and that English is not his mother's tongue).

The malware was hosted on a domain registered by the attacker, and impersonated the Israeli site Walla. Further, this address was previously used in November 2016 to host a phishing site that impersonated a financial organization. According to this event's characteristics, our assessment is that these are small scale attacks, presumably executed manually, possibly by a sole actor located in Syria.

Stampado has multiple variants. One of the most notable one is named Philadelphia, which has several advanced capabilities such as automatically identifying when the ransom is paid and then decrypting the files, infecting removable devices such as thumb drives, and infecting additional computer on a shared network. Further, it has a unique feature of a "Mercy Button" that allow the attacker to decrypt the files according to his discretion, even if the ransom was not paid.

Fraudulent ransomware attacks

A research by Citrix Systems⁷², exposed a new type of scam dubbed "bluff ransomware attacks", in which attackers, via various social engineering techniques and other methods, fool companies to think that they fell victim to a ransomware attack, and must pay a ransom in order to regain access to their databases/systems. According to the report, 39% of large businesses in the UK have experienced such an attempt, and 61% of them choose to pay the ransom. The average ransom was 13,500 pounds, however 6% of the companies paid over 25,000 pounds.

Nation-state attack tools and documents leaks

NSA leaks

Starting August 2016⁷³, a hacker group that goes by the handle Shadowbrokers began leaking various NSA hacking tools and exploits⁷⁴. In May the group began offering a paid "monthly dump service"⁷⁵; a subscription plan providing private members with exclusive access to future leaks. This service was originally offered for 100

Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - FULL LIFETIME LICENSE

Stampado Ransomware - You always wanted a Ransomware but never wanted to pay hundreds of dollars for it ? - This list is for you! :)

Stampado is a cheap and easy to manage ransomware, developed by me and my team. It...

Sold by **The_Rainmaker** - 2 sold since Jul 12, 2016 **Vendor Level 1** **Trust Level 5**

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

⁶⁸ For additional information, see our weekly cyber intelligence report 13.03.17

⁶⁹ [virustotal.com/en/file/08c4db8bf0ef8db94f5016c7e532518ffe77b6b97365a807b62175ea05ac2b3a/analysis/](https://www.virustotal.com/en/file/08c4db8bf0ef8db94f5016c7e532518ffe77b6b97365a807b62175ea05ac2b3a/analysis/)

⁷⁰ <https://heimdalsecurity.com/blog/security-alert-stampado-ransomware-on-sale/>

⁷¹ <https://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/>

⁷² <https://www.scmagazineuk.com/bluff-ransomware-attacks-cost-companies-over-13000-per-sham-attack/article/633666/>

⁷³ <https://arstechnica.com/information-technology/2016/10/new-leak-may-show-if-you-were-hacked-by-the-nsa/>

⁷⁴ https://www.theregister.co.uk/2017/04/10/shadow_brokers_open_sources_hacker_trove/

⁷⁵ <https://www.bleepingcomputer.com/news/security/the-shadow-brokers-announce-details-about-upcoming-monthly-dump-service/>

ZEC (Zcash coins – worth about \$21,000 at the time) per month⁷⁶, however in June they doubled the price to 200 ZEC⁷⁷.

Further, they also announced a VIP service for a onetime fee of 400 ZEC, that will allow members to the ask questions about the exploits and data dumps, as well as request from the group for specific exploits.

CIA document leak Vault7 and Vault 8



On March 7th 2017, WikiLeaks released⁷⁸ about 9,000 documents regarding the CIA's cyber operation. This was the first leak which led to a series of 23, known as Vault 7, and followed by a new series called Vault8.

It appears that most of the CIA tools were largely used to spy on specific individuals, by directly compromising the targets' devices, rather than widescale lateral monitoring as conducted by the NSA. Accordingly, most of the tools exposed in the leak primarily target personal computers and mobile devices (although it should be noted that several of the tools target routers by Cisco and possibly other vendors). Since Vault7 began, some of the tools' source code has also been leaked, and is being used in the wild.

Leak Number	Date of leak	Name of leak	Details
Part 1	March 7	Year Zero	8,761 documents and files regarding CIA hacking exploits for popular hardware and software.
Part 2	March 23	Dark Matter	Document leak, including documents regarding CIA attempts to hack Apple Mac computers and iPhones.
Part 3	March 31	Marble Framework	676 lines of code for a malware signature obfuscation tool.
Part 4	April 7	Grasshopper	27 documents regarding the CIA's malware development platform for Microsoft Windows operating systems named "Grasshopper".
Part 5	April 14	HIVE	6 documents regarding the CIA malware management system named "HIVE". It appears ⁷⁹ that this was related also to a threat agent named "Longhorn".
Part 6	April 21	Weeping Angel	Documents regarding a hack tool for smart TVs that was jointly developed by the CIA with the British MI-5.
Part 7	April 28	Scribbles	Documents and source code of a monitoring tool intended to spy on journalists and whistleblowers.
Part 8	May 5	Archimedes	Documents regarding a tool named Archimedes (aka Fulcrum).
Part 9	May 12	AfterMidnight and Assassin	AfterMidnight – an espionage malware that imitates DLL files. Assassin – similar to AfterMidnight, but runs within a Windows service process.

⁷⁶ <https://thehackernews.com/2017/05/shadow-brokers-exploits.html>

⁷⁷ https://www.theregister.co.uk/2017/06/29/shadow_brokers_threaten_nsa_hacker/

⁷⁸ <https://wikileaks.org/ciav7p1/>

⁷⁹ <https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7>

Leak Number	Date of leak	Name of leak	Details
Part 10	May 19	Athena	Documents regarding two malwares – Athena and Hera.
Part 11	June 1	Pandemic	Documents regarding a malware dissemination tool.
Part 12	June 15	Cherry Blossom	Documents regarding a hacking tool for wireless networking devices.
Part 13	June 22	Brutal Kangaroo	Documents regarding a CIA operation to infiltrate closed networks (or a single air-gapped computers) within organizations without direct access.
Part 14	June 28	Elsa	Documents regarding a geo-location monitoring malware for WiFi-enabled Windows based devices.
Part 15	June 30	OutlawCountry	Documents regarding a hacking and data exfiltration tool from Linux-based systems.
Part 16	July 6	BothanSpy	Documents regarding tools (BothanSpy and Gyrfalcon) developed to steal SSH credentials from Windows and Linux-based systems.
Part 17	July 13	Highrise	Documents regarding a tool named Highrise (aka TideCheck) that intercepts and redirects SMS messages to a remote web server. The tool was developed for Android-based devices.
Part 18	July 19	UCL / Raytheon	Documents regarding a CIA subcontractor that analyzed in-the-wild malware, developed attack tools, and provided the CIA with information on how to develop their malware projects.
Part 19	July 27	Imperial	Documents regarding a hacking tool for Apple Mac OS X and various Linux systems.
Part 20	August 3	Dumbo	Documents regarding a CIA project, exposing the agency's capability to remotely take control of Web cams and even corrupt/delete video recordings.
Part 21	August 10	CouchPotato	Documents regarding a CIA tool to covertly intercept real time live video steaming.
Part 22	August 24	ExpressLane	Documents regarding an espionage tool developed by the CIA to steal biometric data from other intelligence agencies. The tool's penetration vector is by impersonating a software update for the biometric management system.
Part 23	August 31	Angelfire	Documents regarding a hack tool for Windows OS. Persistency is achieved by modifying the partition boot sector and installing a backdoor. The tool has five different components: Solartime, Wolfcreek, Keystone, BadMFS and Windows Transitory File system.
Part 24	September 7	Protego	Documents regarding a guided missile control system that was developed for the CIA by Raytheon ⁸⁰ .

⁸⁰ <https://www.raytheon.com/>

Leak Number	Date of leak	Name of leak	Details
Part 25	November 9	Vault 8	The source code of HIVE, the CIA's malware management software.

Attack against the SWIFT global banking system



Continuing on from the series of SWIFT hacks that took place in 2016, including the Bangladesh Central Bank breach in which \$81 million were stolen, in early January 2017, hackers breached the SWIFT servers of three different banks owned by the Indian government (two in Mumbai and one in Calcutta), and created fake Letters of Credit to be used in fraudulent global business deals.

This breach is unique because no funds were stolen and no ransom was demanded from the banks. Instead, the attackers exploited the banks' systems to issue trade documents such as letters of credit and guarantees. Accordingly, it is presumed that malicious actors will use the stolen document in order to execute fraudulent and illegal business transactions.

Letters of Credit (aka LC or documentary credit) is a written undertaking issued a bank or other financial organization to pay a beneficiary against the delivery of a specified set of documents. LCs are used primarily in large international business trades. Moreover, LC are non-rescindable documents, i.e. once the letter is sent from the beneficiary's bank, as long as all the stated conditions are complied, the letter cannot be revoked. Accordingly, it is feared that the Indian banks will face in the future LC encash demands.

Currently, the identity of the attackers is unknown. In our view, this is due to two possibilities. The first is that the attack was perpetrated by a large international cybercrime group, who carried it out in order to trade prohibited or illegal commodities. The second possibility is that the attack was carried out by a nation-state actor in the form of a country under international embargos and/or sanctions (such as North Korea), who requires these types of LC in order to conduct large international deals.

After the breach was discovered, India's central bank - Reserve Bank of India, instructed banks in India to examine all trade documents issued over the past one year, and cross-check them between their core systems and the SWIFT system. It should be noted that concurrently to these reports, it was revealed that in June 2016, SWIFT systems of four Indian banks have been attacked. In one of attacks the attacker attempted to transfer \$150 million to a bank in the US, however this wire transfer was denied after the US bank suspected that something was amiss.

The North Korean activity against the Global financial sector

In early April 2017, Kaspersky Lab and BEA Systems co-published an extensive report regarding the North Korean nation-state group Bluenoroff, which targets global financial organizations for the purpose of financial gain. This is a subgroup of the Lazarus group. Most of Bluenoroff's activity has occurred over the last year.

Kaspersky are attributing the group with numerous attacks on the financial sector, including the attacks on Bangladesh Swift system, the attack on Polish banks, etc. The report proved for the first time a direct link between the attack infrastructure and North Korea.

The group's main penetration vector (other than searching the organization for vulnerable servers), is via waterhole attacks (aka "drive by attacks"). i.e. compromising legitimate sites, often visited by the target, and injecting them with malware. This was done for example in the attack against the Polish banks in which their systems were infected with a malware after their staff visited the site of the Polish Financial Supervision.

It appears that the watering hole campaign began in late 2016, after another of their operations in South East Asia was interrupted. Lazarus/Bluenoroff responded by regrouping and primarily targeting smaller banks, in mostly poor and less developed countries, as they are seen as "easy prey".

Waterhole sites were found in the following countries: the Russian Federation, Australia, Uruguay, Mexico, India, Nigeria and Peru. A connecting thread between the compromised websites was that they all used the JBoss application server platform. This suggests that attackers may have had o-day exploits for this platform. As of now the group attacked four types of financial organizations:

- **Traditional financial institutions such as banks;**
- **Casinos;**
- **Financial trade software developers; and**
- **Crypto-currency businesses**

The report extensively reviews several attacks against financial institutions, including an incident in a South East Asian country in August 2016, and against a European financial institution in January 2017 (by identifying one of the relevant samples on VirusTotal, it is likely that the latter event took place in Poland).

Analysis of these events, indicates that the attacker meticulously studied the upgrades and changes done to SWIFT's security systems following the attack on Bangladesh central bank, and adapted his tools and methods to overcome them. It appears that at least in some of the cases, the attacker was able to infect both the banks' IT systems and their SWIFT servers.

Main findings from the investigation

The penetration vector, at least in one of the incidents, was by compromising and weaponizing the Polish Financial Supervision Authority website via Adobe Flash Player and Microsoft Silverlight exploits. In this incident the infection was possible due communication problems between the financial organization's end-stations and Adobe's servers, which resulted in the security patches failing to update.

One of the group's long-term strategies seems to be constantly and frequently modifying their code, even without introducing new functionalities. This is done to break Yara recognition and other signature-based detections. The malwares are compiled days or even hours prior to the attacks. This indicates a highly speared method of operation. In most incidents, the malwares did not communicate directly with the C2 servers, but rather connecting to another internal host, which relayed TCP connection to the C2 via a tool dubbed "TCP Tunnel Tool".

It seems that the attackers operate with high operational alertness. This is seen for example by a systematic destruction of all evidence of their activity as soon as they identify any sign of an investigation.

\$60 Million stolen from Far Eastern Taiwanese bank via SWIFT

Following a relatively long hiatus, in early October \$60 million were stolen via a SWIFT transaction from the Taiwanese bank *Far Eastern*. According to reports⁸¹, the attackers transferred the funds to banks in Sri Lanka, Cambodia and the U.S. The attacker exploited the SWIFT system via a custom malware.

Far Eastern bank successfully recovered most of the funds after it promptly contacted the banks involved. Further, SWIFT issued an alert containing initial technical indicators.

Authorities have arrested two individuals in Sri Lanka related to the attack when one of them attempted to withdraw funds. As of now, according to reports another suspect remains at large.

The attacked bank - A medium size Taiwanese bank (2,300 employees) Far Eastern International⁸². The bank has extensive operation with China.

Date of compromise - The initial time of compromise is unclear, however as a custom malware was used in this case, the time of penetration is likely longer than several days. Regardless, on 03.10 Far Eastern employees experienced a slow-down in the bank's systems, which may be related.

Identity of the attackers - Unknown, possibly North Korea.

In Sri Lanka, two money mules were arrested, yet it is unclear if they had a larger involvement in the attack. One possibility is that they were simply commissioned to launder the money, but it is also possible that they are a part of the team behind the attack.

Penetration vector - Currently the penetration vector is unknown and is still being investigated. The possible scenarios are as follows:

- A malicious phishing email containing a malware.
- A USB Flash-drive ("disc on key") containing a malware was used with the bank's internal systems.
- A vulnerability within the bank's systems was exploited.
- An inside job – a blackmailed/disgruntled employee, etc.

Outcome of the compromise - The bank's workstations as well as SWIFT servers and systems were compromised, enabling the attacker to execute transactions.

Date of execution of the transactions - Like the Bangladesh central bank hack, the attackers chose to execute the attack during a Taiwanese holiday and vacation (Mid-Autumn Holiday), hoping that this will help the transaction go unnoticed long enough for the them to launder the money, approximate date of the transactions 05.10.17.

What are the compromised accounts, and where was the money transfer to? - All the transactions were done from the Bank's foreign currency accounts. There were no transactions from clients' accounts. The funds were transferred to banks in Sri Lanka, Cambodia and the U.S.

⁸¹ <http://focustaiwan.tw/news/asoc/201710070007.aspx>

<https://www.tripwire.com/state-of-security/security-data-protection/hackers-steal-60-million-from-taiwanese-bank-using-bespoke-malware/>

<http://focustaiwan.tw/news/asoc/201710090004.aspx>

⁸² <https://www.feib.com.tw>

The bank's control mechanisms and security systems - capability to retrieve the funds - It appears that the bank's control mechanisms systems operated well, recovering most of the funds, with the exception of \$500,000. In our assessment, as the transactions were from the bank's own account, it was easier for the bank to retrieve the money. However, unlike the Control mechanisms systems, it seems that the security systems failed as they did not detect the breach.

Malware Indicators - On December 12th SWIFT has issued an alert containing technical indicators. It was classified as TLP Amber, and was sent to banks in Israel. Client who are interested in receiving the alert are welcome to contact us on the matter.

Hackers stole 4.5 million dollars from a bank in Nepal by hacking its SWIFT server

In early November, it was reported that the largest commercial bank in Nepal - NIC Asia Bank, fell victim to attack, in which their SWIFT server was hacked and \$4.4 million were transferred, Similarly to the other attacks in which the attacker executed the attack just before the weekend or during a national holiday, the SWIFT server of NIC Asia Bank was hacked during the national holiday "Tihar". After the server was breached, the attackers placed wire transfers to various parties in six countries, including Japan, UK, the US and Singapore.

However, the employees quickly identified the suspicious transactions, and promptly alerted the Central Bank of Nepal, which was able to retrieve 3.9 million USD. Currently the forensic investigation is still being conducted. other than that the SWIFT server was hacked, no additional information was released.

Hackers attempted to steal a million dollars from a Russian state bank

In late December, it was reported⁸³ that the Russian state bank Globex fell victim to an attack that targeted its SWIFT system. The attackers attempted to steal 55 million rubles (about 940,000 USD), however only achieved to get about 10% of that (about 95,000 USD).

BEC attacks

Over the last year, BEC scams (aka chairman frauds, aka EAC scams) have grown more prevalent and sophisticated. In these scams, the attacker impersonates an executive at the company and requests an employee via email to do a wire transfer. Often this is done under the pretense of a highly important business deal or payment to a supplier, that needs to be done for some reason in a secrecy and urgent manner. The wired funds are sent the attackers' bank accounts, and then immediately transferred to different bank accounts around the world.

According to the FBI report⁸⁴ published in May, based on financial data and victim complaints filed with the IC3 (Internet Crime Center), fraudulent transfers have been sent to 103 countries, with the most common destinations being **Asian banks located in China and Hong Kong**. However, also banks in the UK also remain prominent destinations. **In 2017 there were several BEC attacks against various companies and Financial institutions in Israel.**

⁸³ <https://www.infosecurity-magazine.com/news/swift-hackers-hit-russian-state/>

⁸⁴ <https://www.ic3.gov/media/2017/170504.aspx>

Common BEC scenarios

Below is IC3's description of the five main BEC scenarios:

Scenario 1: Business Working with a Foreign Supplier

A business that typically has a longstanding relationship with a supplier is requested to wire funds for an invoice payment to an alternate, fraudulent account. The request may be made via telephone, fax, or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears similar to a legitimate request. Likewise, requests made via fax or phone call will closely mimic a legitimate request. This particular scenario has also been referred to as the "Bogus Invoice Scheme," "Supplier Swindle," and "Invoice Modification Scheme".

Scenario 2: Business Executive Receiving or Initiating a Request for a Wire Transfer

The e-mail accounts of high-level business executives (Chief Financial Officer, Chief Technology Officer, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is typically responsible for processing these requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y." This particular scenario has been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," and "Financial Industry Wire Frauds".

Scenario 3: Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail

An employee of a business has his or her personal e-mail hacked. This personal e-mail may be used for both personal and business communications. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal e-mail to multiple vendors identified from this employee's contact list. The business may not become aware of the fraudulent requests until that business is contacted by a vendor to follow up on the status of an invoice payment.

Scenario 4: Business Executive and Attorney Impersonation

Victims report being contacted by fraudsters who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week and be timed to coincide with the close of business of international financial institutions.

Scenario 5: Data Theft

Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entities in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipients of the fraudulent request for W-2 and/or PII. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new BEC scenario even if they were able to successfully identify and avoid the traditional BEC scam. This data theft scenario of the BEC scam first appeared just prior to the 2016 tax season.

Russian intervention with U.S. politics and Presidential Election



In the recent U.S. Presidential Election there were many claims and indications regarding Russian intervention to affect the election's outcome. On June 5th, The Intercept reported⁸⁵ on a highly classified NSA intelligence document⁸⁶, obtained by the website, which sheds light on Russia's involvement in the 2016 USA election. According to the document, the GRU (Russia's Main Intelligence Agency) executed cyber-attacks against at least one e-voting vendor, and sent spear phishing emails to over 100 individuals "involved in the management of voter registration systems", just days prior to the election. It should be noted the document's assessments are inconclusive, and its sources are not specified.

The document, dated May 5th 2017, examines the GRU's efforts against various actors involved in the US elections and its infrastructure. To date, this is the most in depth official US governmental report regarding the Russian intervention in the elections that came to light. Nevertheless, the document focus on the cyber activity, and does not draw conclusions in regards the ramifications of the Russian intervention on the election's outcome.

According to the NSA analysis, the hackers behind the attack were part of a team within the GRU, which had a "cyber espionage mandate specifically directed at U.S. and foreign elections". This team primarily targeted actors directly connected in the voter registration process, such as a private sector manufacturer of devices that maintain and verify electoral registrars.



Attack vector

According to the NSA document, the Russian attackers planned on impersonating an unnamed e-voting vendor to trick local government employees into opening malicious Microsoft Word documents, which contained a malware that could give hackers full control over the infected computers. In order to do so the attackers had to create a convincing fraud, and thus needed access to the vendor's internal systems.

In the first phase of their operation during August 2016, the hackers sent fraudulent emails, supposedly from Google to employees of an unnamed US election software company (likely VR Systems; a US vendor of electronic voting services and equipment. Its products are used in eight states). These spear phishing emails contained a link to a malicious site impersonating Google, which requested the targets' login credentials. The NSA identified seven VR Systems employees who potentially received this phishing email. Three of these emails were confirmed to have been blocked by their email server, however the NSA concluded that at least one of the employee accounts was likely compromised. Once the attackers gained access to the accounts, they exfiltrated documents and data deemed valuable for the next stage of the operation.

The second phase was initiated two months later in late October/early November. The attackers created a new Gmail account that impersonated that of a VR Systems employee, and was used to send spear-phishing emails to

⁸⁵ <https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/>

⁸⁶ <https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1>

local US government organizations. These emails used the stolen VR Systems documents in order to appear more legitimate.

The NSA assessed that these spear phishing emails were sent to 122 individuals associated with local government organizations; likely officials “involved in the management of voter registration systems”. The emails contained a malicious Word file impersonating a VR Systems’ document relating to its EViD voter database product line. The file was embedded with Visual Basic Script that triggered a PowerShell, which if opened, would “very likely” covertly download a second package of malware that could enable the attackers with persistent access to the infected computer.

The NSA, however, is uncertain regarding the outcome of the attack. As noted in the report, it is unknown whether the attack was successful in compromising its targets, and what potential data could have been accessed by the attackers.

Furthermore, the leaked document also provides brief description of two other Russian hacking operations related to the US elections. In the first operation, Russian military hackers sent fake test emails offering “election-related products and services” via a fraudulent email account they created, which impersonated another U.S. election company. The agency was unable to determine whether these emails were spear targeted or not.

In a second Russian operation, the same group of hackers sent test emails to the American Samoa Election Office, presumably for the purpose of determining whether those accounts actually existed prior to launching another phishing attack. The purpose of these operations is unclear, however the NSA’s assessed that the Russians intended impersonating a “legitimate absentee ballot-related service provider”.

Destructive malware attacks against Saudi Arabia



The Shamoon 2 campaign was comprised of three destructive waves of attacks, between late 2016 and early 2017, against multiple organizations in Saudi Arabia, via the wiper malware Shamoon 2 (aka Disttrack). In January PaloAlto exposed new information regarding a wave of Shamoon attacks, planned for late November 2016 against targets in Saudi Arabia.

The malware’s method of operation in this wave is very similar to the one that was used during the wave that was exposed a month prior; however, a key difference is that in this wave malware had the capabilities of nullifying one of the primary countermeasure tools used against wiper malware attacks - “Virtual Desktop Interface snapshots”.

This is done by accessing the VDI’s environment using hardcoded VDI usernames and passwords, and manually carrying out destructive activities against it. The account credentials on the malware were taken from an official Huawei documentation related to their virtual desktop infrastructure (VDI) solutions, such as FusionCloud.

This wave of attacks used a 64-bit variant of the malware, which was configured to begin its destructive activities on November 29, 2016. It should be noted that the malware also had 16 account credentials, presumably to be used in order to further spread in the attacked organization’s network. The existence of these credentials indicates that it is likely that the attacker executed a previous attack in order to obtain these account credentials.

In March Kaspersky lab revealed⁸⁷ that in the attacks two different destructive malware were used:

Name of malware	Details
Shamoon 2.0	Highly similar to Shamoon 1.0 that was used against Saudi Arabia back in 2012 and affected 30,000 computers of the Saudi oil company Aramco.
StoneDrill	This wiper malware is more sophisticated from both Shamoon 2.0 and 1.0.

According to Kaspersky, an initial analysis revealed a strong connection between StoneDrill and the Iranian APT Charming Kitten (aka Newscaster / NewsBeef / Ajax Team). As of now it is unclear whether or not the same actor is behind both Shamoon 2.0 and StoneDrill; however, according to Kaspersky it is most likely that they are used by different groups (possibly Iranian) who are aligned in their interests

According to the findings, it appears that StoneDrill is notably more sophisticated than Shamoon 2.0. Unlike Shamoon, StoneDrill has advanced sandbox evasion capabilities, is capable of using external scripts, can inject itself into the default browser's memory, and can also run with limited user privileges. Moreover, analysis of Shamoon 2.0 revealed that additionally to its wiper functions, it is also capable of encrypting data. Accordingly it could potentially be used as a ransomware tool in future waves.

Kaspersky's report also stated that for the first time there are significant indications that these destructive malwares (specifically StoneDrill) are being used against targets outside Saudi Arabia; and in the specific incident exposed by Kaspersky, against a large European petro-chemical corporation.

Prior to this discovery, on October 2016, Germany's security agency BfV published a report⁸⁸ regarding the Iranian attack group Charming Kitten, and evaluated the risk that the group poses to the European energy sector. Despite the public exposure, the report was mostly overlooked by the general media and security companies (us included).

When we reviewed the report, we identified an overlap between the indicators in the report and those from the destructive attacks against Saudi Arabia (that took place in the following months after the report was published).

We see this information as highly significant, as it appears to be the first indication of an execution of Iranian destructive malware attack against targets outside of Saudi Arabia.

Several weeks after Kaspersky's report, new findings were revealed about the method used by the attackers to distribute the malware. PaloAlto⁸⁹ discovered that the attackers exploited a compromised RDP system (Remote Desktop Protocol) to distribute the Disttrack across the network. Further, the attackers used a combination of legitimate tools and batch scripts to deploy the malware's payload to internal hosts (which the attackers gained knowledge of prior to the attack) from infected machine they gained access to.

It is presumed that the attackers gathered the list of hostnames, either directly from Active Directory, or during their reconnaissance activities conducted from a compromised host. This, in addition to the credential theft indicates that it is highly likely the attackers had obtained access to the targeted networks prior to Shamoon 2 attacks.

⁸⁷ <https://securelist.com/blog/research/77725/from-shamoon-to-stonedrill/>
https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf

⁸⁸ <https://www.verfassungsschutz.de/download/broschuere-2016-10-bfv-cyber-brief-2016-04.pdf>

⁸⁹ <http://researchcenter.paloaltonetworks.com/2017/03/unit42-shamoon-2-delivering-disttrack/>

Moreover, when gathering files attributed to the third wave of Shamoon 2 attacks, PaloAlto identified a Zip archive that contained files used to infect other systems by leveraging the initial compromised system. The attacker deployed the Zip archive to this distribution server by logging in to the compromised RDP using the stolen credentials and downloading the Zip from a remote server.

Once a system is compromised, the Disttrack malware attempted to spread to 256 additional IP addresses on the local network. This effectively enables the attacker to semi-automate infection to additional systems from a single compromised system.

The report also states that there is a possible link between Shamoon 2 attack campaign and reconnaissance operation Magic Hound. This association is based on the following three factors:

1. **Infrastructure** - the IP that was used to deliver Shamoon 2 and the IP used by Magic Hound use the same cloud computing service in the same Class C IP range.
2. **Tools** - Both campaigns used PowerShell and Meterpreter.
3. **Targets** - Both campaigns targeted entities in Saudi Arabia.

Darknet market activity during 2017

Leading darknet markets taken-down by Law Enforcement



In early July, Alphabay, the largest Darknet market was unexpectedly shutdown with no explanation. Initially it was suspected that the reason for the shutdown was that the individuals behind the market stole money from vendors and buyers.

However, later it was revealed that the site's administrator, a 25-year-old Canadian citizen named Alexandre Cazes, was arrested in Thailand and was indicted with trafficking drugs, guns, counterfeit goods and hacking tools, amongst other items⁹⁰. According to the Europol, it is estimated that Alphabay generated over a billion dollars in its three years of operation⁹¹.



Cazes was arrested after the FBI discovered that he listed his personal email "Pimp_alex_91@hotmail[.]com" as the site's administrator contact email. This address was available to any registered user. Moreover, in the investigation it was revealed that Cazes listed this email and used the same handle in various forums, and even his private blog where he stated his full name.

The authorities confiscated over 8 million dollars in various crypto-coins, and numerous other assets such as houses and his luxury cars that were listed under his and his wife's name. A week after his arrest, Cazes took his life by hanging in a Thai prison⁹².

⁹⁰ https://www.theregister.co.uk/2017/07/20/alphabay_hotmail_fbi/

⁹¹ <https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/>

⁹² <https://www.washingtonpost.com/news/morning-mix/wp/2017/07/18/suspected-alphabay-founder-dies-in-bangkok-jail-while-online-black-market-remains-closed/>

Following Alphabay's shutdown, which **at its peak was ten times larger than the now defunct Silk Road Market**⁹³, over 200 thousand users and 40 thousand vendors began searching for a new and robust market. Many chose Hansa Market, which at a certain point had to close registration due to the overwhelming demand. However, a couple of weeks prior, **Dutch authorities seized control of the market and continued operating it while monitoring and documenting its users**, including the new wave of users that followed Alphabay's shutdown.

On July 20th, Dutch police announced that it is shutting down Hansa after it documented and gathered data on tens of thousands of users. Additionally, it stated that the data is transferred to Europol for further investigation jointly with the FBI and DEA (U.S. Drug Enforcement Administration agency). Concurrently, authorities seized the site's servers in Lithuania, the Netherlands and Germany⁹⁴.

Currently law agencies began using login records collected in the investigation to obtain control of additional vendors' Darknet markets accounts, notably Dream Market. This is possible in cases when vendors reused their passwords across several markets and did not activate the 2FA (Two Factor Authentication) function. Moreover, it is reported that during the time Dutch authorities run Hansa, they infected users with a spy malware that logged their IP address unless they used a VPN, proxy, or funneled all OS-level traffic through Tor⁹⁵.

Suspicious activity regarding a large Darknet market, and the shut-down of another major market by Russian authorities



On September 13th one of the largest markets on the Darknet - "Dream Market" - went offline for several hours with no prior notice by its administrators. Users initially suspected of an Exit Scam, a common type of fraud where dark web operators shut down the site and disappear with all the users' cryptocurrency deposited for Escrow

transactions⁹⁶.

Others suspected that the site was taken down by law enforcement agencies, in a similar fashion to how AlphaBay and Hansa market had been taken down two months before, following a large-scale international operation⁹⁷. However, as the site came back several hours later, and remain operational, this does not seem likely.

After the site came back, however, some users discovered that their bitcoins wallets were empty. The site's operators have acknowledged the incident stating they are working to recover the corrupted data, however they did not say if and how affected users will be compensated⁹⁸.

Additionally, earlier that day, presumably during maintenance work, the site's real IP address was exposed. This error could result in a law enforcement raid on the data center where the market is hosted, and legal activity against the owners of the site. Below is their response to the incident

⁹³Silk Road was closed in 2013 after an FBI operation.

⁹⁴ <https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down>

⁹⁵ <https://www.bleepingcomputer.com/news/security/crooks-reused-passwords-on-the-dark-web-so-dutch-police-hijacked-their-accounts/>

⁹⁶ https://motherboard.vice.com/en_us/article/gy5pm7/users-freak-out-after-dark-web-market-goes-down-and-funds-go

⁹⁷ For more information see item "300717 – 5. Two of the largest Darknet markets recently shut down following a joint Europol and FBI international operation".

⁹⁸ <https://www.cryptocoinsnews.com/dark-web-dream-market-users-claim-some-funds-are-missing-after-temporary-downtime/>

“Additionally, earlier that day, presumably during maintenance work, the site's real IP address was exposed. This error could result in a law enforcement raid on the data center where the market is hosted, and legal activity against the owners of the site.”



Several days later on September 19th, Russian authorities have announced⁹⁹ that they have shut-down the popular Darknet market RAMP (Russian Anonymous MarketPlace).

The market, which primarily sold drugs is one of the largest on the darknet and the most popular in Russia, was taken down back in July however Russian authorities only now made their action public. Initially many users believed the website was having hosting issues, or perhaps was under a DDoS attack¹⁰⁰.

About a week later, a new website named RAMP 2.0 appeared, claiming to be a new version of the older portal. The site, which featured an almost identical interface, operated for several weeks until the final takedown and authorities' announcement. As of writing this report it is unclear whether RAMP 2.0 was fake, or was operated by Russian authorities as part of their investigation in an attempt to gather further evidence against users.

Top Darknet markets shut-down, possibly due to another law enforcement agency operation

Throughout October multiple major Darknet markets began shutting-down without any explanation. Early on, some Reddit users¹⁰¹ claimed to have intermitted access to a number of the markets, however shortly thereafter it became apparent that all four of the largest markets - Dream Market, Trade route, Tochka and Wall street, were completely unavailable.

As of writing this report, it is unclear whether this occurred due to DDoS attacks, or law enforcement agencies operation similarly to the Alphabay and Hansa takedown three months ago. Law enforcement agencies in the US, UK and EU told Sky News that they had no statement to make regarding the matter¹⁰². At the time, there were numerous reports of mirror sites for some of the markets¹⁰³, however many were fraudulent¹⁰⁴. These sites are almost identical to the genuine markets, yet are malicious and could steal users' credentials and financial information, and possibly even infect them with malware.

Around mid-November, the markets began returning to normal operation with no official explanation or acknowledgment of what happened. As stated, initially many believed that the markets were shut down by authorities, however now this seems less likely. Nevertheless, this cannot be completely ruled out, as it is possible that some of the markets are controlled by law enforcement, as happened with Hansa market. Another assumption is that the individuals behind the markets coordinated this action in light of the increasing pressure from authorities; however as of writing this report these assumptions have not been officially corroborated.

⁹⁹ <http://tass.ru/proisshestiya/4572560>

¹⁰⁰ <https://www.bleepingcomputer.com/news/security/russian-authorities-announce-takedown-of-ramp-dark-web-marketplace/>

¹⁰¹ <https://www.reddit.com/r/DarkNetMarkets/>

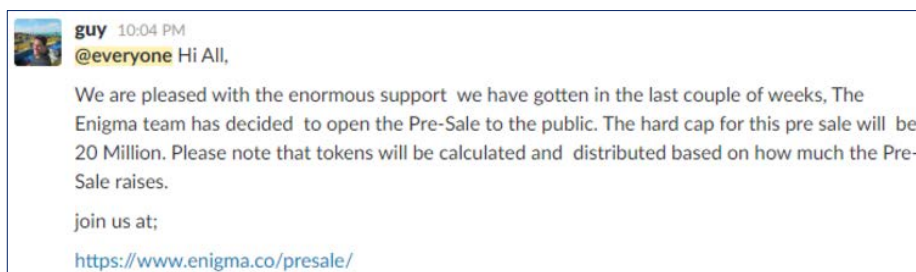
¹⁰² <http://news.sky.com/story/criminals-worry-as-dark-net-markets-disappear-11078811>

¹⁰³ https://www.reddit.com/r/DarkNetMarkets/comments/777xqb/no_aero_market_is_not_dead_mirror_links_are_live/

¹⁰⁴ <https://darkwebnews.com/news/top-darknet-markets-offline/>

Cryptocurrency platform Enigma compromised; over half a million dollars in Ethereum stolen from users

On August 20th, a hacker gained control of the popular cryptocurrency platform Enigma, and conned users from over \$500,000 in Ethereum currency. The attacker executed the scam by compromising Enigma's systems and sent its users "official" messages claiming that they began a pre-sale of an ICO (Initial Coin Offerings).



As of yet, there is no official confirmation regarding how the attacker gained access to the site's systems. However, according to various reports on social media, the attacker obtained Enigma's CEO Guy Zyskind's email login info from the dating site Ashley Madison which took place on July 2015. It appears that the attacker identified that Zyskind reused his Ashley Madison username and password with his email, and has not changed them since the leak¹⁰⁵.

Once the attacker had access to Zyskind's email he got Admin credentials to Enigma, which he used to send the users the messages and blocked the other admins from the site. Moreover, apparently Zyskind did not enable Two Factor Authentication, which might have prevented Enigma being breached. This attack is the latest in a series of attacks against cryptocurrency platforms¹⁰⁶. In just the last couple of months over \$48 million in Ethereum currency were stolen in four different incidents¹⁰⁷.

Russian APT Dragonfly attacks targeting critical infrastructure sectors

On October 20th, the US-CERT issued a public alert¹⁰⁸ regarding a wave of attacks, starting since at least May 20th. 2017, by the Russian APT Dragonfly (aka Energetic Bear), that targets government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors. The alert is based on various sources, notably Symantec report¹⁰⁹.

Exploitation of the supply chain – in their initial attacks the attackers targeted peripheral organizations such as trusted third-party suppliers with less secure networks, and gathers intelligence via open-source reconnaissance.

¹⁰⁵ <https://www.cryptocoinsnews.com/hacker-nets-over-500000-after-hacking-enigma-before-its-ico-date/>

¹⁰⁶ <http://securityaffairs.co/wordpress/62219/hacking/enigma-platform-hacked.html>

¹⁰⁷ <http://thehackernews.com/2017/07/ethereum-hack.html>

<http://thehackernews.com/2017/07/ethereum-cryptocurrency-hacking.html>

<http://thehackernews.com/2017/07/ethereum-cryptocurrency-heist.html>

<https://thehackernews.com/2017/07/bitcoin-ethereum-cryptocurrency-exchange.html#>

¹⁰⁸ <https://www.us-cert.gov/ncas/alerts/TA17-293A>

¹⁰⁹ <https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group>

Spear-phishing emails and malicious documents – the threat actor sends malicious document via targeted phishing emails, however note that these documents do not exploit a vulnerability and do not contain a malicious Macro, but rather leverage legitimate Office features in order to retrieve the content from a remote server.

The malicious documents contain links that automatically loads when the document is opened. Once opened, the documents attempt to retrieve the malicious payload through a “file:\\” connection over SMB using Transmission Control Protocol (TCP) ports 445 or 139.

For example: file[://<remote IP address>/Normal.dotm

When establishing the SMB communication, the computer sends the login password hash to the malicious server. The threat actor then uses password-cracking techniques to obtain the plaintext password. Once valid credentials are obtained, they are used to impersonate authorized users.

Waterhole attack – the attackers compromised the infrastructure of trusted organizations to reach intended targets. They notably targeted websites related to process control, ICS, or critical infrastructure, and injected to them a malicious code that gathers victims' credentials.

Penetration and installation – the attackers used the stolen credentials in order to access organizational networks which did not employ multi-factor authentication. After gaining access, the threat actors downloaded tools from a remote server, that were automatically installed via the use of scripts. Furthermore, the scripts created user accounts, and attempted to add them to administrators group for elevated privileges.

ShadowPad – Chinese attacks on banks and critical infrastructures via malicious software updates

In August Kaspersky lab published a report¹¹⁰ exposing a presumably Chinese APT (identified in July), that targets various organizations via their supply chain. The attacks were executed by compromising a software package produced by NetSarang, and exploiting their software update system to propagate a backdoor.

According to Kaspersky's analysis, recent versions of the software were stealthily modified to include an encrypted payload that could be remotely activated by the attacker. The backdoor was embedded into one of the code libraries used by the software.

The malicious payload was obfuscated by several layers of encrypted code, and thus could only be triggered via a specially crafted DNS TXT record sent from the attackers' C2 server. Prior to its activation, the module exfiltrates only basic target information such as domain and user name, system date and network configuration; this data is presumably used to determine whether the target is of value or not. If deemed valuable, the C2 server sends a decryption key for the next stage of the code, effectively activating the backdoor.

NetSarang products are used by hundreds of companies around the world, including in Israel. Further, it is used by many critical infrastructure companies. NetSarang has issued an official statement¹¹¹ on the matter, in which it confirmed Kaspersky's findings.

¹¹⁰ <https://securelist.com/shadowpad-in-corporate-networks/81432/>

¹¹¹ https://www.netsarang.com/news/security_exploit_in_july_18_2017_build.html

Note that a "clean" software update that supposedly removes the malicious update does not guarantee that an attack is neutralized. If the attackers have executed the attack, it is possible that they have already pivoted to another software/firmware component within the compromised system.

Sweden's Transport Agency exposed sensitive data of nearly all its citizens back in 2015



In late July, it was reported¹¹² that in 2015 the Swedish Transport Agency¹¹³ (STA) out-sourced IBM to maintain and operate its databases and networks, as part of their efforts to migrate their databases to cloud storage. IBM in turn used subcontractors from the Czech Republic and Romania, that were given access to the full dataset from the Transport Authority.

This dataset however included information such photographs and home addresses of Swedish Air Force and special forces personnel, as well as records of people in witness protection programs. Moreover, the sub-contractors did not receive security clearance to handle such sensitive information.

When this issue came to light, instead of creating a redacted version of the database, the STA sent the sub-contractors emails requesting to manually delete the sensitive information they held. Further, the emails contained the full details of the individuals that STA wanted removed. Although that the data leak took place in 2015, the Swedish Secret Service only discovered it and began investigation in 2016. The investigation resulted in firing of STA's director-general Maria Ågren in January 2017¹¹⁴.

Outlook Web Access based attacks, mainly in Office 365 environment



In recent months numerous waves of attacks against various organizations were identified, including targeted extortions that originated from a certain compromised OWA account. This was often achieved by obtaining OWA users' log-in credentials, accessing their account and monitoring their emails and appointment. When the user is away (e.g. a meeting or vacation), the attacker logs in, sends malicious emails (often BEC messages) and then deletes them from OWA¹¹⁵. The best method to mitigate these types of attacks is by enabling Multifactor Authentication and requiring users to use strong passwords.

¹¹² <https://www.itnews.com.au/news/sweden-exposed-sensitive-data-on-citizens-military-personnel-469046>

¹¹³ A Swedish government agency under the Ministry of Enterprise, Energy and Communications agency regulates and inspects transportation systems in Sweden.

¹¹⁴ <http://thehackernews.com/2017/07/sweden-data-breach.html>

¹¹⁵ <https://isc.sans.edu/forums/diary/Outlook+Web+Access+based+attacks/22710/>

An overview of the Deloitte hack

Deloitte.

On September 25th, it was reported that the global email server of Deloitte, one of four largest accounting firms in the world, was recently breached¹¹⁶. According to reports, Deloitte discovered the hack in March 2017, yet the attack took place in October-November 2016. Currently it is believed that the attackers compromised the firm's email server via an "administrator's account" that granted them unrestricted access to all of the firm's emails. Further, it appears that this account did not have a Two-step verification feature, and required only a single password.

According to an analysis of the breach, the hackers had access to the company's emails, usernames, passwords, IP addresses and architectural diagrams for Deloitte's businesses and clients. It should be noted that Deloitte uses Microsoft cloud services "Azure".

According to Deloitte, the breach affected only its US clients; as of now six clients received messages informing them that their info was compromised. An inside source claimed that the forensic investigation revealed that several Gigs of data were transferred to an external server.

The company chose not to inform its clients about the breach, despite being aware of it for a long time. In our assessment, it is doing everything in its capacity to downplay the event while withholding information.

¹¹⁶ <https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails>

Significant Attacks Against Israel in 2017

Persistent Iranian attacks against Israeli targets

January 01.17

Iranian Attack Group OilRig Attacks against Israeli and Global Targets

In early January, Iranian threat agents registered four domains with URLs similar to Oxford University's websites. These domains contained malicious content designed to infect users. At least one of the malicious files on these domains was uploaded for examination to Virus Total by an actor from Israel. Accordingly, it seems that there were impersonation and infection attempts against several organization in Israel (however, it is possible that organization outside of Israel were also targeted).

One of the fraudulent domains had a fake registration form to a conference the required the victim to download and install a "registration" software. Once the malware is executed, concurrently to the infection the victim is presented with a custom registration form created by the attackers, with info about the conference. The victim is instructed to provide various details, save the form and then send it to an email address controlled by the attackers.

Impersonating windows CHM help files in order to execute malware

Other than the abovementioned attacks, we also exposed additional incidents in which the attackers used files with CHM extension that contain JavaScript code. These files are equivalent to executable files. I.e. once they are opened a code is executed on the computer, without any additional action by the attacker.

Throughout January we identified an escalation of Iranian attack group's operations against Israel. Although their technological level is still relatively basic, the Iranians have executed several operations which we see as an advancement of capabilities:

- Rapidity taking control and infecting Israeli websites for the purpose of "waterhole attacks". They after buying the access to these sites and organizational network over the Darknet.
- Signing the malware via a legitimate code signing certificate, which was presumably stolen.
- Impersonating and infecting large IT providers, and using social networks to infect the targeted organizations.
- Sending an unusual amount of spearphishing emails, about 10, to a single individual over the course of two days.
- Retaining operational persistency, and continuing attacks even after their infrastructure and waterhole sites have been exposed. Quickly registering and creating alternative waterhole sites in a matter of several hours (instead of laying low after being publicly exposed as they did this far).

It should be noted that these attacks are executed by three different Iranian attack groups, each with different attack vectors:

1. RocketKitten

- New method of operation – using email tracking services.
- Fraudulent websites impersonating *United Technologies Co.*

- Using sami.exe / DownPaper malware.
- Creating fraudulent sites that contain malicious Javascripts.

2. OilRig

The infection vector is via fake yet credible looking LinkedIn accounts (this is in comparison to fraudulent Facebook entities used by the Hamas, which can easily be identified as fake). These entities contact their targets via LinkedIn, and send them private messages with links to the fraudulent sites.

3. CopyKittens.

Repeatedly infecting Israeli websites via malicious JavaScript. In these attacks, three notable Israeli websites were attacked: Tel Aviv University's student portal login page, Ma'ariv news site, and the website of the Jerusalem Post newspaper.

February 02.17

Rocket Kitten targets Apple Mac computers with OSX malware

In late January/early February, the Iranian attack group Rocket Kitten, begun using MacOS malware. The infection vector is similar to previous attacks – fraudulent sites that lure users to install the malware. In our assessment, this is the first time that this group has created and implemented an attack campaign against Macs.

About a week later on February 6th, a public report¹¹⁷ was published that exposed this malware (note that the report analyzed the same sample we reviewed).

New attacks against Israel by the Iranian attack group CopyKittens and connections to OilRig

During February, we identified new samples of malwares sent to Israeli targets. In our analysis of the malwares we revealed that they were signed with the digital certificate of a company named AI Squared. As a reminder, in recent months we reported on a campaign by another Iranian attack group – OilRig, which also used a compromised digital certificate by this company. Accordingly, in our assessment, these two groups operate under the same organization, and make use of the same resources, including the stolen digital certificate.

March 03.17

Throughout the first two weeks of March we identified infrastructures and various samples, attributed to the Iranian attack group CopyKitten, which were used in recent months against Israeli organizations. It appears that the attacks were executed for the purpose of espionage on military/defense targets.

April 04.17

New CopyKittens and OilRig attacks against Israel

In April we exposed new operations and infrastructures of the Iranian threat agents CopyKittens and OilRig. Note that their attack vector was by impersonating IT firms. During 2016, three Israeli IT companies were impersonated in such attacks.

¹¹⁷ <https://iranthreats.github.io/resources/macdownloader-macos-malware>

May 05.17

Fraudulent news site created by Iranian threat agent Charming Kitten - malicious use of social media to promote attacks

In early May, Charming Kitten created a fake news agency named “The British news agency” or “Britishnews”. This fake news agency and accompanying social media accounts **are not** used to disseminate propaganda and or/fake news. It appears that their content was automatically copied from legitimate sources. Accordingly, it seems that the purpose of this news agency was to create a credible looking site, which the attackers could use to reach out to their targets and infecting them with malware while conversing with them.

More specifically, the website contains that attack kit BeEF (Browser Exploitation Framework – a penetration testing tool that focuses on web browsers), however it seems that the attack is executed only when the victim visits the site from a predetermined IP list.

Additionally, in **late April and early May** we identified that OilRig have been uploading files for examination on VirusTotal. They uploaded malicious documents, each time modifying various components on the files in order to learn why they are identified by AV engines, and how to obfuscate the files from them.

A review of TrapX report regarding the Iranian threat agent OilRig’s post infection activity

The cyber security firm TrapX published a report¹¹⁸ that reviewed a single attack against a security company (likely Israeli), and analyzes the subsequent infection process. This report provides an insight into OilRig’s post infection method of operation.

The research and following insights, notably insights based on OSINT analysis, are **in our assessment likely incorrect. Moreover, the report does not provide adequate evidence to substantiate its conclusions.** In particular, the report claims that after the attackers gained a foothold in the organization, Russian hackers joined the attack and used the Black Energy malware.

These claims are based on Akamai IPs (which receive a lot of traffic that is unrelated to the case, and may have led to the false assessment), and from the registration details of one of the domains (these domains are known to us, and there are no indications that they are linked to Russian actors). Further, despite the claim that Black Energy was used, no evidence is given to corroborate this (notably no hash is given).

Although the report provides an insight regarding the Iranian group’s modus operandi, it does not provide adequate proof of Russian involvement as was reported by the media¹¹⁹.

New Rocket Kitten attack infrastructures

In late May following the May 1st, 2017 “Breaking Alert: [Threat Level - High]: A wave of phishing attacks by the Iranian threat agent Rocket Kitten against organizations in Israel”, we identified new domains used by the Iranian threat agent.

Indicators are available on MISP event number 178.

¹¹⁸ https://deceive.trapx.com/WPAOAOilRig_210LandingPage.html

¹¹⁹ Web Defenders Detect Russian Hand in Iranians’ Hacking Attempt - <https://mobile.nytimes.com/2017/05/15/technology/web-defenders-detect-russian-hand-in-iranians-hacking-attempt.html>

June 06.17

A new wave of attacks by Iranian threat agent against journalists and academics

In early June, attackers (who we attribute to the Iranian threat agent Charming kitten/Rocket Kitten) begun executing attacks using infrastructure that we previously reported on. As of now, four Israeli Journalists are confirmed to have been attacked. Our analysis of the attack infrastructure retrieved over 150 additional targets.

New CopyKittens attacks against an unknown entity in Israel

In our ongoing investigation of attack infrastructures on VirusTotal, we identified two document samples that were uploaded in May from Israel (this indicates that the targets are likely Israeli). According to our initial assessment, these attacks are attributed to the Iranian threat agent CopyKittens¹²⁰.

New Iranian Charming Kitten attack infrastructure used against Israeli targets

In late June, we identified additional infrastructure of the Iranian threat agent Charming Kitten (which operates within the Iranian Defense Agency). Charming Kitten targets Israel and other countries in the Middle East. In the this campaign, they primarily attacked Journalists and academic researches. The attackers compromised email accounts of individuals related to the target, and sent him fraudulent emails attached with a malware. This group has been operating for a while now, with high rate of success.

July 07.17

New Charming Kitten attack infrastructure

In early July, we identified additional infrastructures attributed to the presumably Iranian threat agent – Charming Kitten. MISP event number 187.

August 08.17

In early August, PaloAlto published an extensive report regarding a Web Shell used in attacks against organizations. Although not stated in the report, we have received a confirmation from several security researchers that the campaign is linked to the Iranian threat agent OilRig. However, note that as the Webshell is also used by other non-related actors. Accordingly, while detection of the shell should always be viewed as an indication of a malicious activity that demands an immediate response, attribution to OilRig group requires additional cross referencing.

The Webshell is named TwoFace as it is comprised by two components. The first is named TwoFace Loader, a basic and preliminary shell that extracts and installs the second component, a more advances tool named TwoFace Payload (identified by Microsoft as Seasharpee). These tools are written in #C, and run on Webservers that support ASP.NET.

The attackers also run the tool Mimikatz to steal passwords from compromised servers. After the attackers obtains the passwords (in one case, several months later), they are used in attempts to install the shell on the organization's Exchange servers. The Shell can be interacted with via a custom web interface.

The report briefly reviews another Webshell used by the group, dubbed IntrudingDivisor.

¹²⁰ <http://www.clearskysec.com/report-the-copykittens-are-targeting-israelis/>
<http://www.clearskysec.com/copykitten-jpost/>

In a separate report¹²¹ published by PaloAlto, a connection was found between OilRig and the malware IsmDoor, which was used as a data gathering tool prior to the Shamoon destructive attacks. Later we identified a malicious email sent to a non-Israeli entity. By analyzing the mail, we exposed new, previously unexposed infrastructure.

Additional Charming Kitten attacks and infrastructures

In August we identified additional attack infrastructures of the Iranian threat agent Charming Kitten. This threat agent operates against various Israeli entities. In the recent wave, university researchers and journalists were chiefly targeted.

Charming Kitten attacks and infrastructures

In August, multiple malicious emails were sent to various entities in Israel. Some of the emails did not contain any text, but only images of text linked to a phishing page. This is done presumably in order to bypass text based spam filters. Moreover, several of the emails contained shortened URLs (via the service bit.ly) that directed victims to a phishing page.

Examining the phishing page's source code revealed that the attackers uploaded a code (copied from the attached GitHub link¹²²) that enables them, via WebRTC¹²³, to identify the real IP address of targets who use proxies. Concurrently to sending the emails, the attackers also attempted to do a password reset of one of their target's Facebook account. However, this individual was alerted about this from Facebook.

This vector of sending fraudulent emails while executing additional actions that issue alert to the target may confuse even alert targets. Accordingly, in such situations, consultation with a security personal is required in order to prevent accounts being compromised.

Identification of new OilRig infrastructure

In late August identified new infrastructures of the Iranian threat agent OilRig. It should be noted that these infrastructures were exposed using an experimental investigation method. Accordingly, they may include domains that are likely malicious yet are not a part of the attack infrastructure. Nevertheless, if you identify any internal communication with these domains, we recommend investigating it in order to rule out an infection. MISP event number 220.

September 09.17

In early September, we exposed a new attacks and infrastructures attributed to the Iranian threat agent Greenbug, apparently targeted against Saudi entities. The attackers used a variant of the ISMDoor malware named ISMAgent¹²⁴, that was used as a RAT, and communicated via either DNS or HTTP requests.

Infection is executed via a Word file named *change managment.dot*¹²⁵, that exploits vulnerability CVE-2017-0199. When opening the document, a script file that impersonates an RTF file is downloaded from a website controlled by the attackers. Further, a VBS script is downloaded, which in turn executes a PowerShell command.

The script's main objective is downloading from a file sharing site a base64 coded text file impersonating a digital certificate, as seen by the header and file extension; however, when decoded, an executable file is created. After

¹²¹ <https://researchcenter.paloaltonetworks.com/2017/07/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/>

¹²² <https://github.com/diafygi/webrtc-ips/blob/master/README.md>

¹²³ <https://en.wikipedia.org/wiki/WebRTC>

¹²⁴ <https://researchcenter.paloaltonetworks.com/2017/07/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/>

¹²⁵ <https://www.virustotal.com/en/file/66358a295b8b551819e053f2ee072678605a5f2419c1c486e454ab476c40ed6a/analysis/>

the file is saved as srvRep.txt, it is decoded and then saved as an executable file. The final executable file is the ISMAgent malware¹²⁶.

Charming Kitten attacks and infrastructures

We identified this week additional infrastructures of the Iranian threat agent Charming Kitten. Indicators are available on MISP event numbers 229 and 232.

October 10.17

Exposing attack infrastructures of the Iranian threat agent Charming Kitten

Throughout September and October Charming Kitten has executed spear phishing attacks against academic researchers in Israel. To facilitate the attack the group created at least one fictitious Twitter account under the name of "Yafa Hyatt" (יפה חייט). The attackers sent their targets private messages, leading them to a phishing page impersonating Gmail in an attempt to steal their login credentials.

Below is a screen capture of the account, followed by the messages sent to the targets:



The message contained a link to a Google Sites website, which after a few seconds redirected the user to a different site that is controlled by the attackers.

Fraudulent domains registered by OilRig impersonating Israeli high-tech and security companies

On October 15th, a sample of the ISMDoor¹²⁷ malware was uploaded to VirusTotal from Iraq. As a reminder, this malware was used in the preliminary attacks against Saudi organizations prior to the wiper attacks¹²⁸.

By implementing new investigative methodologies, we identified new elements of the attack infrastructure. Currently it is unclear whether the purpose of the fraudulent domains is to attack the impersonated companies,

¹²⁶ <https://www.virustotal.com/en/file/33c187cfd9e3b68c3089c27ac64a519ccc951ccb3c74d75179c520f54f11f647/analysis/>

¹²⁷ researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan

or to use them against other companies. Nevertheless, it should be stated that as of now we do not have any indication that these companies were attacked or compromised.

As a reminder, previously this group successfully breached several Israeli IT firms and used their access and compromised data to attack the clients of the firms¹²⁹.

Following the identification of the fraudulent domains we promptly alerted the security teams of the targeted companies (with the exception of two that we unable to establish contact). As of writing this report, none have notified us regarding an attack attempt.

New Charming Kitten attack infrastructure

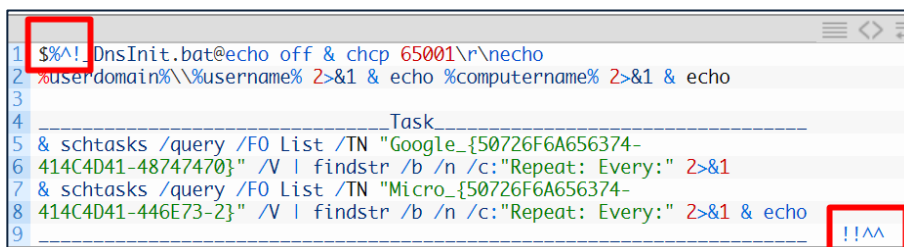
In October we exposed additional Charming Kitten domains. MISP event number 246.

November 11.17

Analysis of OilRig's malware - ALMA: Communicator

In early November, we reported on an attack against Saudi Arabia by the Iranian threat actor OilRig. Several days later PaloAlto published a report reviewing this attack. The report analyzed the malware that was used in the attacks - ALMA Communicator. Similarly to other malware used by other Iranian threat agents, ALMA also **uses DNS requests** to receive commands and exfiltrate data.

It executes DNS queries, and is responded with IP address, however note that it does not attempt to communicate with them. Instead it treats them as binary data. By using this method, each DNS quarry transmits 4 four-digit number, which are then constructed by the malware to commands that are executed on the compromised computer. For example, communication from the server will always begin with the textual command `$%^!` and will end with `!!^^`:



```

1 $%^! DnsInit.bat@echo off & chcp 65001\r\necho
2 %userdomain%\%username% 2>&1 & echo %computername% 2>&1 & echo
3
4 Task
5 & schtasks /query /FO List /TN "Google_{50726F6A656374-
6 414C4D41-48747470}" /V | findstr /b /n /c:"Repeat: Every:" 2>&1
7 & schtasks /query /FO List /TN "Micro_{50726F6A656374-
8 414C4D41-446E73-2}" /V | findstr /b /n /c:"Repeat: Every:" 2>&1 & echo
9 !!^^

```

Re-engagement of the Iranian threat agent CopyKittens' activity

On July 25th, 2017, we published in collaboration with Trend Micro an extensive report regarding the Iranian espionage threat agent CopyKittens, which infiltrated numerous organizations in Israel and additional countries around the world.

In November we identified a malicious email that was sent in late October to Qatari governmental workers. Based on the following indications, our assessment is that this activity is likely part of a reengagement of CopyKittens' activity:

- The targets of the malicious emails – Qatari governmental workers.
- Visual similarities between the C2 server (cisc0[.]net) and prior known servers used by the group.

¹²⁹ <http://www.clearskysec.com/oilrig/>

- The style in which the lure document was designed and phrased.
- The use of Meterpreter in conjunctions with Cobalt Strike
- Overlap of infrastructures identified in previous CopyKittens attacks.

Our investigation of the current attack infrastructure revealed numerous additional components, as well as documents regarding attacks against various Middle Eastern countries (however not Israel). Note that parts of this infrastructure were used in the previous attack wave, which took place prior to the publication of the report.

OilRig attack infrastructure used against Saudi Arabia

In November, we exposed a new OilRig attacks and infrastructure against Saudi Arabia, in which a document with the named - *User list must change password.xls* - was sent to an unknown entity in Saudi Arabia. The document had no content; however, it did contain a Macro.

For persistency and execution, the malicious macro creates a times task. The task runs a malicious VBS file named helminth, followed by a VBS file that in turn executes a malicious PowerShell that grants the attacker with access to the computer.

New OilRig malware

In late November, we detected new sample from the Iranian threat agent OilRig's attack campaign. The sample appear to be related to the previous attack was, as its C2 server has previously been reported. When the sample runs, the malware is extracted and executed via CMD. Further, the malware achieves persistency by installing itself in the Windows start-up folder.

The next stage is extraction and execution of the rest of the components. As is in line with OilRig's modus operandi, the malware exfiltrates data via DNS, using an open source tool¹³⁰ that downloaded to the compromised computer.

Additionally, a tool named CURL, which is used to transfer data to or from servers, is extracted. When dnclient.exe is executed, a small JavaScript creates a local file with the compromised data prior to its exfiltration via DNS quarries.

A summary table of the Iranian threat agent OilRig's attacks against Israeli IT companies

In 2017, numerous attacks by the Iranian group OilRig against Middle Eastern countries including Israel were identified and exposed. One of the group's chief method of operations is attacking their targets' "supply chain", notably IT/software vendors. This vector was also used by the group against banks in Saudi Arabia¹³¹.

The table details the Israeli companies that the group hacked, attempted to hack, or at the very least used their name in attacks against other organizations. It should be noted that it is possible that there are additional cases that are unknown to us, in which companies (possibly in other industry sectors) were attacked/hacked.

Note that the identifying details of the Israeli companies have been obfuscated. This table is a summary tool that illustrates the attack vector for the purpose of assisting companies in mitigating similar attacks.

¹³⁰ <https://github.com/iagox86/dnscat2>

¹³¹ https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html

Company	Sector	Was it breached?	Attack vector
██████	IT	Yes	Malicious emails sent from the company's hacked corporate email account. Further, the attackers registered and created a fraudulent website ██████[.]org that hosted a malware
University of Ben Gurion	Academia	Yes	Malicious and fraudulent emails were sent from hacked university employees' email accounts
██████	IT, ERP	Yes – high likelihood	The attackers used the company's code signature certificate. Accordingly, it is likely that the attackers obtained the certificate from the company's computers or compromised email account. The attackers had the certificate for over three months.
AI Squared	Software development	Yes – high likelihood	(Non-Israeli company) The attackers used the company's code signature certificate. Accordingly, it is likely that the attackers obtained the certificate from the company's computers or compromised email account. The company has publicly admitted that the certificate was stolen.
██████	IT	Yes – intermediate likelihood	It was reported that fraudulent email was sent from the company. A fraudulent domain ██████vpn[.]com was registered and created to host a malware. The domain was used to attack the targeted organizations by impersonating the company.
██████	IT	Possibly hacked. Currently we do not have internal info regarding this company.	The attackers used a document that appears to originate from the company. As of now there is no verified info regarding an infection.
██████	IT	Currently we do not have internal info regarding this company.	The attackers registered the domain ██████-vpn[.]com. There are no indications of a breach or an attack against the company.
██████	computer networking products supplier	Possibly hacked. Currently we do not have internal info regarding this company.	A malicious PowerShell by the threat agent OilRig was uploaded of examination to VirusTotal on 25.04.2017 (e664b6f69d1f90d1bc3fb8fbe123e11c). The file contained that following path, which by indicate that company's name was used in an attack: D:\Install\Malware\██████DnE1.Ps1 However, it should be noted that as of now we do not have any indication that the company was in fact attacked or breached.

Additional Israeli companies	IT	Likely to have been hacked. Currently we do not have internal info regarding this companies.	There are additional Smaller IT companies that received malicious messages. Currently we are unable to share them. It is unknown whether these companies were infected or not.
------------------------------	----	--	--

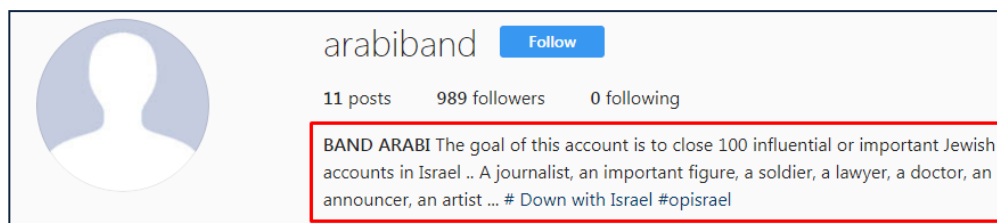
Tens of thousands of malicious emails containing Locky and Trickbot malwares sent to multiple organizations in Israel

In late August-early September, several organizations in Israel received tens of thousands of malicious emails addressed to their employees. It appears that this is a part of a generic campaign in which tens/hundreds of millions of emails are sent to organizations around the world. As of yet, it is unknown how the mailing list used in the campaign was created.

One of our assumptions is that the email addresses were gathered either by compromising the ISP's email server, or a variation of man-in-the-middle attack. Alternatively, it is possible that it was executed via a Microsoft email server 0-day vulnerability. However, it should be noted that currently there is no evidence to corroborate these assumptions.

Popular Israeli Instagram accounts compromised by an Arab hacker

An Instagram account by the handle @arabiband, has been posting screen captures of Israeli accounts allegedly hacked and shut down by him. The account has 989 followers and currently has only 11 posts. According to the account description, arabiband intends to "close 100 accounts of influential or important Jewish accounts in Israel".



Amongst the compromised accounts are the accounts of the Mayor of Jerusalem Nir Barkat, and that of the Likud (ליכוד) party, which we have verified as compromised.

Additionally, on a post from 04.11.17 an Israeli Instagram user that was attacked by arabiband, reported that her account was hacked:



Two Israeli news sites defaced by Turkish hacktivists in commemoration of the Balfour declaration's 100 year anniversary



On Thursday 31.10, two Israeli news sites were defaced for several hours, by a nationalistic Turkish group known as AkinCilar (meaning "raiders"), that appear to have connections to the Turkish government.

The group defaced the websites of "Davar Rishon" and "Times of Israel", presumably by accessing the websites' management systems.

In the past year, AkinCilar attacked media sites across multiple countries, including Belgium and Myanmar, who oppose Turkish policies.

The recent attacks against the Israeli sites were executed in commemoration of the 100-year anniversary of the Balfour declaration, and as an act of solidarity with Palestinians from Gaza. As a reminder, the group previously

attacked and defaced dozens of Israeli sites following the 2010 Gaza flotilla raid.

Concurrently, AnonGhost group, who took a notable part of the recent OpIsrael campaigns, posted threats against Israel, also claiming that they have modified their attack vector. This following the recent IDF attacks against the Hamas and Islamic Jihad organizations in Gaza. Below is their full announcement:

1. We are AnonGhost we are here to punish you israhelli because we are voice of Palestine we will not remain silent we are Fuck you hard more then previous but now we change the method of target ... Soon as possible we access to your Fucking iron dome .
2. Listen.....!
3. We are support every cyber and arms resistance against everyone how hate Palestine and Al-Qassam brigade.. Be aware Zionists p!gs and pro israhelli dogs..

Phishing emails impersonating 013 Netvision's email service E-Box

On August 22nd, several hundred Israelis received a phishing email impersonating the Israeli ISP Netvision. This is likely a part of an international generic campaign that was modified by the attacker according to the targeted countries. Below is the content of the message:

From: Netvision [mailto:postmaster@mail.protection.outlook.com]
Sent: Tuesday, August 22, 2017 2:26 PM
To: [REDACTED]@netvision.net.il
Subject: Action required: Mails on Hold

Dear [REDACTED]@netvision.net.il,

This account needs more space. You will be blocked from sending and receiving emails.

To avoid exceeding quota and continue receiving emails, please follow your email address below to maintain service.

[REDACTED]@netvision.net.il

We apologize for any inconvenience and appreciate your understanding.

Thanks,
 2017 Netvision Admin Center.

The email contains a shortened URL link¹³² that directs to a fraudulent website impersonating E-Box, 013 Netvision's email service:

A phishing attack against the Israeli Ministry of Economy

An ongoing research we are conducting revealed a phishing email that was sent to the Israeli Ministry of Economy. This appears as a fairly generic phishing email rather than a targeted attack. Our examination of the email, which was uploaded to VirusTotal, indicates that it is a part of a two-email conversation sent from and replied to the address - valeria.amaral@unicesumar.edu.br.

In the first email, the sender identifies as a " professor of pharmaceutical":

```
Valeria do Amaral
Professor de Farmacia
44 30276360| Ramal 1899
valeria.amaral@unicesumar.edu.br
<http://imagens.ead.cesumar.br/2015/ITO/Logo/unicesumar.png>

As informações contidas neste e-mail são confidenciais e dirigidas
exclusivamente aos seus destinatários. A divulgação, utilização,
reprodução ou distribuição não estão autorizadas por outras pessoas e,
na hipótese de ocorrência destes atos, as medidas legais cabíveis
poderão ser tomadas. As opiniões e declarações contidas expressam
somente a ideia dos seus remetentes.

This message has confidential information expressly addressed to its
recipients. Disclosure, use, reproduction or distribution are not
authorized by others. In case of it occurs, appropriate legal action may
be taken. The opinions and statements involved may express only the
thoughts of their senders.
```

¹³² According to the shortened URL service statistics page, the link was clicked in over 200 times

Note however that the second message is written in broken Hebrew (likely due to being translated with Google translate). In this email, the attacker identifies as the head of ICT support department and informs the target that his Webmail password has expired, followed by a link to reset it.

הסיסמה שלך פג היום. אתה מוזמן בזאת ללחוץ על Helpdesk כדי לעדכן את [publish/publish_form/199515](#)

הסיסמה שלך כדי להמשיך עם תיבת הדואר שלך ופעל לפי ההוראות.

אי עמידה בהנחיות אלה עלולה לגרום לאובדן גישה לחשבון ה- Webmail שלך. אנא השתמש בקישור לעיל כדי להשלים את טופס האימות של משתמש הדואר האלקטרוני שלך.

מנהל התמיכה.
מחלקת התמיכה של ICT
© זכויות יוצרים © Microsoft 2007

The link directs to an online form, created via the form creator site Form2pay, that contains a request to provide the user's email account credentials. This link is likely meant to lure victims in providing their credentials. The site is presumably spoofed or hacked. The email, which was relayed via a Brazilian server, was sent to the email address of the Washington office of the Israeli Ministry of Economy - usa-washington@moital.gov.il.

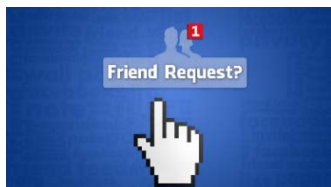
Email attacks (likely generic) against Israeli companies and individuals

As part of our new monitoring system, in the table below is a list of malicious emails sent throughout recent weeks to companies and individuals in Israel. Our initial assessment is that these are generic attacks (i.e. the attacks do not specifically target Israeli entities). Note that the senders' address may be fake, and thus are not necessarily compromised.

If you identify similar emails in your organization, we can assist in investigation the event (type of malware/phishing etc.), and thus confirm our assessment that this is indeed a generic campaign rather than a spear attack. Note that several of the emails have in their content some Cyrillic letters.

Sender	Subject	Content	Attached file name
admin@mbs723.vps.phps.kr	FW: Pending Payments.	See attached payment.	USD11715MT103.docx
<dsymonds@iinet.net.au>			292473186.zip
<sales88@gsmland.pl>			780323483917847.zip
gertrude marquis <16marquis@dream-card.com>	PAYMENT	Here is a copy of your payment receipt. Thank you have a great weekend GERTRUDE MARQUIS 16marquis dream-card.com 810-278-0119 Ex. 7410	20170814823305876.rar
<inbal@bat-7.co.il>			683373.zip
PayPal Security Update <secure519@jmp.net>	Account records must be kept up-to-date	Please understand that if you don't update your account information, you're violating our Terms Of Service	FormAttachment.html

Sender	Subject	Content	Attached file name
PayPal Security Update <safeguard@secured.com>	Update required	At PayPal, protecting your account's security is our top priority. Recently, we have received reports from other registered users that y	PAYPAL-FORM.html
PayPal Update Notice <info1@inform.us>	Your records must be valid	Keep your account records up-to-date is	paypal-attach.html
PayPal Security Update <information@great.net>	Update inquiry.	It is of utmost importance that you're able to update your account information	Update-Form456.html
PayPal <mandate@star.net>	Please update your information now	Please get your account information up-to-date. After reviewing your records, some	paypal-form.html
Apple <Unoreply@appstorezap.co.il>	Your Apple-ID Temporarily locked	Apple Inc. This email confirms that your subscription with iTunes has been expired with all additional services Your account is on hold, waiting for renewal, you have 48 hours or we will be obliged to close it please renew your subscription as fast you can Click on renew now and follow all steps	
Casey Sawers <casey.sawers@louisesamphotography.com>	PIC_5561		PIC_5561.7z
Noe Tozer <noe.tozer@web-time.co.il>	JPEG_6005		JPEG_6005.7z
Rosalyn <rosalyn.nethercote@repairpc.co.il>	Paper		f5b31cf86.pdf
Shahid Ullah Shahid <shahid.alnahr@gmail.com>	proforma inv	Dear Sir, Please find the attach book list and send to us proforma of the same as soon as possible. Thanks. KB Sharma proforma inv.pdf	image.png
"PayPa@ Support" <unconfirmedinformation>	Paypal Support:Suspicious Transaction-case id PP-123-432-12-0	Thank you for using PayPal. Suspicious Transaction. Your account just make suspicious transaction, We've temporary limited your account due to this suspicious activity until the issue is resolved. If You didn't authorize this transaction, please dispute transaction soon.	Dispute case id @PP-123-432-12-0.html



Over the last few years there have been two notable Gaza cyber-terror groups targeting Israeli companies and organizations – Arid Viper and Molerats (Hamas and the Islamic Jihad respectively). These groups’ attacks are characterized by a low-intermediate technological level. Accordingly, their operations are exposed by law enforcement agencies and cyber security companies (the operations we exposed were reported in our weekly intelligence reports and public reports such as DustySky¹³³).

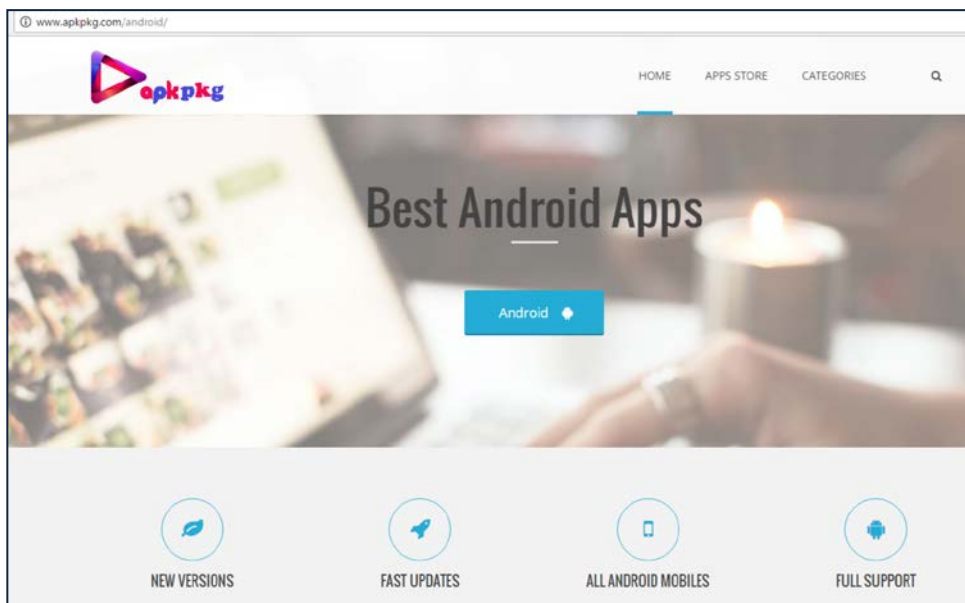
On 11.01.2017 the IDF exposed an attack campaign, in which the Hamas created 17 fraudulent Facebook profiles used to lure soldiers to install malicious apps on their cellphones. The fake profiles showed various public photos and of soldiers in Israel and abroad.

As seen below, most of the profiles have pictures of attractive women:



These virtual entities lured soldiers to enter an alternative Android app store create by the Hamas (apkpkg[.]com) and download video chat Apps:

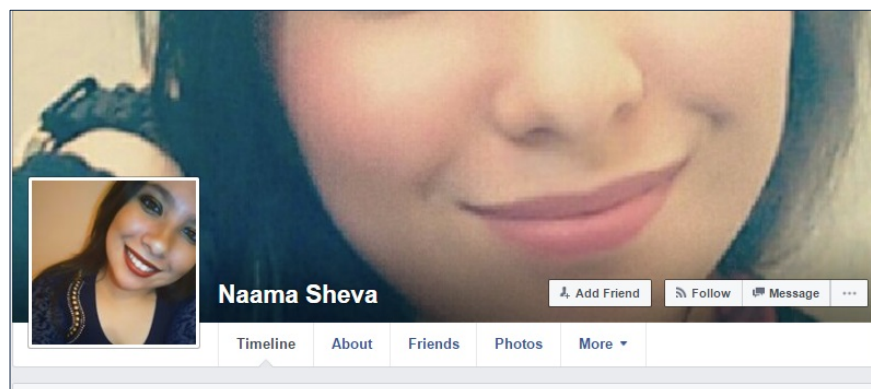
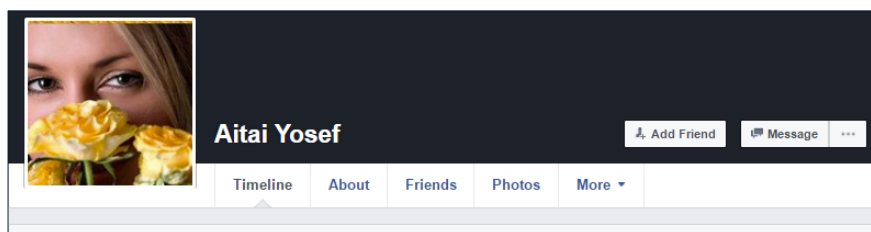
¹³³ www.clearskysec.com/dustysky2/



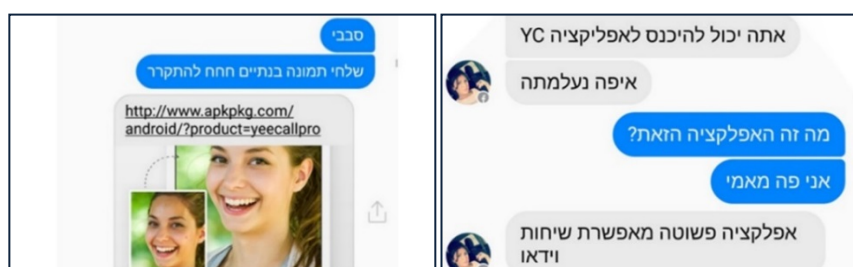
The site's source code contains text in Arabic, which indicates carelessness and low technical capabilities.

The malicious apps, named **YeeCall Pro**, **SR Chat** and **Wowo messenger**, enables attackers to gather data such as contact list, SMS and call history, and GPS location from infected devices. Additionally, it enables them to take control of the device and take photos, record the surrounding and calls, download and remove files and apps. Below are screen captures of several of the fake profiles before they were shut down:





Below are examples of conversations between the malicious actors and IDF soldiers, who are prompt to use the fake store and Apps:



BEC attacks against Israeli companies

Due to the constant proliferation and growing sophistication of BEC attacks we recommend reviewing these events in order to increase awareness and improve your mitigation protocols for such attacks.

First incident: Israel Police jointly with International law agencies shut down an Israel-based financial criminal group (case 278)

In early March Israel Police arrested 20 Israeli citizens who allegedly executed BEC frauds (Business Email Compromise) ¹³⁴ ¹³⁵. Concurrently, the FBI jointly with additional law agencies around the world, have arrested and indicated 19 People following investigations into international fraud and money laundering rings.

The US indictments claims that over \$13 million were stolen from more than 170 organizations, primarily in the United States. Further, the indictment details over \$10 million in transactions involving six companies from Germany, Spain, Finland, and Portugal. However, it is also stated that the FBI's investigation has yielded the disruption or return of more than \$56 million in victim funds.

Further, while investigating, the FBI also uncovered an-unlicensed money transmitting network ("hawala") operating in the United States, Europe, and Israel. Hawala is a system of transferring money, in which the money is paid to an agent who then instructs an associate in the relevant country or area to pay the final recipient¹³⁶. Moreover, according to Israel Police, the Israeli-Arab Hariri crime organization (one of Israel's most powerful and dangerous organized crime groups) was hired to provide protection through the use of threats and extortion, in exchange for a percentage of the proceeds

Second incident: targeted spear BEC attack against an Israeli company

In late May we assisted an Israeli company that was hit by a targeted spear BEC attack. Below is an outline the attack vector; however, note that no identifying details of the company are disclosed.

Phase One – gathering intelligence prior to the attack (from the post-attack analysis)

Prior to the attack, the attackers begun collecting targeted info about the company. As of now, it is unclear why the attackers chose to attack this specific company. It is possible that they came across sensitive intelligence about the company which they realized could assist them in an attack. In any case, the attackers obtained critical info, and in particular about the company's accountant.

Phase Two – opening a fraudulent bank account at a foreign bank for the purpose of impersonating the company

The attackers opened a bank account under the company's name at a legitimate European bank.

Phase Three – taking control of the accountant's email account

At this stage, the attackers took control of the accountant's email account (the attack vector is unknown – either via a malware or a direct attack. In either case, from this point onwards, the attackers were able to monitor all of the account's conversations). By monitoring the accountant's email account, they apparently learned which of the

¹³⁴ <http://www.israelhayom.co.il/article/456457>

¹³⁵ <http://www.timesofisrael.com/as-israel-based-financial-fraud-soars-police-swoop-on-20-suspects-as-part-of-global-fbi-led-sting/>

¹³⁶ <https://www.justice.gov/usao-dc/pr/19-people-indicted-following-investigations-international-fraud-and-money-laundering>

company's clients are expected to pay significant sums of money (from invoices and wire transfer requests that the accountant received and issued). **The company's email is hosted on Microsoft 365 services.** One question is whether during that time, Microsoft tried alerting about unusual access to her account, and whether the attackers intercepted and block them.

Phase Four – setting up the scam

The attackers registered domains almost identical to the company and one of their larger clients.

Phase five – implementation of the con

Shortly before the company was supposed to receive a large wire transfer payment from one of their clients, the attackers sent an email from the accountant's email to the client's accounting department, requesting that just this one time they transfer the funds to a different account due to a tax audit.

Phase Six – sending an email from a fraudulent client's domain to verify the wire transfer request

In order to make the wire transfer request look more legitimate, the attackers sent the client's accountant a fraudulent email supposedly from one of their senior directors, "approving" the transaction. **This is a very interesting vector, which indicates that the attackers are highly organized and methodical.**

Phase Seven – the scam fails due to the client's awareness

Despite the attacker's considerable efforts to create an appearance of legitimacy for the unusual transaction request, the client's accounting department was alarmed and suspected that something was amiss. Consequently, the client directly called the company's accountant, and thus thwarted the attack.

Following this, the company realized that it had been targeted, and reached out to a law firm for legal and technical assistance.

Phase Eight – sending another client fraudulent emails from a domain impersonating the company

The attackers do not give up on their attack. After they were blocked from the accountant's email account, they began sending fraudulent emails to different client. The emails were sent a fake domain impersonating the company.

Our actions upon receiving the referral of assistance:

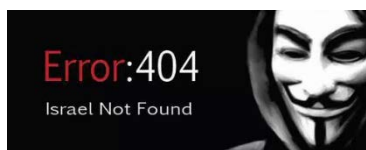
1. We requested to conduct a forensic investigation of the company's computers and systems (unfortunately the accountant's computer was immediately formatted upon discovery of the breach, thus preventing a comprehensive analysis of it).
2. We advised the company to issue its clients a notice regarding the fraud, warning them on the matter and inquiring whether any other client received similar requests; the company did so promptly.
3. We advised the company to file a complaint at the police's major crime unit Lahav 433, or with the relevant law agencies of the country in which the attackers opened the impersonating bank account.
4. We conducted a forensic investigation of the emails in an attempt to identify the attackers or find any identifying details – our investigation revealed several interesting indicators.
5. We began an ongoing monitoring of registrations of domain that may impersonate the company. Consequently, we identified fraudulent domains that impersonated both the company and one of its clients.

6. We contacted the CERT of the country in which the bank account was opened, and requested that the account will be immediately blocked and suspended (**this was executed promptly by the local CERT and the bank**).

Continued spearhead BEC attempts against Israeli companies

In early June, we assisted an additional Israeli company in resolving a BEC attack. The attackers attempted to steal money by taking control of the CEO's email account (Outlook 365), and using it to send the company's accountant fraudulent wire transfer requests. In this case the content of the email was written in proper Hebrew; presumably copied from the CEO's previous emails. Below are several reoccurring issues in regard to the companies' conduct leading up to the attacks:

1. They did not enable 2FA for accessing their organizational email accounts hosted on Microsoft cloud service.
2. They did not enable the cloud email security features.
3. They did not monitor the access log to the cloud accounts.
4. Most of their financial operations were conducted via email, which consequently made them to prime targets for BEC attempts.
5. The companies did not monitor their employees email accounts rules. This was exploited by the attackers by creating new sets of rules, including selective deletion of emails.
6. The attackers studied the companies' financial correspondences with their clients, and focused on large financial transactions.
7. Both companies encountered difficulties in obtaining the logs needed to examine the attack from their ISPs (both in Israel and abroad).
8. In the latter incident, the attackers were able to compromise the CEO's smartphone (Android OS), and subsequently his email account.



OpIsrael 2017 – the failure of anti-Israeli hackers

The outcome of the April 4th OpIsrael 2017 campaign illustrates the failure of anti-Israeli hackers activity. This year's campaign had a relatively low volume of activity, with few participants, and no significant attacks. In our assessment this campaign failed due to the following reasons:

1. The Israeli cyber deterrence – this effected both the number of participants and their level of capabilities.
2. The national infrastructure cyber defenses were adequately hardened.
3. The Arab/Islamic world is preoccupied with internal conflicts such as Syria and ISIS. As a result, the Israeli issue received little traction this year.
4. Most of the Israeli organizations and companies adequately prepared for this year's campaign.
5. Very few professional hackers took part of the campaign.

There is a gap of capabilities: the discrepancy between the baseline security level of Israeli organizations and the technical capabilities of the hackers has widened. The most significant events were hacking attacks and data leaks executed by the group #LaResistance against several Israeli companies. The leaked data contained personal and organizational information about both the targeted companies and their clients. This also exposed many other companies that hosted sites on the compromised platforms. It should be noted that LaResistance was not known prior to the OplIsrael 2017 campaign. Further, following the campaign, no activity attributed to them has been identified. It is possible that this is a nation-state or semi-nation-state actor that provided support to the campaign.

Concurrently to OplIsrael, **a counter-campaign named OplIslam was executed by Israeli hackers.** In this campaign, Arab sites were hacked or defaced, and credit cards details from various Arab countries were leaked. Although the campaign attempted to infect OplIsrael participants with malware, most of OplIslam's "achievement" were innocent individuals from Arab countries and Iran.

Operational insights from the campaign

1. Large organization and companies must examine their level of exposure with small/medium third-party service provider: the most significant leaks during this campaign were from medium sized Israeli companies (ad firms), that have considerable amounts of information on their clients. These companies often do not have adequate security systems. Note that a systems and/or database breach to such companies' may pose a significant threat to their clients. Accordingly, it is advised that when conducting business with such service providers to inquire and if needed demand that they have satisfactory security measures.

2. Large organization and companies must examine their level of exposure with their ISPs' web hosting services: most of the Israeli ISPs offer virtual servers to host websites and apps. Several of these servers were hacked in the recent campaign, compromising hundreds of the hosted websites. Breached ISP virtual servers endangers all the websites hosted on them. We recommend examining and confirming that there is a full segmentation between this system and where your site or App is hosted.

3. The level of the attackers' capabilities/campaign outcome do not indicate the robustness of organizations security system: in our assessment this campaign level of execution was notably low. Accordingly, organizations should not extrapolate from this event conclusions regarding their capability to mitigate future cyber-attacks.

Significant hacks and data leaks

During the event, only a handful of Israeli websites were successfully hacked. Further, most of the leaks published in this event were reused from older campaigns. **Unlike previous years, no new credit cards were leaked.**

Successful OplIsrael 2017 hacks

The most significant OplIsrael 2017 event is the activity of the group #LaResistance that hacked several Israeli websites of companies from various sectors. However, none of the sites that were hacked had security measures.

The sites that were hacked by the group are:

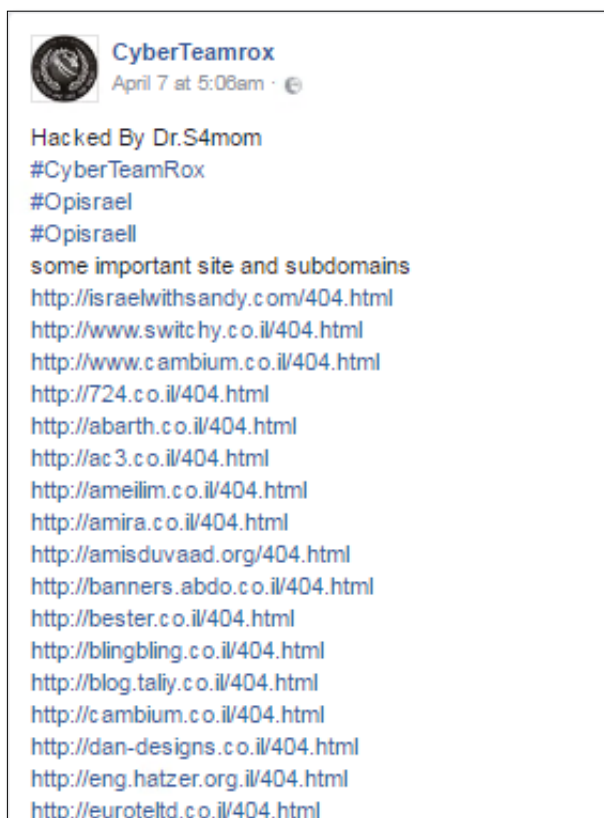
6. The advertising firm Pigment-Adv.
7. DataPlus – a company that provides management solutions for the advertising industry.
8. IATI (Israel Advanced Technology Industries). The website contained credentials of various prominent Israeli industrialists.
9. Amisragas – an Israeli-American gas company.

10. TOREC – a website for TV shows and movies subtitles (although the group claimed to have hacked the site, they did not leak its databases).

The group also claimed to have obtained the Admin password for Hotmobile's soldiers portal. Additionally, they published XSS vulnerability of several Israeli websites. However, only a handful of sites were actually hacked, from which the attackers leaked list of emails and passwords. Amongst these was a list of passwords for several hundreds to several thousand routers and online cameras in Israel that still had their default passwords. This list was likely compiled by wide scale scans.

Dafacements

Throughout the campaign, several hundreds minor websites were defaced. There were succesful defacement of any significant Israeli site.



DDoS attacks

There were no succesful DDoS attacks of note. Im most cases there were calls to execute attacks against the Israeli fincial/govermental sector, however none of these were succesful. Furthermore, in coninuation of the trend we seen since the previous campaign, some of participating members of the campaign took resposibilty for unrelated succesful DDoS attacks, or claimed to have succesful taken down fake websites that suposibly belong to the Israeli government.

Notable groups and individuals

Below are two of the most notable groups that took part in the campaign:

1. **LaResistance** - This group executed the most successful hacks during OplIsrael. The following hackers appear to be members of the group: x00, Sh4d0w, and Dl0rdN. There is no indication of activity by this group prior or following the campaign. Further, it has no social media presence.
2. **Giant's – ps** - This is a hackers group that supports the Palestinian cause. According to the location stated on the group's Facebook account¹³⁷ (Brooklyn New York), and the group's name (the Giants is New York's Baseball team), it is likely that the group is based in New York. The group is comprised by the following members: Sniper jo, m0oDyPl, Mahmoud Hacker, Marwan 007, InfoXmas, Matrix Hacker Gaza, MF-PS, Haxor.ps and Zrabba Rabba Zaki Ops.

Additionally, we saw low volume of activity and success rate from the following actors:

1. **Tunisian Fallaga Team**
2. **Minion-Ghost**
3. **Anonymous Lebanon**
4. **MajHoul and Anonymous RedCult**
5. **AnonymousGaza**
6. **John Kennedy**
7. **Dr. S4mom**

Activity of Israeli hackers

Concurrently to OplIsrael, a counter campaign dubbed OplIslam, was executed by Israeli hackers who defaced or hacked Arab websites, and leaked credit cards of citizens of various Arab countries. Further, they attempted to infect OplIsrael participants with malware; however, this campaign primarily effected innocent companies and individuals in Arab countries and in Iran.

In our assessment, this operation was executed by a group of Israeli hackers who are known to the cyber community, however currently have not yet caught the attention of law enforcement agencies in Israel and around the world.

¹³⁷ <https://www.facebook.com/pg/Giants.ps.official/posts/>
<https://www.youtube.com/channel/UCfd6KLmm31INE0OG3RcJYrQ>

OpIsraelFreeJuly - attempts to re-engage OpIsrael campaign

Throughout May we identified multiple posts announcing the re-engagement of OpIsrael campaign. These posts initially stated that the campaign will take place on May 5th, however, other than these statements no additional info was posted and eventually to actual operation came to fruition.

In early May we identified similar posts with a new date – June 15th. However, this time the actors behind this initiative also posted a list of targets and a generic propaganda manifesto by the group AnonGhost, claiming that they are involved in numerous campaign but are focusing at the moment on OpIsrael.

Similarly to the recent campaign, this list is mostly a repost from previous campaigns. It should be noted that this list does not have a clear theme, and contains many sites that are very loosely related to Israel. For example, it contains non-Israeli sites that have “Israel” tags or categories, such as tourism sites and porn sites.

Concurrently, the threat agent MinionGhost created a Facebook¹³⁸ event page for the campaign, now dubbed #OpIsraelFreeJuly2017, stating that it will take place between July 9th and July 15th. However, the event page did not provide any additional information, and the page’s Details box showed only AnonGhost’s manifesto.



This event received remarkably little exposure and interest (only 33 stated that they are “Going” and only 27 stated that they are interested). Further, the event had only two comments. The first was a link to the Pastebin target list, and the second was a link to the campaign’s non-operational IRC channel.

Additionally, our monitoring of Telegram groups revealed no new posts relevant to the campaign.

In accordance to our assessments, there was no noteworthy attacks against Israeli organizations and companies. Since April numerous posts containing target lists and list of leaked emails and IP

address were posted, however the vast majority of them were reposts from previous campaigns. It is possible that until next year's campaign there will be isolated defacement or DDoS attack attempts, however from previous experience, it is likely that the attackers will target small websites without any significant security measures, and that the overall technical level of the attackers will be notably low.

¹³⁸ <https://www.facebook.com/events/135611853669135/>

Timeline – Cyber Events and Attacks 2017

Target	Attack vector	State	Sector	Comments
January				
German Bundeswehr (armed forces)	Targeted attack	Germany	Military and Defence	The computer systems of the German army were rapidly attacked hundreds of thousands of time for 9 weeks in early 2017.
SWIFT	Targeted attack	India	Financial	Hackers issued fraudulent letters of credit by hacking the SWIFT systems of banks in India.
Czech Foreign Ministry	Targeted attack	Czech Republic	Government	Dozens of the ministry's email accounts were hacked.
Prominent politicians and business people	Targeted attack/ Malware	Italy	Government and businesses	Ongoing espionage campaign – used a variant of the EyePyramid malware
Advanced Flexible Composites Inc.	Hacking/Malware	USA	Manufacturing	The company's systems were hacked and infected with malware, shutting down all of the company's operation.
Australian Nuclear Science and Technology Organization (ANSTO)	Hacking	Australia	Governmental research agency	The attack vector was not reported.
Verity Health System	Hacking	USA	Healthcare	10,000 patient records stolen.
National Aids Research Institute (NARI)	Hacking	India	Healthcare	Private medical records were stolen.
Ukrainian shipping company	Wiper malware/ Ransomware	Ukraine	Shipping	New activity of the destructive malware KillDisk against the Ukrainian shipping company – the attacker demanded ransom of 200,000 dollars.
Several biomedical research facilities	Malware – industrial espionage	USA	Bio-med research	The malware was not detected for over two years.
St Louis Public Library	Ransomware	USA	Municipality	The attackers demanded a ransom of 35,500 dollars.
Washington DC police	Ransomware	USA	Law enforcement	A ransomware attack effected 70 percent of the public surveillance cameras employed by Washington D.C. The attack took place only eight days prior to the inauguration of U.S. president Donald Trump.
Racingpulse.in	Ransomware	India	Internet	Popular gambling site – infected by the Dharma ransomware.
Linking County	Ransomware	USA	Municipality	
The Los Angeles Valley College (LAVC)	Ransomware	USA	Academia	28,800 dollars were paid in Bitcoin.
Cancer Services of East Central Indiana - Little Red Door	Ransomware	USA	Healthcare	The hacker TheDarkOverlord contacted the CEO by SMS and demanded by threats a ransom.
Cockrell Hill Police	Ransomware	USA	Law enforcement	8 years' worth of evidence was lost.
Susan M. Hughes Center	Ransomware	USA	Healthcare	11 thousand patient records were compromised.
Emory Brain Health Center	Ransomware	USA	Healthcare	The ransomware encrypted a MongoDB database that was misconfigured – contained documents of over 90 thousand patients.
Bowlmor AMF	PoS Malware	USA	Entertainment	21 branches were affected.
POPEYES	Malware	USA	Fast food	10 branches' PoS systems were infected for 3 months. .
Ohio State Veterinary Medical Center	Malware	USA	Healthcare	Compromised financial records of 4,611 clients.

Target	Attack vector	State	Sector	Comments
Polish Foreign Ministry	Malware	Poland	Government	Attributed to APT28 (aka Fancy Bear)
India National Defense Academy (NDA) and National Investigation Agency (NIA)	Malware	India	Military and Defence	The attackers distributed a malware that steals personal and financial information via WhatsApp.
University of Alberta	Malware	Canada	Academia	About 300 computers were infected and the personal records of about 30 thousand students were compromised.
Princeton University	Malware	USA	Academia	Encrypted a MongoDB database.
Sunrun	Phishing - BEC	USA	Solar panels manufacturing	Spear phishing attack – employee tax forms were stolen.
Argyle school district	Phishing - BEC	USA	Education	Employee tax forms were stolen.
Netflix	Phishing	USA	Entertainment	Sophisticated phishing attack against US Netflix users – credentials and credit card details were stolen.
Dr. Web /Emsisoft	DDoS	Russia / Austria	Cyber security	The attacks were executed as revenge against the firms' investigation of criminal activity.
Lloyds Banking Group	DDoS	UK	Financial	The attack lasted two days and 100 thousand ransoms was demanded.
fbi.gov	Hacking - Plone CMS Vulnerability	USA	Government	Private records and document of 155 FBI agents were leaked.
Victoria's Human Rights Commission	Defacement	UK	Government	Executed by Anonymous
Google Brazil	DNS Hijacking	Brazil	Internet	Hackers hacked Google Brazil and redirected users to defaced sites.
Jabbim	N/A	Czech Republic	Internet	The chat services were hacked and an 8GB database was leaked on the Darknet.
Cellebrite	N/A	Israel	Data recovery and exfiltration	900GB database leaked – contained a technical data and information about the company's clients.
Multiple Thai Governmental job portals	N/A	Thailand	Government	Anonymous campaign – sensitive data of employees and citizens was leaked.
General Motors	N/A	USA	Car manufacturing	Compromised private employee data.
Sentara Healthcare	N/A	USA	Healthcare	Compromised private records of 5 thousand patients.
Several Chinese Internet Giants	N/A	China	Internet	Over a Billion accounts of various online Chinese services sold on Darknet market.
February				
Norwegian Labour Party	Targeted attack	Norway	Government	Executed by APT29 – 9 email accounts of members of the Labor party were hacked.
Italian Foreign Ministry	Targeted attack	Italy	Government	Hackers, likely Russian, hacked the email system and monitored for months the email communications.
Military and aerospace -Russia and Belarus	Targeted attack	Belarus / Russia	Military and aerospace	Chinese nation-state attackers
Mazagon Dock Shipbuilders Limited	Targeted attack	India	Defense	Nation-state espionage on a ship building company – builds submarines for the Indian army.
Ukraine	Hacking	Ukraine	Government – critical infrastructure	Renewed and ongoing campaign by Russian threat agents against critical Ukrainian infrastructure.
Over 60 governmental and academic organizations around the world	SQL	Global	Government/ Academia	Executed by a Russian hacker by the handle Rasputin

Target	Attack vector	State	Sector	Comments
Taiwanese Ministry of Foreign Affairs' Bureau of Consular Affairs (BOCA)	Hacking	Taiwan	Government	Over 15 thousand records of citizens were potentially compromised after the email system of the governmental agency was hacked.
Alton Steel, Inc.	Hacking	USA	Steel manufacturing	Compromised private employee data.
FunPlus	Hacking	China	Gaming industry	The penetration vector is unknown – 3.3 million clients account details and the source code of a developed game were stolen.
San Antonio Symphony	Hacking	USA	Entertainment	Hackers stole sensitive records of about 250 employees.
PharmaNet	Hacking	Canada	Healthcare	Hackers stole sensitive records of 7,500 citizens.
City of Troy	Ransomware	USA	Municipality	
Tiverton Town Council	Ransomware	UK	Municipality	
InterContinental Hotels Group	Ransomware	USA	Hotels	Effected the restaurants and bars of 12 properties.
Arby's	PoS Malware	USA	Fast food	About 1,100 branches were infected.
National Payments Corporation of India (NPCI)	Malware	India	Financial	Hitachi's PoS services in India were infected by malware – effected 3.2 million credit cards.
Ongoing campaign against the global financial sector	Malware	Global	Financial	Executed by Lazarus APT – the campaign began in October 2016.
Citizens Memorial Hospital	Phishing - BEC	USA	Healthcare	Spear phishing attack – employee tax forms were stolen.
Five Taiwan brokerages	DDoS/RDoS	Taiwan	Financial	Five brokerages firms were extorted by the group Armada Collective.
UPI (United Press International)	N/A	USA	Media	A hacker by the handle extorted was selling a UPI database - contained over 80 thousand credentials of the organization's website.
March				
WikiLeaks - Vault 7	Data leak	USA	Government	First leak from a series of leaks (25 so far) known as Vault7.
Lower House of Dutch Parliament	Ransomware	The Netherlands	Government	
Datapoint POS	PoS Malware	USA	Financial	
Mid-Michigan Physicians Imaging Center	Hacking	USA	Healthcare	The attackers gained access to medical records of over 106,000 patients. Reported only in July.
Lane Community College	Malware	USA	Academia	For over a year sensitive data was exfiltrated from the college infirmary.
Arkansas Department Workforce	Malware	USA	Government	The agency's databases were infected by malware that compromised sensitive data of about 19 thousand citizens.
Two un-named US Tech Companies	Phishing - BEC	USA	Tech industry	A Latvian citizen conned two unnamed American Tech companies for over 100 million dollars.
Defense Point Security, LLC	Phishing - BEC	USA	Defence	Spear phishing attack – employee tax forms were stolen.
Alfa Bank	DDoS	Russia	Financial	Widescale DNS botnet attack.
Undisclosed US College	DDoS	USA	Academia	Mirai botnet – the attack lasted for 54 hours.
McDonald's	N/A	Canada	Fast food	The company's Canadian job application site was hacked - compromised sensitive data of 95 thousand applicants.

Target	Attack vector	State	Sector	Comments
Major US Universities	N/A	USA	Academia	14 million emails addresses with passwords of major US universities were sold on the Darknet.
April				
SWIFT – ongoing campaign against the global financial sector	Targeted and ongoing hacking campaign	Global	Financial	Kaspersky lab together with BAE systems exposed the North Korean APT that attacked the global financing sector. Exposed a subgroup of the Lazarus threat agent – Bluenoroff.
Companies and organizations around the world	Ongoing hacking campaign – industrial espionage	Global	Various industries	The Chinese APT10 was exposed – executes industrial espionage to steal intellectual properties.
South Korean users in the public sector	Targeted attack	South Korea	Government	Speared and sophisticated attack against users of governmental systems and services.
IAAF	Targeted attack	Global	Sports	Executed by APT28 (aka Fancy Bear) – leaked medical information about athletes. .
South Korea Military	Targeted attack	South Korea	Military and Defence	Chinese hackers APT10 and Tonto team.
Danish Armed Forces	Targeted attack	Denmark	Military and Defence	Over two years military and defense personal were hacked. The attack is attributed to APT28 (aka Fancy Bear).
120 Israeli Targets	Targeted attack	Israel	Government	Widescale attack by the Iranian threat agent OilRig.
Grozio Chirurgija - Lithuanian cosmetic surgery clinic	Hacking - OpenCMS Vulnerability	Latvia	Healthcare	Hackers hacked the clinic's database and stole over 25 thousand photos, some of which nude pictures of patients. Sold on the Darknet for 300 Bitcoin.
Northrop Grumman	Hacking	USA	Military and Defence	Employees' tax forms were stolen.
WannaCry	Ransomware/Wiper malware	Global		Unprecedented widescale malware attack.
ABCD Paediatrics	Ransomware	USA	Healthcare	
Atlantic Digestive Specialists	Ransomware	USA	Healthcare	
Erie County Medical Center (ECMC)	Ransomware	USA	Healthcare	It took the hospital over a month to restore their systems and return to normal operation.
Greenway Health	Ransomware	USA	Healthcare	
City of Newark	Ransomware	USA	Government	
Pekin Community High School	Ransomware	USA	Education	The attackers demanded 37 thousand in ransom – the school chose not to pay.
Cleveland Medical Associates	Ransomware	USA	Healthcare	
Chipotle	PoS Malware	USA	Fast food	The magnitude of the breach was unreported.
Brooks Brothers	PoS Malware	USA	Retail	The malware went undetected for over 11 months.
20 UK Banks	Malware	USA	Financial	Trickbot banking malware. Escalation of attacks against UK banks. In April alone 5 different campaigns were executed.
Virginia State Police	Malware	USA	Law enforcement	The infection encrypted the email systems and sex offender's database.
KCG Holdings	Malware	China	Financial	IT staff member infected the company's systems in an attempt to steal sensitive information.
Westminster College	Phishing - BEC	USA	Academia	Spear phishing attack – employee tax forms were stolen.

Target	Attack vector	State	Sector	Comments
Melbourne IT	DDoS	Australia	Telecommunication	The attack disabled the ISP's services. .
Yapizon	N/A	South Korea	Financial	3,816 bitcoins were stolen (worth about \$10 million at the time). This was about 37% of all the crypto coin trade at the time.
Youku	N/A	China	Internet	A hacker sold on the Darknet sensitive information of over 100 million users.
May				
Several high-profile technology and financial organizations	Targeted attack	Global	Various sectors	Microsoft exposed an ongoing global campaign dubbed WilySupply targeting supply chains.
Aesthetic Dentistry OC/ Gastrocare Tampa/ Bay Surgery Centre	Hacking – data leak	USA	Healthcare	TheDarkOverlord leaked sensitive information of over 180,000 patients of 3 clinics.
Women's Health Care Group of PA (WHCGPA)	Ransomware	USA	Healthcare	300,000 patients were affected. Reported only in July.
German O2-Telefonica	Hacking	Germany	Telecommunication/finance	Some of the company's clients bank accounts were emptied.
Tufts University	Hacking	USA	Academia	Sensitive financial information of the university was leaked. Included also information of thousands of employees and students.
Debenhams	Hacking	UK	Retail	26,000 clients' personal details were stolen.
Wellington's Victoria University	Hacking	New Zealand	Academia	IT systems were hacked - management and student data was compromised.
Bell Canada	Hacking	Canada	Telecommunication	Compromised 1.9 million client accounts.
Nayana Web Hosting	Ransomware	South Korea	Internet	Erebus ransomware – a million dollars was paid.
St. Mark's Surgery Center	Ransomware	USA	Healthcare	Compromised medical records of 33,877 patients. The attack took place between April 13-17 however the center only detected it on May 8 th .
Sabre Corp. Hospitality Unit	Malware	USA/Global	Tourism	Compromised data of over 32,000 hotels around the world. The breach took place around September 2015.
UK Banks	Phishing - Domain Squatting	UK	Financial	Sensitive financial data was stolen via hundreds of phishing domains impersonating British banks sites.
NY Supreme Court Judge	Phishing - BEC	USA	Private individual	Supreme Court Judge was conned for over 1 million dollars.
Southern Oregon University	Phishing - BEC	USA	Academia	Over 1.9 million dollars were stolen.
Gannett Co.	Phishing - BEC	USA	Entertainment	Compromised 18 thousand employee records.
Bank of France	Phishing - BEC	France	Financial	Phishing campaign impersonating the bank.
UC Davis Health	Phishing / BEC	USA	Healthcare	Via email phishing attack the attacker compromised various systems and records of about 15 thousand patients. Leveraged the data to execute BEC attacks.
FCC (Federal Communications Commission)	DDoS	USA	Government	Disrupted the agency's normal operation.

Target	Attack vector	State	Sector	Comments
Molina Healthcare	Security Flaw	USA	Healthcare	Security vulnerability exposed sensitive patients' data – it is unknown how long the systems were compromised.
June				
Texas Association of School Boards	Hacking	USA	Education	Compromised sensitive data such as Social Security Number of thousands of teachers.
Several water utility providers across the US East Coast	Hacking	USA	Infrastructure	A former employee hacked and sabotaged the IT systems of 6 water supply stations.
Unprotected DB of 198 Million US Voters	Data leak	USA	Government	Unprotected DB of 198 Million US Voters hosted on an Amazon Bucket was identified by security researchers.
Airway Oxygen	Hacking and ransomware	USA	Aviation	Hackers hacked the company's systems and installed a malware. 5,000 clients were affected.
University College London (UCL)	Ransomware	UK	Academia	The university did not pay the ransom. As their systems were backed up hourly they were able to restore their data quickly and with no harm. The university claims that the infection was executed via a 0-day vulnerability.
Ulster University	Ransomware	UK	Academia	Similarly to the UCL attack, the university conducted hourly backups and thus could restore their data quickly and with no harm.
Radio station - KQED	Ransomware	USA	Entertainment	The attack deleted numerous systems and databases, shutting down the station for over 12 hours. The attackers demanded 1.7 Bitcoin for every infected computer, however the station chose not to pay and restore it systems instead.
Delaware Medical Oncology Hematology Consultants	Ransomware	USA	Healthcare	Medical records and documents of over 19,000 individuals were compromised. The attack was reported in in July.
Seven South Korean banks	DDoS/RDoS	South Korea	Financial	The banks were extorted by the group Armada Collective. Demanded 315 thousand dollars. .
Microsoft Skype	DDoS	Global	Software and communication	The attacks disrupted Skype services.
Petya/NotPetya - large-scale destructive attack against Ukraine	Wiper Malware	Ukraine/Global	Multiple sectors	Destructive malware impersonating a ransomware. Propagated by presumably Russian threat agents via an accounting software update. Effected over 2,000 governmental organizations and companies, including large international corporations from many sectors. Amongst the most notable companies that were hit are DLA, Merck, Maersk and Piper Mondelez.
Ohio government websites	Defacement	USA	Government	Pro ISIS hackers by the handle Team System DZ defaced the state's government sites.

Target	Attack vector	State	Sector	Comments
UK Parliament	N/A	UK	Government	The attack prevented access to email accounts of about 90 Members of Parliament.
July				
CoinDash	Hacking	Global	Financial	7 million dollars' worth of Ethereum were stolen.
Parity	Hacking	Global	Financial	32 million dollars' worth of Ethereum were stolen.
Dow Jones	Security breach	USA	Financial	A misconfiguration of an Amazon server exposed personal info of 2.2 million customers.
Hard Rock Hotels & Casinos	Hacking	USA	Entertainment	Following the Sabre breach (May 2017), for over six months the attackers had access to the chain's booking system, compromising clients' personal and credit card info.
Loews Hotels	Hacking	USA	Entertainment	Following the Sabre breach the attackers had access to the chain's booking system, compromising clients' personal and credit card info.
Four Seasons Hotels and Resorts	Hacking	USA	Entertainment	Following the Sabre breach the attackers had access to the chain's booking system, compromising clients' personal and credit card info.
B&B Theatres	Malware	USA	Entertainment	In September 2015 the chain's PoS system was infected by malware, compromising clients' credit card info.
Swiss banks	Malware	Switzerland	Financial	Infected by a Trojan malware.
Alaska Department of Health and Social Services	Malware	USA	Healthcare	The attack possibly compromised personal info of 500 individuals.
Kaleida Health	Phishing	USA	Healthcare	Largest healthcare provider in New York state. Sensitive medical records of 2,800 patients were compromised.
Kansas Department of Commerce	Hacking	USA	Government	The breach exposed sensitive info (such as SSN) of citizens across 10 US states.
Bank of America customers	Phishing	USA	Financial	The attackers sent fraudulent emails impersonating the bank's clients and stole sensitive private and financial info.
Cryptocurrency exchange	Hacking	USA	internet/financial	8.5-million-dollar worth of Ethereum coins were stolen.
Unnamed Canadian Organization	Ransomware	Canada	N/A	A ransom of 425,000 dollars in Bitcoin was paid. Reported by the cyber security firm Cytelligence, who are also investigating the attack. The organization was infected via a spear email with an attachment of a malicious PDF file. When opened, the ransomware exploited unpatched security flaws.
Sweden's Transport Agency	Data leak	Sweden	Government	Sweden's Transport Agency exposed sensitive data of nearly all its citizens back in 2015. The event was detected in 2016 and was publicly reported in July 2017.
August				
Loopia	Hacking	Sweden	Internet	The web hosting's entire client database was leaked.

Target	Attack vector	State	Sector	Comments
Crystal Finance Millennium	Hacking	Ukraine	Internet / financial	Popular accounting software vendor – had their web server hacked.
CeX	Hacking	UK	Retail	The second hand electronic retailer reported that it was hacked and personal info of 2 million clients were stolen, including passwords and credit card details.
Pacific Alliance Medical Center	Ransomware	USA	Healthcare	266,123 medical records were compromised.
Sinopec	Ransomware	China	Critical infrastructure	One of the oil field offices of the petro-chemical corporation was infected by ransomware. The scale and ramifications of the infection was not reported.
Scottish Parliament	Brute force	Scotland	Government	The attack disrupted operation and prevented access to various systems.
Cryptocurrency platform Enigma	Hacking	USA	Internet / financial	Over half a million dollars in Ethereum coins were stolen.
Tettagouche State Park	PoS Malware	USA	Entertainment	The park advised clients to check their bank accounts.
Bittrex	Phishing	USA	Internet / financial	A fake site impersonated the crypto coin exchange market. Users' Crypto coins and credentials were stolen.
Kaleida Health	Phishing	USA	Healthcare	The healthcare provider fell victim to a second phishing attack within two months, compromising personal info of 744 patients.
German state parliament	Spear phishing - Ransomware	Germany	Government	The attack shut down the parliament's phone and internet systems.
September				
Equifax	Targeted attack – vulnerability exploitation	USA	Financial	One of the largest credit rating companies in the world. The attackers stole personal and financial data of over 140 million US, UK and Canadian citizens
Multiple US and European energy companies	Targeted attack	USA and European countries	Infrastructure	Symantec exposed a wave of attacks beginning in May 2017 by the Russian threat agent Dragonfly (aka Energetic Bear) against governmental and private organizations within the energy sector.
Deloitte	Hacking	USA	Financial Industry	The attack was detected in March but the attack was executed in October 2016
Sonic	Hacking	USA	Food industry	Millions of clients' stolen credit card info is sold on various darknet markets for 25-50 dollars per card.
Taringa	Hacking	Argentina	Internet	The social network (known as the Latin Reddit), was breached, and data about all of its users – 28 million individuals was leaked.
West Australian TAFE	Hacking	Australia	Academia	Personal info of 13,000 students was stolen.
AXA Insurance	Hacking	Singapore	Financial	Personal info of 5,400 clients was stolen. The breach vector was not reported.
Adult Internal Medicine of North Scottsdale	Hacking	USA	Healthcare	Executed by TheDarkOverlord. Stole records of about 11,800 patients.

Target	Attack vector	State	Sector	Comments
Line 204 – film production	Hacking	USA	Entertainment	Executed by TheDarkOverlord. Stole a database with client info. The vector was not report nor if any financial info was compromised.
Whole Foods Market	PoS Malware	USA	Food industry	Credit card info was stolen from several branches.
Danish Ministries of Immigration and Foreign Affairs	DDoS	Denmark	Government	Attacked by the Turkish group Aslan Neferler Tim.
October				
FirstHealth of the Carolinas	Malware	USA	Healthcare	A new variant of WannaCry.
Bad Rabbit	Ransomware	Russian and Ukraine	Government/industries/private individual	A new variant of Petya.
Czech Election Sites	DDoS	Czech Republic	Government	The attack shut down the websites of candidates.
Sweden' Transport Agencies	DDoS	Sweden	Government	The attack caused delays.
Several Spanish government websites	DDoS	Spain	Government	Was executed as part of OpCatalunya.
Tarte Cosmetics	Data leak	USA	Cosmetics	Due to misconfiguration of the security system, a database with data pertaining to 2 million clients, was publicly exposed. identified and leaked by the hacktivist group CRU3LTY.
Daewoo Shipbuilding & Marine Engineering Co Ltd	Hacking	South Korea	Government/ship building industry	Suspected that North Korea executed the attack. Stole South Korean warship blueprints. The attack was reported in October but was executed in April 2016.
Hyatt	Hacking	Global	Tourism	Credit card and private info of clients from around the work were exposed. Was executed between March 18 and July 2 2017, but was only reported publicly in October.
Pizza Hut	Hacking	USA	Food industry	Private and credit data of undisclosed number of customers was compromised.
Microsoft	Hacking	USA	Software industry	In October it was reported that Microsoft that in 2016 it detected a breach with its internal network error monitoring system. The firm resolved the breach but did not report it. The incident was exposed after five ex-employees gave interviews on the matter to Reuters.
London Bridge Plastic Surgery (LBPS)	Hacking	UK	Healthcare	TheDarkOverlord stole sensitive photos of patients.
Midland County	Hacking	USA	Government	Third party provider was breached. Unknown if sensitive data was exposed.
NATO	Hacking	Global	Military	4,000 NATO soldiers serving in Europe were hacked.
NSA (National Security Agency)	Hacking	USA	Government	Russian threat agents hacked the agency and stole secrete data regarding its cyber operation. Including its security systems and operations targeting foreign actors. Possibly executed via a backdoor with Kaspersky's AV.
John Kelly - White House Chief of Staff	Hacking	USA	Government	His phone was hacked around December 2016.

Target	Attack vector	State	Sector	Comments
The Far Eastern International Bank	Malware	Taiwan	Financial	60 million dollars were stolen after the attackers installed a malware within the bank's servers, enabling them to exploit the SWIFT system.
Japanese banks	Malware	Japan	Financial	Part of Ursif campaign (Gozi).
FirstHealth	Malware	USA	Healthcare	Variant of WannaCry.
Iranian citizens	Ransomware	Iran	Government/industries/private individuals	The Iranian CERT issued an alert warning about a ransomware named Tyrant that impersonates a popular VPN software
Chase Brexton Health Care	Phishing	USA	Healthcare	Four employees fell victim to a phishing attack. Granted the attackers with full access to their email accounts. IT was not disclosed if any sensitive info was compromised.
Myethereumwallet.com	Phishing	Global	Financial Industry	Over 15,000 dollars' worth of crypto coins were stolen.
November				
Swedish radio station RadioPlay - MixMegapol	Hacking	Sweden	Entertainment	The attacker hacked the station's systems and broadcast for 30 minutes pro-ISIS songs.
Tether	Hacking	Global	Financial Industry	31 million dollars' worth of USTD crypto coins were stolen.
Imgur	Hacking	USA	Social media	The company reported that in 2014 it was hacked and 1.7 million accounts emails and passwords were exposed.
Forever 21	Hacking/ Malware	USA	Retail	Clients' credit cards info was stolen from several stores after their PoS systems' encryption feature was not enabled. Was executed between March-October 2017. The penetration vector was not reported.
Bulletproof 360, Inc.	Hacking / malware	USA	Food industry	The coffee supplier's website was hacked and over five months between June 20 and October 19, 2017, credit card info was stolen.
Vault 8	Data leak	USA	Government	Source code of HIVE, the CIA's malware management software, was leaked.
Uber	Hacking	USA	Transportation	Executed in late 2016. Full names, email addresses and phone numbers of 57 million clients and 600,000 drivers were compromised.
Toms River police	Hacking	USA	Government	Sensitive info of 3,700 residents was possibly compromised.
NIC Asia Bank	Hacking	Nepal	Financial	4.5 million dollars were stolen.
Companies and organizations in Germany	Ransomware	Germany	Multiple sectors	Ordinrypt ransomware is sent to numerous companies via phishing emails impersonating Curriculum Vives.
Global ransomware attack – malicious emails attached with Scarab	Ransomware	Global	General	Massive wave of over 12 million malicious emails containing the malware Scarab. Propagated via the largest spam botnet in the world – Necurs.
Proctor School District	Ransomware	USA	Education	

Target	Attack vector	State	Sector	Comments
The City of Spring Hill, Tennessee	Ransomware	USA	Municipality	Infected after an employee opened a malicious email. 250,000 dollars were demanded but it was decided not to pay the ransom and restore the systems instead.
Central Statistics Office Ireland	Data leak	Ireland	Government	Due to human error, sensitive info of about a thousand citizens was exposed.
INSCOM (United States Army Intelligence and Security Command)	Data leak	USA	Government	Highly classified data was hosted on an unsecure Amazon server.
The National Credit Federation	Data leak	USA	Government	110Gb of sensitive data was hosted on an unsecure Amazon server.
December				
Nissan Canada	Hacking	Canada	car manufacturing	The attack compromised info such as full names and address, VIN numbers, credit score, loan amount and monthly payment of 1.13 million customers. Nissan claims that no payment information was compromised.
Globex	Hacking	Russian	Financial	The attackers attempted to steal 10 million USD, but achieved only 95,000 dollars.
Netshoes	Hacking	Brazil	Retail	The hackers leaked on Pastebin a database containing emails, addresses and date of birth of 17,000 Netshoes consumers.
NiceHash	Hacking	Global	Financial	Crypto-Mining Marketplace - 4,736.42 Bitcoins were stolen (worth about 65 million dollars).
Osaka University	Hacking	Japan	Academia	Personal info of 80,000 students and staff may have been compromised.
Fox-IT	DNS Hijacking	The Netherlands	Cyber security	
State of California	Data leak	USA	Government	A database containing personal info of almost all of the state's voters was hosted on an unprotected MongoDB databases, which was stolen and held to ransom.
Mecklenburg County, North Carolina	Ransomware	USA	Municipality	Infected several servers, preventing access to computer systems that manage inmate populations, child support, and other social services. The county is refusing to pay the 23,000 ransom.
National Capital Poison Center	Ransomware	USA	Government	It was not reported whether a ransom was paid or the org attempted to restore its systems.
John Kahlbetzer	Phishing - BEC	Australia	Individual person	Richest man in Australia – lost 1 million dollars in BEC scam.
Baptist Health Louisville	Phishing	USA	Healthcare	An employee's email account was compromised and was used to send phishing emails.

Target	Attack vector	State	Sector	Comments
Warwick University	DDoS	UK	Academia	
Bitfinex	DDoS	Global	Financial	The Cryptocurrency market place was forced to shut down operation following a series of continuous attacks.