



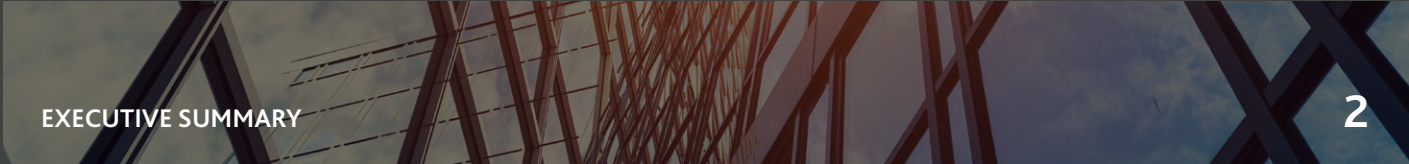
AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

BDO CYBER THREAT INSIGHTS REPORT 2017-2018

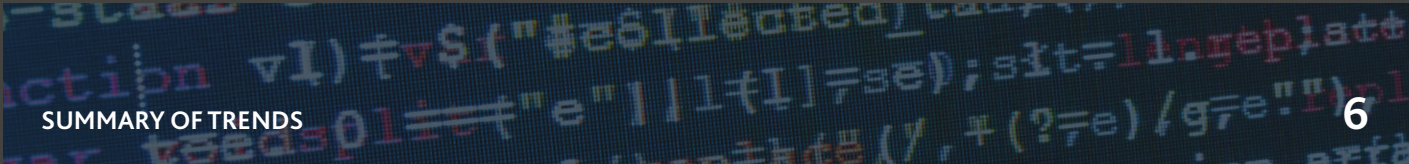
Contents



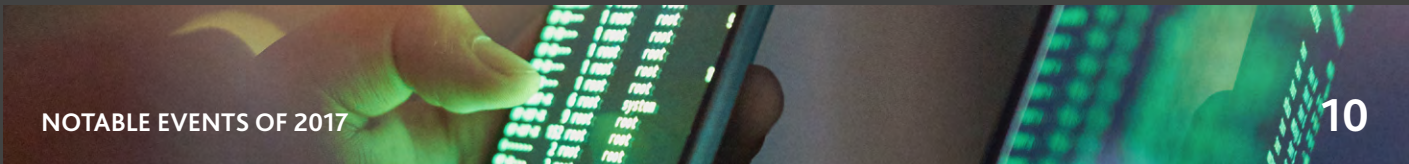
INTRODUCTION 1




EXECUTIVE SUMMARY 2



SUMMARY OF TRENDS 6



NOTABLE EVENTS OF 2017 10



TIMELINE OF MAJOR EVENTS 43



ABOUT BDO CYBER THREAT INSIGHTS 66

Introduction

In 2017, we saw the security risk environment continue to rise as a major concern for many organizations. In order to protect an organization's risk, executives must maintain awareness of recent cyber-attacks, significant trends, and changes in the threat environment. The BDO Cyber Threat Insights Report presents a compilation of the significant cyber events of 2017, cybersecurity trends, and some predictions for 2018 based on our ongoing research, which BDO has conducted for clients across many market sectors globally.

Throughout this report, BDO will provide a summary of significant trends, a focus on the major events of the past year, and a timeline of the most notable attacks, information that all c-suite executives should be aware of.

Our research is based on open source information in addition to insight gathered by our analysts through their daily activities in monitoring & investigating client-defined intelligence objectives and targets. This report does not represent a survey of our clients, present any client confidential information or opinion, nor is it based on confidential end-user or victim disclosures.

This report is designed to highlight the key aspects that have characterized 2017 and will delve into the following significant cyber events:

- ▶ Petya/NotPetya
- ▶ WannaCry
- ▶ Equifax breach
- ▶ SWIFT
- ▶ The return of Shmoon as 2.0
- ▶ StoneDrill in use against Saudi Arabian interests, and
- ▶ Interesting developments within 'darknet markets'.

In many of these cases and others, this report offers key focused insights on the events and recommendations for mitigation. These cases prove the importance of basic-but-key security sanitary measures and the need for a robust security controls framework. In many cases monitoring and detection is highly recommended as part of risk mitigation, as is a formalized response plan for a broad range of scenarios and 'unknowns', irrespective of the size of the organization.

FOR MORE INFORMATION PLEASE CONTACT

GREGORY GARRETT

Head of U.S. &
International
Cybersecurity
703-770-1019
ggarrett@bdo.com



ERIC CHUANG

Managing Director
Incident Response &
Threat Intelligence
202-644-5435
echuang@bdo.com



Executive summary

SIGNIFICANT TRENDS

CRASH OF THE "EGGSHELL SECURITY" PARADIGM

The Eggshell Security model, primarily based on implementing comprehensive outer security measures and keeping the inner "core" exposed, has 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 have been neglected.

Many organizations allocate considerable resources to their outer security layer at the expense of inner security systems. This imbalance enables attackers to easily spread across various systems once an organization has been penetrated.

In retaliation of hybrid attack vectors that use multiple techniques to ensure success, this paradigm is becoming increasingly ineffective. Attacks such as NotPetya and WannaCry have demonstrated and emphasized that this paradigm is outdated and no longer sufficiently effective.

EXPLOITATION OF SUPPLY CHAINS

2017 brought about a significant increase in successful attacks exploiting supply chains (i.e. third-party service providers) in order to compromise their targets. Often, these attacks have been executed in conjunction with the exploitation of vulnerabilities in OS and communication protocols.

INSTANTANEOUS EXPLOITATION OF 1-DAY VULNERABILITIES

In 2017, attackers were more frequently exploiting 0-day vulnerabilities and developing new attack tools following the publication of corporate reports.

WIDESCALE DDoS ATTACKS

2017 has registered a significant increase in the frequency of global Distributed Denial of Services (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. 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.

2017 has illustrated that attackers no longer need to invest time and effort into uncovering unknown vulnerabilities in order to execute significant attacks; they merely need to monitor channels of information that report newly discovered weaknesses. At that point, they are able to leverage the gap between the vulnerability being discovered and the organization updating their systems with the relevant security update. This may take several weeks or even months. The WannaCry event is a prime example of such an attack.

PROLIFERATION OF ATTACK TOOLS

Similarly to exploitation of 1-day vulnerabilities, we have seen a rapid increase of attack tools. Recently, leaked NSA attack tools were quickly adopted by attackers from North Korea, Russia, China, and other countries.

PRIME TARGETS

DEMOCRATIC PROCESSES AND PUBLIC PERCEPTION

In 2017, cyber-attacks aimed to undermine democratic processes and change the political status quo both in the U.S. and globally. Attackers have spread misinformation designed to alter public opinion, as well as attempted to sabotage elections and public opinion polls. The creation of thousands of fake social media profiles contributed to this. Some examples of politically minded cyber-attacks are: the propagation of fake news in the Ukraine; attempting to alter election results in the U.S. and France; and aiming to influence the outcome of the Brexit referendum in the UK.

PROMINENT MULTINATIONAL CORPORATIONS

Wide scale destructive attacks against prominent multinational corporations has been one of the most prominent trends witnessed in 2017. Tens of thousands of work computers and corporate organizational core systems have been corrupted due to cyber-attacks, billions of dollars of damage, as well as months of disrupted operation, have illustrated this threat to c-suite executives across the world.

FINANCIAL SECTOR

Core banking systems such as SWIFT and ATM networks have been prime targets for cyber-attacks in 2017. More specifically, banks located in Eastern Europe and East Asia, have been targeted, and successful attacks have resulted in the theft of hundreds of millions of dollars.

CRYPTOCURRENCY MARKETS AND WALLETS

As use of cryptocurrency rises as an accepted means, attackers are turning their attention towards them. This year, several hundreds of millions of crypto coins have been stolen through various scams and attacks.

PROMINENT ATTACK VECTORS

- ▶ **Attacks exploiting the supply chain:** This consists of 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 government, in the Ukraine.
- ▶ **Exploitation of native vulnerabilities with OS and communication protocols:** This vector grew in 2017, in part, due to a series of nation-state attack tool leaks dubbed Vault7. This threat increased after November 9th when the source code of HIVE, the CIA's malware management software, was leaked.
- ▶ **Ransomware extortion attacks:** Throughout 2017, hundreds of businesses, NGOs, government organizations and private individuals have fallen victim to ransomware attacks.
- ▶ **BEC (Business Email Compromise) scams:** Attackers impersonate executives in the company, requesting that the target (often someone in a financial department) immediately and covertly wire transfers money for reasons such as an urgent and secretive, yet highly important, business deal. According to an FBI report, companies in the U.S. have lost over \$5 billion to such attacks over the last two years.

MAJOR ATTACKS OF 2017

1. PETYA/NOTPETYA

One of the largest and most destructive cyber-attacks, Petya/NotPetya took place in late June 2017. The attack wiped thousands of computers and disrupted the operation of numerous companies in the Ukraine and countries that conduct business with them.

As of December 2017, this was the single most costly cyber-attack of the year. It is estimated that the total sum of damages reached around \$1.2 billion.

2. WANNACRY

On Friday, May 12th, the WannaCry attack initiated an unprecedented global event, infecting and damaging over 230,000 computers across 150 countries within a single day.

3. EQUIFAX BREACH

In early September 2017, the consumer credit rating agency, Equifax Inc., reported falling 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 citizens.

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

4. LEAK OF NATION-STATE ATTACK TOOLS AND DOCUMENTS

The CIA document leak, in conjunction with the NSA 0-day vulnerabilities and attack tools leak, has 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).

PREDICTIONS FOR 2018

CONTINUED EXPLOITATION OF THE SUPPLY CHAIN FOR VARIOUS ATTACK VECTORS

The largest attacks this year have illustrated that breaching a third-party service provider in order to execute an attack on a company that uses its services or product, is highly effective. However, this vector can be used to considerably expand the scale of attacks, as well as the success rate. In our assessment, this vector will be extensively utilized in 2018.

INCREASED ATTACK ATTEMPTS AGAINST THE FINANCIAL SECTOR

Throughout the past two years, 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 the moment it becomes used as an attack tool around the world is rapidly shrinking. A prime example can be seen in 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 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 potential initial difficulties in adapting, going forward, we expect to see more transparency from European organizations regarding malicious activity.

7 RECOMMENDATIONS FOR 2018



1

Allocate additional resources to interorganizational security systems.

Recent developments in hybrid attack vectors prove that the outer security shell can no longer prioritize the inner security framework.



2

Transition to a more holistic cybersecurity model.

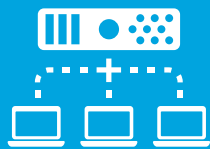
Organizations will have the ability to more effectively cope with the accelerated evolution of attack methods that we have witnessed in recent years.



3

Segment networks

and take core systems offline.



4

Create an emergency backup system.

This will allow organizations to operate for up to three months after being hit by a destructive cyber-attack.



5

Minimize the time-gap between the release of security patches and their installation.

Examine how to rapidly implement a policy to install security patches, despite the potential risk of disruption to an organization's normal operation.



6

Raise employee awareness about new attack vectors.

Most notable are social engineering techniques and significant campaigns.



7

Optimize Monitoring, Detection, and Response (MDR) capabilities.

Explore the use of highly qualified Managed Security Services Providers to reduce operational expenses and enhance incident detection and response.

A woman in a dark green shirt is pointing at a computer monitor in a dimly lit office. In the foreground, a man with a beard is looking at a tablet. Another woman is visible in the background, working at a desk. The scene is illuminated by the glow of computer screens and a desk lamp.

Summary of trends for 2017

MAIN ATTACK TOOLS AND VECTORS OF 2017

RANSOMWARE/VIPER MALWARE

Ransomware attacks are becoming increasingly sophisticated and widespread. In several recent cases, attackers distributed wiper malware masquerading as ransomware, aiming to prolong the attacks.

MALICIOUS E-MAILS

Spear-phishing 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 over 51 million malicious emails.

In order to bypass security and email filtration systems, malicious actors are also incorporating social engineering techniques in their attacks.

Most common files attachments used in email attacks are .doc, .exe, .scr, .xls, .bin, .js, .class, .ace, .xml, and .rtf.

DYNAMIC DATA EXCHANGE (DDE)

In the latter part of 2017, a macro-less code execution method began receiving attention. This method is based on a native Windows function named DDE (Dynamic Data Exchange). However, Microsoft views this as a native feature rather than a vulnerability and therefore, has not released a security patch for it.

When opening a document that exploits this method, the user is presented with two notifications that he must approve in order for the code to run. The attacker has the ability to modify the wording on the second notification, causing it to appear less suspicious.

While this is not a new method, it is being used widely. Talos reported that this method was used in attacks impersonating the U.S. SEC (Securities and Exchange Commission), presumably by the cybercrime group FIN7. Recently, it was reported that nation-state threat agents, such as APT28 (a.k.a. Fancy Bear), are using this vulnerability.

This attack vector is one of the reasons Microsoft Office became the second most attacked software in 2017. On October 23rd, Microsoft published advice on mitigating this issue. Aside from recommendations to manually disable the DDE fields and OLE links automatic, Microsoft advised users to install the Windows 10 Fall Creator Update. This update enhances Windows Defender Exploit Guard's security capabilities by blocking DDE based malware.

SQL INJECTION

Attackers exploit websites or applications by escaping the SQL syntax in the application and then executes code on the remote machine. This is typically achieved using a login form or user controlled input which has not been properly sanitized. This vector has grown 62% since 2016.

WATERHOLE ATTACKS

Criminals lure targets to fraudulent sites utilizing methods such as phishing emails and spear-phishing. Once the site is accessed, the target is exposed to malware or exploit codes.

A spear-targeted attack occurs when the attacker creates content that is custom to a target's interests. Attackers often create websites that imitate a warning against malicious sites and prompt users download malware or provide sensitive information, such as login credentials or credit cards details. Over 72 million unique sites with malicious content have been identified between Q1 and Q3 of 2017.

Another common waterhole attack occurs when an attacker creates a website with a minor, almost invisible change in the URL. This past year, attackers registered the domain google[.]com to impersonates Google.com (the little G is a Latin character). As this method grows, the difficulty of identifying a fake URL remains difficult, as entire domains are registered with various languages that have similar characters to English.

MALICIOUS ANDROID APPS

Attackers lure victims to download and install malicious applications and external APK (Android application package) files using waterhole attacks. Pokémon Go users were tempted to install malicious versions under the ruse of an early release. Attackers promoted these malicious "early release" versions throughout various social networks.

DDoS ATTACKS EXECUTED WITH IoT BOTNETS

As attackers increasingly harness IoT devices such as botnets, 2017 has marked a 91% increase in DDoS attacks.

RDoS (RANSOM DENIAL OF SERVICE) EXTORTING COMPANIES WITH THREATS OF DDoS ATTACKS

Criminals are increasingly threatening organizations to pay ransoms through DDoS attacks, known as RDoS attacks. Seven South Korean banks fell under attack by the Armada Collective group, prompting them to pay a total \$315,000. These attacks are increasingly prevalent, as DDoS-for-hire services are becoming more commonly and easily available.

SOURCES AND FURTHER READINGS REFERENCES

[Spam and phishing in Q1 2017](#)

[Cybercrime tactics and techniques Q1 2017](#)

[Macro-less Code Exec in MSWord](#)

[Spoofed SEC Emails Distribute Evolved DNSMessenger](#)

[Russian 'Fancy Bear' Hackers Using \(Unpatched\) Microsoft Office DDE Exploit](#)

[Microsoft Security Advisory 4053440](#)

[Q3 2017 Akamai State Of The Internet / Security Report Reveals Significant Increase In Web Application Security Attacks, Evolution Of Attacker Strategies](#)

[Windows Defender Exploit Guard: Reduce the attack surface against next-generation malware](#)

[IT threat evolution Q3 2017. Statistics](#)

[Corero DDoS Trends Report](#)

MALICIOUS ACTIVITY TRENDS IN 2017

2017 has marked a dramatic increase in the proliferation and sophistication of malware activity. In Q3 of 2017, over 198 million malware samples have been detected by Kaspersky Lab, and almost 400 million malware incidents were detected by Comodo.

Evolved tactics and increased attacks have caused ransomware to become highly profitable for attackers making our previous prediction true; Ransomware has been the most significant cyber threat of 2017.

MOST ATTACKED SYSTEMS

During the latter of 2017, Microsoft Office rose to become the second most attacked software, comprising of 22.80% of all attacks, an increase from 10.26% in the first half of the year. This overtook Android OS, which now accounts for 22.71% of system attacks. This shift is due, in part, to the growing trend of DDE attacks, relying on macro-less execution of malicious code via a native Office function.

DDoS ATTACKS

As discussed earlier, 2017 has registered a significant increase in the frequency of global Distributed Denial of Services (DDoS) attacks, which have nearly doubled over the previous year, increasing 91% since January 2017.

MOBILE THREAT TRENDS

While computer systems remain the most significant cyber platform, 2017 showed an increase on malware attacks on mobile devices. These attacks have demonstrated a sharp increase in both their frequency and sophistication.

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

Table 1: Proportion of Attacks by Type of Software (Q3 & Q4 2017)

| Software | % of attacks |
|------------------|--------------|
| Browsers | 35 |
| Microsoft Office | 22.8 |
| Android OS | 22.71 |
| Java | 7.62 |
| Adobe Flash | 5.48 |
| PDF software | 1.39 |

Source: BDO Based on various open sources

Table 2: Most Common Ransomware Families 2017 (by % Attacks)

| Malware Family | % of attacks |
|----------------------|--------------|
| WannaCry | 16.78 |
| Crypton | 14.41 |
| Purgen/Globelmposter | 6.9 |
| Locky | 6.78 |
| Cerber | 4.3 |
| Cryrar/ACCDFISA | 3.99 |
| Shade | 2.69 |
| Spora | 1.87 |

Source: BDO Based on various open sources

Table 3: Most Common Mobile Malware 2017 (by % Attacks)

| Mobile Malware | % of victims |
|--------------------------------------|--------------|
| 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 | 2.2 |
| Trojan-Dropper.AndroidOS.Hqwar.i | 2.09 |
| Trojan.AndroidOS.Hiddad.pac | 2.05 |
| Trojan.AndroidOS.Triada.pac | 1.98 |
| Trojan.AndroidOS.lop.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 |

Source: BDO Based on various open sources

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 and disrupting the operation of numerous companies, both in Ukraine and that conduct business with Ukraine. The malware was disseminated via a software update of a legitimate, yet compromised, third party provider. At the time of this attack, this was the largest attack of its type.

THE DATE OF THE ATTACK

The attack took place the night prior to a Ukrainian holiday and vacation day – “constitution day”. This time was likely selected in order to inflict the most damage by ensuring that little or no staff were 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 update.

This is the first time this type of vector was seen in such 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 continued to spread within the company's internal networks by using the following two vectors:

1. Stealing credentials from infected computers that had access to different computers' admin. Note that malware propagated with this vector can also compromise up-to-date computers and servers that have the latest security patches.
2. 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 piece of malware and not a piece of ransomware. Therefore, the attackers did not seek financial gain, but specifically aimed to wipe/corrupt the infected computer's hard-drive and cause as much harm as possible. 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 to gain retribution against Ukraine, in addition to creating deterrence.

TARGETS

The malware was used against companies and organizations in Ukraine. In total, it seems that about 2,000 companies and organizations were affected, including governmental offices, banks, corporations, and small to medium business. Furthermore, as many international companies who operate in/with Ukraine also use MeDoc, they too have sustained considerable damage. Amongst them are Maersk (the world largest shipping company) and TNT, who struggled for a long time to restore their operations to normal levels. 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.

INVESTIGATION OF THE EVENT

About a week after the NotPetya attack (a.k.a Diskcoder, ExPetr, PetrWrap), the cybersecurity firm, Talos, and ESET published investigative reports revealing new findings regarding the attack. Findings proved that malware was disseminated in April 2017, rather than 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 of the software's users in April 2017.

THE WIPER MALWARE

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

Despite the fact that the attacker 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 module did not use any external servers for command & control. 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.

HOW TO BETTER PREPARE FOR FUTURE ATTACKS

In the days following the attack, we spoke to multiple information & cybersecurity executives 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 necessary, block malicious software updates from legitimate sources. Accordingly, a similar attack against companies outside the Ukraine 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 a robust security baseline with a key emphasis on – segmentation, implementation of strict authorization management, and maintenance of an 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 decide the course of action while having only fragmented and inaccurate information. Improving the information pipeline will allow organizations to receive more credible and accurate information, enabling them to implement better contingency plans to mitigate attacks. This is where cybersecurity services, anti-virus alerts and CERT alerts are central.
4. Global companies prepare to disconnect compromised branch offices from the organizational network during an attack. However, 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 email. Many organizations have been able to develop relatively effective defense mechanisms against it. However, these recent attacks exploit new vulnerabilities that require organizations to reevaluate their defenses and develop new security measures.

IMPLICATIONS

- ▶ Both the targeted organizations' security teams and security firms failed to identify the malware over a long period of time.
- ▶ Despite the fact that malware was disseminated to thousands of organizations in April and was used maliciously during that time, it was not identified until it began its destructive activity.
- ▶ There are no IOCs [Indicators of Compromise] that could have indicated the malware traffic and block it.
- ▶ Similarly to WannaCry and APT10's operations targeting the supply chain, it is currently impossible to identify, monitor, and block malware traffic sent through legitimate channels by using malicious IPs and domains IOCs.

SOURCES AND FURTHER READINGS REFERENCES

[BU has identified the involvement of RF special services in attacking the virus-extortionist Petya.A](#)

[The MeDoc Connection](#)

[XData ransomware making rounds amid global WannaCryptor scare](#)

[Ukraine Fears Second Ransomware Outbreak as Another Accounting Firm Got Hacked](#)

ANOTHER UKRAINIAN ACCOUNTING SOFTWARE PROVIDER WAS HACKED

In August, a similar attack was suspected after web servers of a Ukrainian accounting software, "Crystal Finance Millennium" (CFM), was hacked and used to host malware. However, unlike NotPetya, the attacker did not compromise the CFM server, which is used to distribute software updates.

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.

According to the investigation, it appears that this attack was in fact generic and unrelated. As of early December 2017, there have been no attacks, similar to NotPetya, against Ukraine.

On Friday, May 12th, the 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 underlying difficulties in rapidly implementing these updates concurrent to the evolution of the malware, it continued inflicting harm even several weeks after the event began.

On May 19th, Honda shut down operations in one of their Japanese plants after systems were infected by WannaCry malware. Several days later, on June 22nd, it was reported that 55 traffic lights and speed cameras in Australia were taken down after an employee used an infected USB drive.

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

**INSIGHT 1:**

The timeframe between being alerted to a threat and preventing damage to the organization 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 3:30PM, 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 global coverage of the events.

Within several hours, it became clear to all cybersecurity organizations around the world that this was a unique event. Furthermore, 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.

Aside from official reports, numerous social media outlets, including Twitter, were reporting directly from victims and employees of various affected organizations.

- ▶ 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.
- ▶ Large organizations are incapable of updating all its systems in the necessary timeframe of several hours.
- ▶ Organizations are challenged by their inability to quickly execute major changes to their systems, such as shutting down networks, servers, and suspending the organizations operation.



INSIGHT 2:

No security company or cyber researcher can fully contain and respond to a 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 similar 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 the cybersecurity eco-system. During the initial hours of the event, it was reported that the attack vector was through emails attached with malware. These reports were proven wrong, and currently, no sample of such malicious email has been 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 agents that further disseminated the malware. However, there is no evidence to support this theory. A possible alternative hypothesis is that the initial infection vector was through 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? Due to similarities in the code of the Swift malware, the standing theory attributes the attack to North Korea. However, the reason for an "off button" remains unanswered.
- c) Why didn't the attacker implement a more sophisticated mechanism to collect the ransom, and why did he not provide a decryption key? The fact that the system allowing victims to transfer ransom payments was lacking (for example, there were only three Bitcoin wallets), and the decryption mechanism was not activated (i.e. victims who paid the ransom did not receive decryption key), raises many of questions. Did the attacker not care about the money? Or, did he lack adequate capabilities which resulted in critical malware errors?

- ▶ 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 needed to provide adequate real-time assistance for these organizations.
- ▶ The process of investigating, analyzing, and exposing cyber-attacks is often lengthy and limited. The willingness of organizations and companies to adapt to defense of new attack vectors is fairly limited and demands a re-evaluation of the situation.

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

Many of the affected organizations took a significant amount of time to return to normal operations. Organizations' ability to recover following a major cyber-attack is slow and painful. This is primarily due to the need to continue providing service to their customers throughout the attack and the recovery period. The requirements for IT departments to both operate compromised systems, while also cleaning them and bringing them back to normal operation, is a near impossible task.

- ▶ Due to its complexity and the limited understanding most companies have of situations, rapid recovery from a debilitating event is impossible.
- ▶ Practicing and preparing for various scenarios will assist in shortening the response time but will not guarantee rapid recovery.

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

Achieving a robust security baseline is fundamental. Most of the affected organizations were unable to fulfill the basic info-sec requirements needed to limit the scope of this cyber-attack. Three core pillars are critical to mitigate such attacks and listed below:

- a) Installing security updates: Making sure that all of an organization's computer systems (workstations, servers, routers, switches, software, etc.) and/or computer-based systems, have the most current security patches. In our assessment, large organizations' capability of ensuring every server is continually updated with security patches is practically unachievable. Workstations have improved the situation, as most organizations update their workstations within every two months. In comparison, the server update is scheduled between two months and a year. For non-Microsoft based systems, this can be several years. Systems that cannot be updated with security patches should be removed from the network and segmented.
- b) Compartmentalizing and segmenting the organization's network is essential to significantly minimize a malware's ability to disseminate within the organization's system. Furthermore, the network segmentation and separation to different environments and components must implement principles of least privileged (PoLP; a.k.a Principle of Least Privilege) i.e. promoting minimal user profile privileges on systems, based on users' job requirements.
- c) Organizations must ensure that the system is backed up and set up in a manner that allows quick recovery. Backups should be capable of both surviving unharmed from a cyber-attack allowing for a rapid recovery process following a debilitating attack.

- ▶ Old school "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 report 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 2017, 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 and hptasks.exe, which 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, and two are variants of Destover - a tool used in the Sony Pictures attacks. The third, Volgmer, is a malware that was used by Lazarus in attacks against South Korean targets.

March – April WannaCry variant

By 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 through two different backdoor 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. Bravonc communicates with the same command and control 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 also has been previously linked to Lazarus.



MONITORING WANNACRY DISCUSSIONS ON RUSSIAN CYBERCRIME FORUMS

WannaCry created heated discussions amongst cybercrime communities, primarily revolving 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 to be 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.

Another possible explanation for this is that a large percentage of the operating systems (as well as software) used in these countries are pirated, thus preventing them from installing Microsoft's security patches.

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 comments, are because:

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 hard to use various attack vectors based on JS, DOC, and Macros as more organizations began blocking them.
4. They make it harder to distribute malware through spam.
5. Many compromised servers change their passwords.

Although there was support for this initiative, including from various notable and prominent attackers, there was also adamant opposition by other users. As of December 2017, it seems that this initiative has not succeeded.

SOURCES AND FURTHER READINGS REFERENCES

[Honda Shuts Down Car Production Plant Due to WannaCry Infection](#)

[WannaCry Virus Takes Down Traffic Lights and Speed Cameras in Australia](#)

[FirstHealth Network Downtime](#)

[WannaCry: Ransomware attacks show strong links to Lazarus group](#)

MOST SIGNIFICANT ATTACKS IN 2017

Equifax Breach

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

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 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 December 2017, details regarding the content of these documents had not been revealed.

The third database contains records and details of about 209,000 companies, Equifax clients, and 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 and executing fraudulent online transactions, etc.

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

THE ATTACKERS

In light of the fact that none of Equifax's databases have been offered for sale yet on Darknet markets, it is becoming more likely that Chinese nation-state attackers are behind the attack.

Many of the attack tools used were Chinese, and as reported by Bloomberg, inside sources 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 data.

1. First group – conducted preliminary reconnaissance identifying the Equifax servers' vulnerability and executed the initial breach.
2. 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, likely 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 the Darknet for the sum of 600 bitcoins by a previously unknown group that goes by the handle "PastHole Hacking Team". The ultimatum was to pay the ransom by September 15th or the attackers would 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, it was supposedly by the real attackers, who allegedly exposed the entirety of Equifax's website management system, as well as a significant amount of new data regarding the attack that appeared to be genuine.

However, the samples of the supposedly stolen records appeared to be fake. Nevertheless, we cannot rule out that these were the attackers. In order to verify this, attackers were demanding an initial sum of 4 Bitcoins.

BDO can provide additional information regarding means of communication with these actors.

THE INVESTIGATION

In August, Equifax contracted the cybersecurity firm Mandiant to assist in conducting a comprehensive forensic investigation. Mandiant, which is owned by FireEye, has been routinely linked to investigations of nation-state attacks.

POSSIBLE ATTACKER COURSE OF ACTION

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

1. Try to extort Equifax. There was one such fraudulent attempt (likely in order to make an easy profit while humiliating Equifax). Nevertheless, this option is still viable.
2. 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.
3. Use the data to execute various malicious actions from stealing phone numbers and tax frauds.
4. Publicly leak U.S. citizens' data, thus disrupting the capabilities of U.S. government agencies to identify citizens who require services.
5. If a nation-state attacker is indeed behind the attack, 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 U.S. citizens, including governmental and Department of Defense employees.

SOURCES AND FURTHER READINGS REFERENCES

[Equifax Announces Cybersecurity Incident Involving Consumer Information](#)

[The Equifax Hack Has the Hallmarks of State-Sponsored Pros](#)

[How Equifax got Hacked](#)

[Identity Verification Becomes Trickier in Wake of Equifax Breach](#)

[Breaking Down the China Chopper Web Shell - Part I](#)

[CVE-2017-9805](#)

[A Week of Web Application Hacks and Vulnerabilities](#)

[Content-Type: Malicious - New Apache Struts2 0-day Under Attack](#)

[Apache Foundation Refutes Involvement In Equifax Breach](#)

[Equifax](#)

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 sources.
- ▶ **May – July 2017:** Most of the information that was revealed 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.

ATTACK TIMELINE

- ▶ **March 6th:** 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:** Information regarding the vulnerability was posted on the Chinese security website freebuf.com. On the same day, the exploit code was introduced into Metasploit, a popular penetration software.
- ▶ **March 10th:** Hackers scanned the internet for vulnerable computer systems and identified Equifax's Atlanta server.
- ▶ **From this date until late July:** The second group installed over 30 web shells, notably China Chopper, 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 through a critical vulnerability, 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 U.S. to develop Java based web applications.

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

The security firm Contrast Security, was 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 2017, enables attackers to execute HTTP requests to Sturt Apache servers prior to authentication.

According to research, this vulnerability was used to inquire the database in order to exfiltrate data.

This vulnerability seemed much more likely because it is easier to exploit, much better known, and also fit the timeline better. Nevertheless, much is still unknown. The theory that **concurrently to venerability CVE-2017-5638, a Zero-Day-Exploit was used**, cannot be ruled out.

Moreover, Apache stated that it appears that Equifax did not apply patches for flaws discovered in 2017. Note that this Apache platform is also used in products of companies such as Oracle and Cisco. **As such, it should be confirmed that the systems of these companies have been updated with the 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 compromised. However, it appears that this tool is not working properly and provides unreliable results. For example, when it was launched, CNET tried this tool with fake names and SSNs and was told that their records have not been compromised. In other cases, Twitter users have reported the opposite results when inputting false data.
- ▶ Moreover, this tool raised concerns on many security issues. Most notably, it was hosted on the stock WordPress platform, which is a cause for concern when considering the sensitivity of the data that is requested 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 username. 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 phishing.
- ▶ These problems are not limited to this site. It was reported that 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 still may be in.

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

Following the revelation of the breach, Equifax announced 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 point. The old numbers were essentially date-time stamps and could be brute-forced to unlock a credit report for malicious purposes such as identity theft.

In light of these developments, many U.S. citizens opted to enact a security freeze on their accounts. However, Equifax was not adequately prepared, as some consumers reported problems with the system when trying to use it, including crashing.



CLASS ACTION LAWSUIT AGAINST EQUIFAX

Following the attack, many citizens affected by the breach filed class action lawsuit claims against Equifax. 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 losses. If they win the lawsuit, Equifax will have to pay reparations of hundreds of millions and possibly billions of dollars. One of the class action lawsuits is seeking as much as \$70 billion in damages nationally.

OUR INSIGHTS 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 organization and company 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 relatively long time to install security patches. Furthermore, they do not require much effort to identify.

- ▶ 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 breaking down their attack vector. Nevertheless, Equifax apparently was able to almost fully reconstruct every step of the attack. This is due to the fact that prior to the attack, it implemented an open source monitoring tool named “Moloch,” which kept a record of the company's network's internal communications and data traffic.

SOURCES AND FURTHER READINGS REFERENCES

[Moloch](#)



MOST SIGNIFICANT ATTACKS IN 2017

Leak of Nation-state Attack Tools & Documents

NSA LEAKS

Starting in August 2016, a hacker group, Shadowbrokers, began leaking various NSA hacking tools and exploits. In May, the group began offering a paid “monthly dump service.” This is a subscription plan that provides private members with exclusive access to future leaks. This service was originally offered for 100 ZEC (Zcash coins – worth about \$21,000 at the time) per month. However, in June, the price was doubled to 200 ZEC.

Further, they also announced a VIP service for a one-time fee of 400 ZEC that allows members to ask questions about the exploits and data dumps, as well as request specific exploits.

CIA DOCUMENT LEAK VAULT 7 AND VAULT 8

On March 7th, Wikileaks released about 9,000 documents regarding the CIA's cyber operation. This was the first leak before a series of 23, known as Vault 7. This was followed by Vault 8 which is the beginning of another series.

It appears that most of the CIA tools were largely used to spy on specific individuals by directly compromising the targets' devices, rather than wide scale lateral monitoring that is 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 the Vault 7 began, some of the tools' source code has also leaked, and is being used in the wild.

Table 4: Vault 7 and Vault 8 Leaks (By Name and Date)

| NUMBER | DATE | NAME OF LEAK | DETAILS |
|---------|----------|----------------------------|--|
| Part 0 | March 7 | Year Zero | 8,761 documents and files regarding CIA hacking exploits for popular hardware and software. |
| Part 1 | March 23 | Dark Matter | Document leak, including documents regarding CIA attempts to hack Apple Mac computers and iPhones. |
| Part 2 | March 31 | Marble | 676 lines of code for a malware signature obfuscation tool. |
| Part 3 | April 7 | Grasshopper | 27 documents regarding the CIA's malware development platform named "Grasshopper". |
| Part 4 | April 14 | HIVE | 6 documents regarding the CIA malware management system named "HIVE". It appears that this was related also to a threat agent named "Longhorn". |
| Part 5 | 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 6 | April 28 | Scribbles | Documents and source code of a monitoring tool intended to spy on journalists and whistleblowers. |
| Part 7 | May 5 | Archimedes | Documents regarding a virus named Archimedes (a.k.a Fulcrum). |
| Part 8 | May 12 | AfterMidnight and Assassin | AfterMidnight – an espionage malware that imitates DLL files. Assassin – similar to AfterMidnight, but runs within a Windows service process. |
| Part 9 | May 19 | Athena | Documents regarding two malwares – Athena and Hera. |
| Part 10 | June 1 | Pandemic | Documents regarding a malware dissemination tool. |
| Part 11 | June 15 | Cherry Blossom | Documents regarding a hacking tool for wireless networking devices. |
| Part 12 | 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 13 | June 28 | Elsa | Documents regarding a geo-location monitoring malware for WiFi-enabled Windows based devices. |
| Part 14 | June 19 | OutlawCountry | Documents regarding a hacking and data exfiltration tool from Linux based systems. |
| Part 15 | July 6 | BothanSpy | Documents regarding tools (BothanSpy and Gyrfalcon) developed to steal SSH credentials from Windows and Linux based systems. |

| NUMBER | DATE | NAME OF LEAK | DETAILS |
|---------|-------------|----------------|--|
| Part 16 | July 13 | Highrise | Documents regarding a tool named Highrise (a.k.a TideCheck) that intercepts and redirects SMS messages to a remote web server. The tool was developed for Android based devices. |
| Part 17 | 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 18 | July 27 | Imperial | Documents regarding a hacking tool for Apple Mac OS X and various Linux systems. |
| Part 19 | 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 20 | August 10 | CouchPotato | Documents regarding a CIA tool to covertly intercept in real time live video steaming. |
| Part 21 | 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 22 | 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 23 | September 7 | Protego | Documents regarding a guided missile control system that was developed for the CIA by Raytheon. |
| New | September 9 | Vault 8 | The source code of HIVE, the CIA's malware management software. |

Source: BDO Based on Wikileaks

SOURCES AND FURTHER READINGS REFERENCES

[Longhorn: Tools used by cyberespionage group linked to Vault 7](#)

[Raytheon Company](#)

[New leak may show if you were hacked by the NSA](#)

[Shadow Brokers crack open NSA hacking tool cache for world+dog](#)

[The Shadow Brokers Announce Details About Upcoming Monthly Dump Service](#)

[Shadow Brokers Launches 0-Day Exploit Subscriptions for \\$21,000 Per Month](#)

[Shadow Brokers hike prices for stolen NSA exploits, threaten to out ex-Uncle Sam hacker](#)

[Wikileaks - Vault 7: CIA Hacking Tools Revealed](#)



MOST SIGNIFICANT ATTACKS IN 2017

Paradise Papers – leak exposes tax evasions of trillions of dollars

On November 5th (a.k.a Guy Fawkes day), 13.4 million financial documents and records for assets in the sum of \$10 trillion were leaked. The leak was reported by ICIJ (International Consortium of Investigative Journalists), a fully independent organization, comprised of hundreds of investigative journalists 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.

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 (10/20), an anonymous post was shared on the Panama Reddit thread with the headline "Do not give up. More is coming." This implied that a major leak, similar to the Panama Papers was about to go public. The post was signed "Paradise."

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 the Panama Papers in 2016.

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

EXPOSED ENTITIES

The exposed documents detail over 120,000 individuals and organizations from around the world. The list includes past and present heads of states, members of parliament, prominent business people, artists, athletes and major companies.

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 online. Furthermore, all of the heads of states directly involved were exposed. ICIJ has a platform that allows users to review the available documents.

SOURCES AND FURTHER READINGS REFERENCES

On November 5th, 1605, a group of anarchists, headed by an individual named Guy Fawkes, 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

[#OpVendetta Message](#)

[What are the Paradise Papers and who has been named in leaked documents?](#)

[A huge leaking reveals: the plane of Idan Ofer, Jonathan Kolber's businesses - and the tax shelters](#)

[The Paradise Papers: Haaretz Reveals Some of the Israeli Businessmen and Firms Registered in Offshore Tax Havens](#)

[Someone on Reddit hinted at the Paradise Papers 16 days before they were released](#)

[Reddit: Do not give up. More is coming.](#)

[ICIJ Investigation on Paradise Papers](#)

[List of people and organisations named in the Paradise Papers](#)

SIGNIFICANT RANSOMWARE ATTACKS IN 2017

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. D.C. police discovered it when they noticed that four of their camera sites were not functioning properly, and they could not access video from their DVRs.

The investigation further revealed that 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 CTO claimed that their system was designed 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.

Currently, 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 access.

In early March, it was reported that two suspects, a British man and Swedish woman were arrested in London in relations to the attack. In late December, it was reported 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.

SOUTH KOREAN WEB HOSTING FIRM PAYS A RANSOM OF \$1,000,000

The South Korean company, Nayana, paid a \$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 amount.

RANSOMWARE ATTACKS AGAINST HOSPITALS AND HEALTHCARE ORGANIZATIONS

In 2017, we witnessed a significant increase of ransomware attacks against healthcare organizations. Due to the critical nature of hospitals and healthcare providers and the extensive and possibly even immediate damage that can take place if systems are shut down, in many incidents, these organizations are forced to pay the ransom. Below are several notable attacks from 2017.

Ransomware attacks against UK NHS hospitals

UK's National Health Service (NHS) fell victim to several significant attacks over the last year. The most notable was WannaCry. However, this was only the latest of a series of attacks against its hospitals.

In November 2016, they reported that the operation of three hospitals were impacted following a Globe2 ransomware attack. About two months later, on January 13th, 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 unknown.

Initially, it was reported as a ransomware attack, however the trust stated that this was not the case, and that they were infected by a Trojan that had not previously been seen. According to the trust, "while 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 were patient medical records compromised, and medical services for patients were not affected.

Ransomware attack against NHS Lanarkshire Hospitals

On August 18th 2017, several Scottish hospitals, all part of NHS Lanarkshire, were infected by a sophisticated variant of the Bit Paymer ransomware. The attack shut down hospital systems, which were badly hit several months prior during the WannaCry attack. The recent penetration vector was through brute force attacks on exposed RDP endpoints. After gaining access to one of the systems, the attackers laterally moved on the compromised network and manually installed the malware on additional stations.

Currently, there is no way to decrypt files that were encrypted by this ransomware. 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).

Wide-scale 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 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 a ransomware was e-mailed to them alongside a social engineering attack.

According to a hospital spokesperson, there has been no indication that patient medical records were compromised. Following this event, the hospital scaled down its operations 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 to 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 Protenus, 2017 outpaced 2016 in regard to attacks against healthcare providers, with more than 1 breach or ransomware infection per day. During the first half of 2017 alone, 233 breaches were reported to the HHS (US Department of Health & Human Services), with 41% caused by internal factors – either human error, technical error, or malicious action.

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, in 2017, thousands of databases from all sectors were stolen or corrupted in attacks described as “ransacking.” However, only a fraction of those incidents were reported to the HHS.

Many companies and organizations do not report ransom attacks, regardless if the ransom was paid. They do not consider that the attackers may have copied the data with the intent of selling it.

On average, based on the 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 an average of 57 days from the time a breach was detected until it was reported (median – 57). This is a significant improvement from previous years and 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.

Fraudulent ransomware attacks

Citrix Systems exposed a new type of scam dubbed “bluff ransomware attacks.” Attackers utilize various social engineering techniques and other methods to fool companies into thinking that they fell victim to a ransomware attack and must pay a ransom in order to regain access to their databases/systems. According to Citrix System's report, 39% of large businesses in the UK have experienced such an attempt. 61% of them choose to pay the ransom. The average ransom was £13,500. However, 6% of the companies paid over £25,000.

SOURCES AND FURTHER READINGS REFERENCES

[Ransomware attack impacted 70% of Washington DC police surveillance cameras](#)

[DC police surveillance cameras were infected with ransomware before inauguration](#)

[UK arrests 2 suspected in DC police camera hacking](#)

[Two Romanians Charged With Hacking Police CCTV Cameras Before Trump Inauguration](#)

[Web host agrees to pay \\$1m after it's hit by Linux-targeting ransomware](#)

[Trojan malware blamed for cyberattack at Barts Health NHS hospitals](#)

[Bit Paymer Ransomware Hits Scottish Hospitals](#)

[WannaCry victim NHS Lanarkshire hit by new ransomware strain](#)

[ECMC, hit by cyberattack, continues massive task of restoring computer functions](#)

[2017 Breach Barometer Mid Year Review](#)

['Bluff' ransomware attacks cost companies over £13,000 per sham attack](#)

SIGNIFICANT ATTACKS IN 2017

SWIFT- ATTACK AGAINST THE GLOBAL BANKING SYSTEM

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 attackers will use the stolen document in order to execute fraudulent and illegal business transactions.

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

Currently, the identity of the attackers is unknown. In our assessment, this is due to two possibilities. The first is that a large international cybercrime group is behind the attack, which perpetrated the attack in order to carry out trade of prohibited or illegal commodities. The second possibility is that the attacker is a nation-state actor belonging to a country under international embargos and/or sanctions (such as North Korea), which 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 12 months and cross-check them between their core systems and the SWIFT system. In addition to these reports, it was revealed that in June 2016, SWIFT systems of four Indian banks had been attacked. In one of the attacks, the attacker attempted to transfer \$150 million to a bank in the U.S. This wire transfer was denied after the U.S. bank suspected that something was amiss.

THE NORTH KOREAN ACTIVITY AGAINST THE GLOBAL FINANCIAL SECTOR

In early April 2017, Kaspersky Lab and BEA Systems 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 been evident in the past 12 months.

Kaspersky is attributing the group with numerous attacks on the financial sector, including the attacks on Bangladesh Swift system and the attack on Polish banks. The report established 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 waterhole attacks (a.k.a "drive by attacks"). This was evident 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 is that they all used the JBoss application server platform. This suggests that attackers may have had 0-day exploits for this platform. Currently, the group attacked four types of financial organizations:

- ▶ Traditional financial institutions (such as banks)
- ▶ Casinos
- ▶ Financial trade software developers
- ▶ Crypto-currency businesses

The report extensively reviews several attacks against financial institutions, including an incident in a South East Asian country and one against a European financial institution. 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 to SWIFT's security systems following the attack on Bangladesh Central Bank and adapted his tools and methods to overcome them. In some of the cases, it appears 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 through Adobe Flash Player and Microsoft Silverlight exploits. In this incident, the infection was possible due to 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 frequently modifying their code, even without introducing new functionalities. This is done to break Yara recognition and other signature-based detections. The malware is compiled days or even hours prior to the attacks. This indicates a highly targeted method of operation.

In most incidents, the malware did not communicate directly with the C&C servers, but rather connects to another internal host, which relayed TCP connection to the C&C through a tool dubbed "TCP Tunnel Tool". It seems that the attackers operate with high operational alertness. As soon as a company shows sign of an investigation, there is systematic destruction of all evidence of the attack.

HACKERS STOLE \$4.4 MILLION FROM A BANK IN NEPAL BY HACKING ITS SWIFT SERVER

In early November 2017, 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 was transferred. Similarly to other attacks occurring prior to a 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 U.S., and Singapore.

The employees quickly identified the suspicious transactions and promptly alerted the Central Bank of Nepal, which was able to retrieve \$3.9 million. Currently, the forensic investigation is still being conducted.

No additional information has been released.

HACKERS ATTEMPTED TO STEAL \$1,000,000 FROM A RUSSIAN STATE BANK

In late December 2017, it was reported 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). They only succeeded in getting about 10% of that (about \$95,000).



\$60 MILLION STOLEN FROM FAR EASTERN TAIWANESE BANK THROUGH THE SWIFT

Following a relatively long hiatus, in early October 2017, \$60 million was stolen via a SWIFT transaction from the Taiwanese bank Far Eastern. According to reports, the attackers transferred the funds to banks in Sri Lanka, Cambodia, and the U.S. The attacker exploited the SWIFT system through a custom piece of 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. According to recent reports another suspect remains at large. Below is an overview of what is currently known:

- ▶ **The attacked bank** – A medium size Taiwanese bank (2,300 employees) Far Eastern International. 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 October 3rd, 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. The approximate date of the transactions was October 5th.
- ▶ **What are the compromised accounts, and where was the money transferred 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.
- ▶ **The bank's control mechanisms and security systems - capability to retrieve the funds** – It appears that the bank's control mechanism 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 October 12th, SWIFT issued an alert containing technical indicators. It was classified as TLP Amber.

BEC ATTACKS IN 2017

Over the last year, BEC scams (a.k.a chairman frauds, a.k.a EAC scams) have grown more prevalent and sophisticated. In these scams, the attacker impersonates an executive at the company and uses e-mail to request a wire transfer. According to the FBI report 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, most commonly to banks located in China, Hong Kong, and the UK.

COMMON BEC SCENARIOS

Below is IC3's description of the four 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 C-level business executives 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."

On July 20th, Dutch police announced that they are shutting down Hansa after they 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 Germany.

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 ran 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 Tor.

Scenario 3: 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 4: Data Theft

Fraudulent requests are sent using 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 department, 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.

DESTRUCTIVE MALWARE ATTACKS AGAINST SAUDI ARABIA

Between late 2016 and early 2017, the Shamoon 2.0 campaign was comprised of three destructive waves of attacks against multiple organizations in Saudi Arabia. In January, PaloAlto exposed new information regarding a wave of Shamoon attacks (planned for 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 this malware had the capability to nullify 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 were taken from 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. 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 the attacker likely executed a previous attack in order to obtain these account credentials.

In March, Kaspersky Lab revealed that in the attacks two different destructive malware were used:

1. 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.
2. 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 (a.k.a Newscaster, NewsBeef, and Ajax Team). Currently, 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 in addition to 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 report 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.

We identified an overlap between the indicators in the report and those from the destructive attacks against Saudi Arabia, taking 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. PaloAlto discovered that the attackers exploited a compromised RDP system (Remote Desktop Protocol) to distribute the Disttrack across the network. Furthermore, 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 the 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 that the attackers obtained access to the targeted networks prior to Shamoon 2.0 attacks.

Moreover, when gathering files attributed to the third wave of Shamoon 2.0 attacks, PaloAlto identified a zip archive that contained files used to infect other systems. It did this 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 the Shamoon 2.0 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 2.0, 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.

SOURCES AND FURTHER READINGS REFERENCES

[From Shamoon to StoneDrill - Wipers attacking Saudi organizations and beyond](#)

[From Shamoon to StoneDrill - Wipers attacking Saudi organizations and beyond / Version 1.05](#)

[BfV Cyber-Brief No. 04/2016](#)

[Shamoon 2: Delivering Disttrack](#)

DARKNET MARKET ACTIVITY DURING 2017

LEADING DARKNET MARKETS TAKEN DOWN BY LAW ENFORCEMENT

In early July 2017, Alphabay, the largest Darknet market was unexpectedly shutdown with no explanation. Initially it was suspected that the individuals behind the market stole money from vendors and buyers.

However, it was later revealed that the site's administrator, a 25-year-old Canadian citizen named Alexandre Cazes, was arrested in Thailand and indicted with trafficking drugs, guns, counterfeit goods, and hacking tools, amongst other items.

According to the Europol, it is estimated that Alphabay generated over a billion dollars in its three years of operation.

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, investigation revealed that Cazes used the same handle in various forums, including his private blog where he stated his full name.

The authorities confiscated over \$8 million in various cryptocurrencies and numerous other assets, such as houses and luxury cars listed under both his name and his wife's. A week after his arrest, Cazes took his life by hanging himself in a Thai prison.

Following Alphabay's shutdown, which at its peak, was ten times larger than the now defunct Silk Road Market, over 200,000 users and 40,000 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. This included the new wave of users that followed Alphabay's shutdown.

On July 20th, Dutch police announced a shutdown of Hansa, after it documented and gathered data on tens of thousands of users.

Additionally, the data was transferred to Europol for further investigation jointly with the FBI and DEA. Concurrently, authorities seized the site's servers in Lithuania, the Netherlands, and Germany.

Law enforcement 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 do not activate the 2FA (Two Factor Authentication) function. Moreover, it is reported that during the time Dutch authorities ran 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 Tor.

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 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 transactions.

Others suspected that the site was taken down by law enforcement agencies, in a similar fashion to months prior, when "Alphabay" and "Hansa market" were taken down following a large scale international operation. However, several hours later, the site came back and is still operational. Therefore, this does not seem likely.

Once the site came back, some users discovered that their bitcoin wallets were empty. The site's operators acknowledged the incident, stating that they are working to recover the corrupted data, however they did not say if and how affected users will be compensated. Below is their response to the incident:

"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, Russian authorities announced that they 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. It was taken down in July but was not made public. Initially, many users believed the website was having hosting issues or under a DDoS attack.

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 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 2017, multiple major Darknet markets began shutting-down without any explanation. Early on, some Reddit users claimed to have intermittent access to a number of the markets. However, it became apparent that all four of the largest markets - Dream Market, Trade Route, Tochka, and Wall Street, were completely unavailable.

Currently, it is unclear whether this occurred due to DDoS attacks or law enforcement agencies operations similarly to the Alphabay and Hansa takedown.

At the time, there were numerous reports of mirror sites for some of the markets, but many were fraudulent. 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. Initially, many believed that the markets were shut down by authorities; currently, this seems less likely. Although unlikely, it 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, currently these assumptions have not been officially corroborated.

SOURCES AND FURTHER READINGS REFERENCES

[Alphabay shutdown: Bad boys, bad boys, what you gonna do? Not use your Hotmail...](#)

[Global Police Spring a Trap on Thousands of Dark Web Users](#)

[Suspected Alphabay founder dies in Bangkok jail after shutdown of online black market](#)

[Dark web marketplaces Alphabay and Hansa shut down](#)

[Crooks Reused Passwords on the Dark Web, so Dutch Police Hijacked Their Accounts](#)

[Users Freak Out After Dark Web Market Goes Down And Funds Go Missing](#)

[Reddit DarkNetMarkets](#)

[Top Darknet Markets Go Offline](#)



OTHER NOTABLE ATTACKS IN 2017

CRYPTOCURRENCY PLATFORM ENIGMA COMPROMISED; OVER \$500,000 IN ETHEREUM STOLEN FROM USERS

On August 20th, a hacker gained control of the popular cryptocurrency platform Enigma and conned users from over half a million dollars 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 Offering).

Currently, 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 in July 2015. The attacker identified that Zyskind reused his Ashley Madison username and password with his email and had not changed them since the leak.

Once the attacker had access to Zyskind's email he had admin credentials to Enigma, which he used to send messages to the users, 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 platforms. In just the last couple of months over \$48 million in Ethereum currency was stolen in four different incidents.

RUSSIAN APT DRAGONFLY ATTACKS TARGETING CRITICAL INFRASTRUCTURE SECTORS

On October 20th, the US-CERT issued a public alert regarding a wave of attacks that began at least five months prior. Referred to as APT Dragonfly (a.k.a Energetic Bear), the attacks targeted government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors. The alert is based on various sources, notably Symantec report from September 6th 2017.

Exploitation of the supply chain.

In initial attacks, attackers targeted peripheral organizations, such as trusted third-party suppliers with less secure networks and gathered intelligence via open-source reconnaissance.

Spear-phishing emails and malicious documents.

Attackers sent malicious documents through targeted phishing emails. However, these documents do not exploit a vulnerability nor do they contain a malicious macro. They leverage legitimate office features in order to retrieve the content from a remote server.

The malicious documents contain links that automatically load 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 attacker uses password-cracking techniques to obtain the plaintext password. Once valid credentials are obtained, they are used to impersonate authorized users.

Waterhole attack.

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

Penetration and installation.

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 was automatically installed through 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

In August 2017, Kaspersky Lab published a report exposing a presumably Chinese APT (identified in July) that targets various organizations through 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 obscured by several layers of encrypted code, and thus could only be triggered by a specially crafted DNS TXT record sent from the attackers' C&C 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 C&C 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. Further, it is used by many critical infrastructure companies. NetSarang has issued an official statement on the matter, in which it confirmed Kaspersky's findings. Note that a "clean" software update that supposedly removes the malicious update does not guarantee that an attack is neutralized. If the attackers executed the attack, they may have pivoted to another software/firmware component within the compromised system.

DATA FROM SWEDEN'S TRANSPORT AGENCY EXPOSED

In late July 2017, it was reported that the Swedish Transport Agency (STA) outsourced maintenance and operation of its databases and networks to IBM two years prior in effort to migrate their databases to cloud storage. IBM, in turn, used subcontractors from the Czech Republic and Romania, providing access to the full dataset from the Transport Authority.

This dataset, however, included information such as 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 investigating in 2016. The investigation resulted in firing of STA's director-general Maria Ågren in January 2017.

OUTLOOK WEB ACCESS BASED ATTACKS, MAINLY IN OFFICE 365 ENVIRONMENT

In 2017, 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 OWA. The best method to mitigate these types of attacks is by enabling Multifactor Authentication and requiring users to use strong passwords.

SOURCES AND FURTHER READINGS REFERENCES

[Sweden exposed sensitive data on citizens, military personnel](#)

[Sweden Accidentally Leaks Personal Details of Nearly All Citizens](#)

[Outlook Web Access based attacks](#)

[Deloitte hit by cyber-attack revealing clients' secret emails](#)

[Hacker Nets over \\$500,000 after Hacking Enigma before ICO Date](#)

[Enigma platform hacked, hackers stole over \\$470,000 worth of Ethereum](#)

[Hacker Steals \\$8.4 Million in Ethereum \(4th Heist In A Month\)](#)

[Hackers Stole \\$32 Million in Ethereum; 3rd Heist in 20 Days](#)

[Hacker Uses A Simple Trick to Steal \\$7 Million Worth of Ethereum Within 3 Minutes](#)

[Largest Cryptocurrency Exchange Hacked! Over \\$1 Million Worth Bitcoin and Ether Stolen](#)

[Alert \(TA17-293A\) - Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors](#)

[Dragonfly: Western energy sector targeted by sophisticated attack group](#)

[ShadowPad in corporate networks](#)

[Security Exploit in July 18, 2017 Build](#)

Timeline of Major Events



Table 5.1: Cyber Events, Targets and Attack Vectors by Month 2017 (January)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|--------------------------------|----------------|------------------------------|--|
| German Bundeswehr (armed forces) | Targeted attack | Germany | Military and Defence | The computer systems of the German army was rapidly attacked hundreds of thousands of time for 9 weeks in early 2017. |
| SWIFT | Targeted attack | India | Financial Industry | 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 operations. |
| 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. |
| 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. |
| 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. |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|----------------|---------|-----------------------------------|---|
| 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 was 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 | 11,000 patient records were compromised. |
| Emory Brain Health Center | Ransomware | USA | Healthcare | The Ransomware encrypted a MongoDB database that was misconfigured – contained documents of over 90,000 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. |
| Polish Foreign Ministry | Malware | Poland | Government | Attributed to APT28 (a.k.a Fancy Bear) |
| India National Defense Academy (NDA) and National Investigation Agency (NIA) | Malware | India | Government – 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 30,000 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. |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|-----------------------------------|------------------|--------------------------------|---|
| Netflix | Phishing | USA | Entertainment | Sophisticated phishing attack against U.S. Netflix users – credentials and credit card details were stolen. |
| Dr. Web /Emsisoft | DDoS | Russia / Austria | Cybersecurity | The attacks were executed as revenge against the firms' investigation of criminal activity. |
| Lloyds Banking Group | DDoS | UK | Financial Industry | The attack lasted two days and a £100,000 ransom was demanded. |
| fbi.gov | Hacking - Plone CMS Vulnerability | USA | Government | Private records and documents 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 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 5,000 patients. |
| Several Chinese Internet Giants | N/A | China | Internet | Over a billion accounts of various online Chinese services sold on Darknet market. |

Source: BDO Based on various open sources



Table 5.2: Cyber Events, Targets and Attack Vectors by Month 2017 (February)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|-----------------|------------------|------------------------|--|
| Norwegian Labour Party | Targeted attack | Norway | Government | Executed by APT29 – 9 email accounts of members of the Labor party were hacked. |
| 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. |
| Taiwanese Ministry of Foreign Affairs' Bureau of Consular Affairs (BOCA) | Hacking | Taiwan | Government | Over 15,000 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. |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|----------------|---------|--------------------|---|
| 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 | Government | Hackers stole sensitive records of 7,500 citizens. |
| City of Troy | Ransomware | USA | Government | |
| Tiverton Town Council | Ransomware | UK | Government | |
| InterContinental Hotels Group | Ransomware | USA | Hotels | Affected 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 Industry | 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 Industry | 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 Industry | 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 80,000 credentials of the organization's website. |

Source: BDO Based on various open sources

Table 5.3: Cyber Events, Targets and Attack Vectors by Month 2017 (March)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|----------------|-----------------|--------------------|---|
| NSA/WikiLeaks - Vault 7 | Data leak | USA | Government | Executed by TheShadowBrokers – 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 Industry | |
| 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 19,000 citizens. |
| Two un-named U.S. Tech Companies | Phishing - BEC | USA | Tech industry | A Latvian citizen conned two unnamed American Tech companies for over \$100 million. |
| Defense Point Security, LLC | Phishing - BEC | USA | Defence | Spear-phishing attack – employee tax forms were stolen. |
| Alfa Bank | DDoS | Russia | Financial Industry | Widescale DNS botnet attack. |
| Undisclosed U.S. 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 95,000 applicants. |
| Major U.S. Universities | N/A | USA | Academia | 14 million email addresses with passwords of major U.S. universities were sold on the Darknet. |

Source: BDO Based on various open sources

Table 5.4: Cyber Events, Targets and Attack Vectors by Month 2017 (April)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|---|-------------|-----------------------------------|--|
| SWIFT – ongoing campaign against the global financial sector | Targeted and ongoing hacking campaign | Global | Financial Industry | 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 | Speread and sophisticated attack against users of governmental systems and services. |
| IAAF | Targeted attack | Global | Sports | Executed by APT28 (a.k.a 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 personnel were hacked. The attack is attributed to APT28 (a.k.a 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 25,000 photos, some of which were nude pictures of patients. Sold on the Darknet for 300 Bitcoin. |
| Northrop Grumman | Hacking | USA | Government – Military and Defence | Employees' tax forms were stolen. |
| WannaCry | Ransomware/Wiper malware | Global | | Unprecedented widescale malware attack. |
| ABCD Paediatrics | Ransomware | USA | Healthcare | |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|-----------------------------------|----------------|-------------|--------------------------------|---|
| 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 a \$37,000 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 Industry | Trickbot banking malware. Escalation of attacks against UK banks. In April alone, five 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 Industry | 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. |
| Melbourne IT | DDoS | Australia | Telecommunication | The attack disabled the ISP's services. |
| Yapizon | N/A | South Korea | Cryptocurrency exchange market | 3,816 Bitcoins were stolen (worth about 10 million USD 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. |

Table 5.5: Cyber Events, Targets and Attack Vectors by Month 2017 (May)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|---|---------------------|-------------|---------------------------|---|
| 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 three 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 – \$1 million was paid. |
| St. Mark's Surgery Center | Ransomware | USA | Industry - Healthcare | Compromised medical records of 33,877 patients. The attack took place between April 13-17 however the center only detected it on May 8th. |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|---|-----------------------------|------------|-----------------------|--|
| 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. |
| Southern Oregon University | Phishing - BEC | USA | Academia | Over \$1.9 million was stolen. |
| Gannett Co. | Phishing - BEC | USA | Entertainment | Compromised 18,000 employee records. |
| Bank of France | Phishing - BEC | France | Financial | Phishing campaign impersonating the bank. |
| UC Davis Health | Phishing / BEC | USA | Industry - Healthcare | Via email phishing attack the attacker compromised various systems and records of about 15,000 patients. Leveraged the data to execute BEC attacks. |
| FCC (Federal Communications Commission) | DDoS | USA | Government | Disrupted the agency's normal operation. |
| Molina Healthcare | Security Flaw | USA | Industry - Healthcare | Security vulnerability exposed sensitive patients' data – it is unknown how long the systems were compromised. |

Source: BDO Based on various open sources



Table 5.6: Cyber Events, Targets and Attack Vectors by Month 2017 (June)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|------------------------|---------|----------------|---|
| 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 U.S. East Coast | Hacking | USA | Infrastructure | A former employee hacked and sabotaged the IT systems of six water supply stations. |
| Unprotected DB of 198 million U.S. voters | Data leak | USA | Government | Unprotected DB of 198 million U.S. 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. |



| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|------------|-------------|----------------------------|---|
| 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 its 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 July. |
| Seven South Korean banks | DDoS/RDoS | South Korea | Financial | The banks were extorted by the group Armada Collective. \$315,000 was demanded. |
| Microsoft Skype | DDoS | Global | Software and communication | The attacks disrupted Skype services. |
| Ohio government websites | Defacement | USA | Government | Pro ISIS hackers by the handle Team System DZ defaced the state's government sites. |
| UK Parliament | N/A | UK | Government | The attack prevented access to email accounts of about 90 members of Parliament. |

Table 5.7: Cyber Events, Targets and Attack Vectors by Month 2017 (July)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|---|-----------------|-------------|---------------|---|
| CoinDash | Hacking | Global | Financial | \$7 million worth of Ethereum was stolen. |
| Parity | Hacking | Global | Financial | \$32 million worth of Ethereum was 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. |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|-------------------------------|------------|---------|-------------------------------|--|
| 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. |
| 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 | Industry – internet/financial | \$8.5 million worth of Ethereum coins were stolen. |
| Unnamed Canadian Organization | Ransomware | Canada | N/A | A ransom of \$425,000 in Bitcoin was paid. Reported by the cybersecurity 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. |

Source: BDO Based on various open sources

Table 5.8: Cyber Events, Targets and Attack Vectors by Month 2017 (August)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|---------------------------------|-----------------------------|----------|-------------------------|--|
| Loopia | Hacking | Sweden | Internet | The web hosting's entire client database was leaked. |
| 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. |
| Tettegouche 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. |

Source: BDO Based on various open sources

Table 5.9: Cyber Events, Targets and Attack Vectors by Month 2017 (September)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|--|----------------------------|--------------------|--|
| Equifax | Targeted attack – vulnerability exploitation | USA | Financial Industry | One of the largest credit rating companies in the world. The attackers stole personal and financial data of over 140 million U.S., UK and Canadian citizens |
| Multiple U.S. 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 (a.k.a 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 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 Industry | 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. |
| 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. |

Table 5.10: Cyber Events, Targets and Attack Vectors by Month 2017 (October)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|---|------------|---------------------|--|--|
| 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 world 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 in 2016 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. |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|---|------------|---------|--|--|
| 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 secret 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. |
| The Far Eastern International Bank | Malware | Taiwan | Financial Industry | \$60 million was stolen after the attackers installed a malware within the bank's servers, enabling them to exploit the SWIFT system. |
| Japanese banks | Malware | Japan | Financial Industry | 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 did not disclose if any sensitive info was compromised. |
| Myethereumwallet.com | Phishing | Global | Financial Industry | Over \$15,000 worth of crypto coins were stolen. |

Source: BDO Based on various open sources

Table 5.11: Cyber Events, Targets and Attack Vectors by Month 2017 (November)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|----------------------|---------|--------------------|--|
| Swedish radio station RadioPlay - MixMegapol | Hacking | Sweden | Entertainment | The attacker hacked the station's systems and broadcast pro-ISIS songs for 30 minutes. |
| Tether | Hacking | Global | Financial Industry | \$31 million 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. |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|--|------------|---------|--------------------|---|
| NIC Asia Bank | Hacking | Nepal | Financial Industry | \$4.5 million was stolen. |
| Companies and organizations in Germany | Ransomware | Germany | Multiple sectors | Ordinypt Ransomware is sent to numerous companies via phishing emails impersonating Curriculum Viaes. |
| 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 | |
| The City of Spring Hill, Tennessee | Ransomware | USA | Government | Infected after an employee opened a malicious email. \$250,000 was 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. |

Source: BDO Based on various open sources

Table 5.12: Cyber Events, Targets and Attack Vectors by Month 2017 (December)

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|------------------------------------|---------------|-----------------|--------------------|--|
| 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 Industry | The attackers attempted to steal \$10 million, but achieved only \$95,000. |
| 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 Industry | Crypto-Mining Marketplace - 4,736.42 Bitcoins were stolen (worth about \$65 million). |
| Osaka University | Hacking | Japan | Academia | Personal info of 80,000 students and staff may have been compromised. |
| Fox-IT | DNS Hijacking | The Netherlands | Cybersecurity | |
| 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 | Government | 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 if the organization attempted to restore its systems. |

| TARGET | VECTOR | COUNTRY | SECTOR | COMMENTS |
|---------------------------|----------------|-----------|--------------------|---|
| John Kahlbetzer | Phishing - BEC | Australia | Individual person | Richest man in Australia – lost \$1 million in a BEC scam. |
| Baptist Health Louisville | Phishing | USA | Healthcare | An employee's email account was compromised and was used to send phishing emails. |
| Warwick University | DDoS | UK | Academia | |
| Bitfinex | DDoS | Global | Financial Industry | The Cryptocurrency market place was forced to shut down operation following a series of continuous attacks. |

Source: BDO Based on various open sources



About BDO Cyber Threat Insights

Our Cyber Threat Insights [CTI] reports service is based on an array of tools that optimize the ongoing intelligence information collection and analysis, to create an effective and reliable intelligence picture.

Our Cyber Threat Insights [CTI] as-a-service leverages our methodologies and staff skills to create an effective and reliable intelligence picture that would identify intelligence leads as required and allow cyber intelligence specialists to follow those leads. This can be built on our expert reporting on any applicable and actionable conclusions or in support of your analysts.

INTELLIGENCE SOURCES

- ▶ Monitoring Domain and DNS databases.
- ▶ VirusTotal intelligence.
- ▶ Using BDO internal databases, search engines.
- ▶ Peer connections around the world.
- ▶ Monitoring main leak websites.
- ▶ Monitoring honeypot networks.
- ▶ Monitoring of Facebook groups and pages, Twitter feeds and other social networks.
- ▶ Monitoring password protected and open discussion groups of various communities, such as Russian groups; Islamic groups; Chinese groups; and case septic.
- ▶ Monitoring of open discussion groups of the same communities.
- ▶ Monitoring of sinkholes to Command & Control bot networks.
- ▶ Virtual identities operations.
- ▶ Worldwide Computer Emergency Readiness Teams (CERT) notifications.
- ▶ Hundreds of blogs and websites authored by leading researchers, security companies, and other cyber security information resources.
- ▶ Shareable information accumulated from our client-base, partners and ongoing analysis.

CYBER THREAT INSIGHTS REPORTING

Bronze Package - Global

- ▶ A monthly cyber intelligence report focused on the most important, Cybersecurity events and incidents.
- ▶ Breaking News: an ad-hoc email notification on new information related to the Global Cybersecurity News.
- ▶ Those breaking news will be included in the following monthly Global Cybersecurity News.
- ▶ Monthly Cybersecurity Webex on the most important news and events and time for Q&A.

Silver Package – Sector Specific

- ▶ A bi-monthly cyber intelligence report on news & intelligence related to the client's sector.
- ▶ Analysis & recommendations on mitigating cyber incidents.
- ▶ Alerts on known hactivists Ops related to the client's sector / region.
- ▶ Research on cyber-attacks and their effects.
- ▶ Technical research on new vulnerabilities.
- ▶ Analysis of new malware.
- ▶ The sectors already in coverage are: financial, critical infrastructure, health, government.
- ▶ Quarterly Cybersecurity discussion on the most important news and events and time for Q&A.

Gold Package – Customized 24/7 Alerting

- ▶ 24/7 alerts of immediate threats of the client organization. In urgent cases, can be accompanied by phone/SMS notification.
- ▶ Alerts on leaked information related to the client and his related parties (clients, known suppliers, etc.).
 - Alerts on fake domains and domains similar to the client's known domains.
 - Alerts on phishing attempts.
 - Social media research of planned attacks against the client.
 - Stolen/leaked client information.
- ▶ Feed of Technical Indicators (IoC's) based on MISP open platform/
- ▶ Supply of malware sample per client request, and analysis of malware on demand/
- ▶ Assist the client investigating Malware source, attribution of attack, IP history, and other cyber-attack research and analysis.
- ▶ DarkNet Alerts: On leaked information change hands; hacking tools sold; hacking services sold with relation to the client.
- ▶ A bi-weekly cyber intelligence report and special alerts related to the client.

Platinum Package – 24/7 Analyst Support / Gold service +

- ▶ Cybersecurity Intelligence 24/7 support services.
- ▶ High-level cyber expert research and forensic services to help the customer mitigate attacks in real time (Up to 15 hours per month, remotely).
- ▶ Prepare high level presentation of cyber events, for the company management or board.
- ▶ Annual cyber crisis tabletop exercise.

DELIVERING INSIGHT AND FORESIGHT

BDO has developed a cyber intelligence capability, built upon:

Dedicated Infrastructure

Through the use of anonymous infrastructure that allows the operating team to act without revealing their identity, our organization or any technical indicators. Our team can approach suspicious identities that might be involved in malicious attempts against your organization.



Online Fictitious Identities (Avatars)

The cyber intelligence team maintains online fictitious identities to enable their activity within the threat communities, to infiltrate an online forum, or to contact real suspected attackers or hackers. In order to establish 'safe' conversations, BDO can establish online 'chatter' platforms.



Monitoring Cybercrime Forums

The cyber intelligence team monitors specific cybercrime forums to identify premeditated attacks on the organizational network or personnel by monitoring any type of hostile chatter regarding the organization.



Monitoring Relevant Social Platforms

BDO monitors relevant social platforms to identify any type of chatter that might identify an organization's lost or leaked data being discussed or traded. The monitoring of social platforms can be targeted to pinpoint suspected individuals inside or outside an organization.



Monitoring Data Leakage Platforms

Our team can trawl hacker-oriented data leakage platforms to identify data leakage that may lead to a potential attack against an organization.





BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 550 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 73,800 people working out of 1,500 offices across 162 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

© 2018 BDO USA, LLP. All rights reserved.