
CYLANCE
2017
THREAT
REPORT

CONTENTS

EXECUTIVE SUMMARY

The cyberattacks of 2017 proved more numerous, sophisticated, and ruthless than in years past. Threat actors, armed with knowledge stolen from the CIA and tools lifted from the NSA, demonstrated an elevated level of proficiency. WannaCry and NotPetya, two prominent threats from last year, successfully exploited these stolen assets in their assault on systems worldwide.

As 2017 progressed, new opportunities developed in ransomware-as-a-service (RaaS), opening the gates of malware-for-profit to everyone. Advancements in fileless attacks provided new ways for threats to hide from once reliable detection methods. Malware features such as polymorphism continued to play a powerful role in evading traditional defenses.

The victims of cybercrime ranged from private businesses to the fundamental practices of democracy. France and the United States saw significant data breaches during their recent presidential elections. Several high-profile companies lost their customers' personally identifiable information to cyberattacks, blemishing their brands and costing them untold millions in recovery operations.

This report contains an overview of the threat trends and malware families Cylance's customers faced in 2017. This information is shared with the goal of assisting security practitioners, researchers, and individuals in our collective battle against emerging and evolving cyberthreats.

METHODOLOGY

Cylance® provides security solutions that are focused on protecting endpoints and servers from being compromised by malware, malicious scripts, fileless attacks, and other advanced threats. Through a lightweight endpoint agent and encrypted communication channels, when a threat is detected information about the event, including telemetry data, is transmitted to the customers' private tenant in the Cylance cloud. This report is based in large part on this anonymized threat data collected between January 1, 2016 and December 31, 2017.

2017 THREAT ANALYSIS KEY FINDINGS

- On average, Cylance prevented 3,918 attacks per enterprise in the year 2017, representing an increase of nearly 13.4% over last year
- Within our customer base, the food and hospitality industries suffered the highest volume of attacks
- Ransomware attacks grew threefold during 2017, affecting all verticals, but impacting healthcare the most
- The top two infection vectors remained email and drive-by downloads
- System damage and data destruction represented top risks from threats executing within an enterprise environment

CYLANCE THREAT REPORT

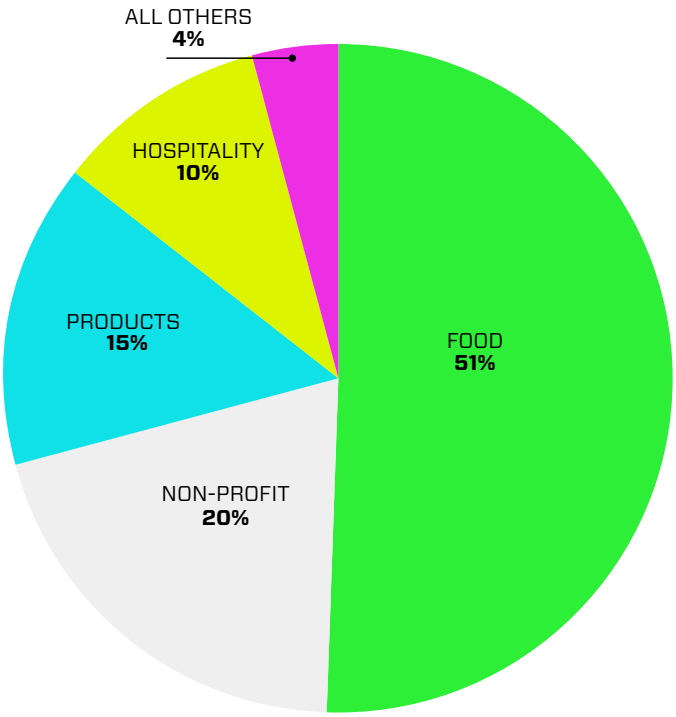
OVERVIEW

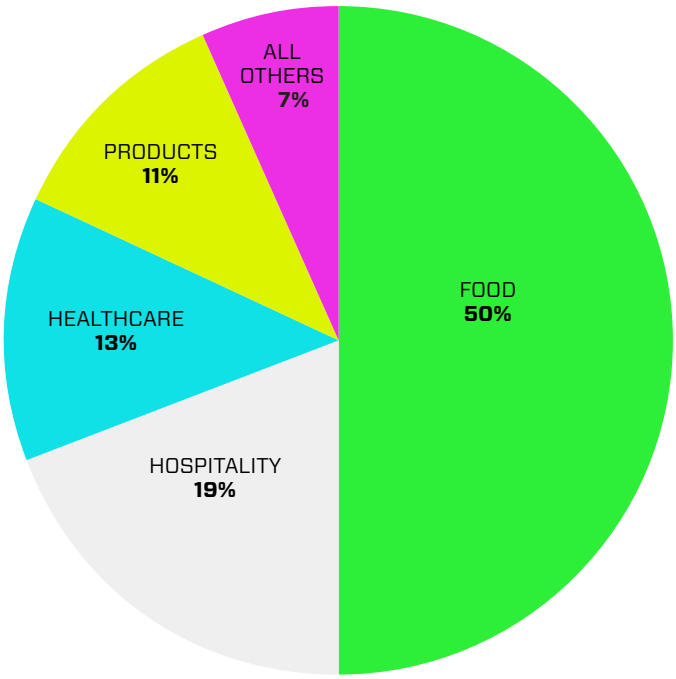
OVERVIEW

As with previous years, we observed an increase in overall threat activity across our customer base. With commoditized malware, malicious scripts, and new attack delivery methods available, it is now easier than ever before for anyone with minimal attacker skills to initiate targeted attacks.

In 2017, Cylance prevented over **3,900** unique attacks per enterprise worldwide across more than 160 countries. This was a growth of about **13.4%** in the amount of attacks seen within the Cylance ecosystem as compared to 2016.

Additionally, we observed that in 2017, the food industry was hit the hardest with different types of malware, followed by the hospitality industry. **These results are averaged out per industry to reduce bias around the Cylance ecosystem.** The food industry was also the hardest hit by malware attacks in 2016, followed that year by non-profit organizations.





MALWARE 2016

IMPACTED INDUSTRIES

Food	51%
Non-Profit	20%
Products	15%
Hospitality	10%
All Others	4%

MALWARE 2017

IMPACTED INDUSTRIES

Food	50%
Hospitality	19%
Healthcare	13%
Products	11%
All Others	7%

THE RISE OF SINGLE USE, HIGHLY-TARGETED MALWARE

Part of the exponential growth of malware, and the bulk of the attacks on various industries, can be attributed to the continued rise in polymorphic and single-use malware. Within the Cylance customer community, more than 70% of the threats blocked were never seen by anyone other than Cylance. In the next section, we discuss what we call The Big Ten, which are the families of malware that are generally used in opportunistic attacks and exemplify this trend.

There is a general misconception that publicly-available repositories of malware signatures are a complete catalog of in-the-wild malware. This misguided perception is further elevated by thin endpoint controls that rely on looking up hashes or validating binaries against these public sources to determine if a file is a threat. The fact of the matter is that public repositories of signatures are by no means comprehensive, complete, up-to-date, or a reliable record of all the malware that could impact an organization. This is somewhat analogous to Common Vulnerabilities and Exposures (CVE)[1].

CVE is the closest thing we have to a full standard of cataloging and documenting software and hardware vulnerabilities. Arguably, it does this very well. However, it would be inaccurate to say it is complete or covers all software and hardware vulnerabilities. CVE assignments often take time as well, meaning post-disclosure, there may be a few days or longer before a CVE is assigned to a flaw. Likewise, one should not assume that a flaw is not dangerous if there is no assigned CVE. Similarly, malware not found in public repositories is still dangerous malware. **One must also take into account that malicious actors do not want their creations to end up on public malware lists (or otherwise in-the-wild) and frequently take specific steps to ensure that does not occur**. If you are a malicious actor, and your binaries end up in a public repository, you are caught, and you must react/pivot/abort any related activities.

Attackers often use single-use or host/campaign-specific binaries to remain hidden and prolong persistence. We have seen variations on this approach in the last couple of years with the Project Sauron and Poseidon targeted attacks, as well as others. Tightly controlling where malicious files in a target environment exist, and managing it with great regularity, ensures that weak security controls that rely on public hash/checksums/IOC lookups will never trigger. Successful malicious campaigns often remain hidden or dwell for months or even years before components become known. Even at that point, it is often only by a stroke of luck that a file gets uploaded to a public repository, starting the chain of events where it is picked up by other analysts, pivoted upon, and exposed for what it is. It is also well known that attackers take steps to complicate/inhibit analysis of their creations if they are discovered. Techniques to defeat virtual machines (VM), hard-coded time constraints, and host/environment-specific logic all aid in obfuscation and complication of analysis.

It is critical to point out that this single-use/avoid-leakage-to-the-wild approach does not only apply to ultra-sophisticated targeted attacks. We observe this with everyday commodity malware as well. This includes ransomware with host-specific keys, and execution and general remote access trojans, other trojans, etc. Some of these evasion techniques are even built into cheap/free packers and crypters.

Bottom line, you can't rely on a public repository as a source for all that is evil. **The most worrisome malware, from the high-level commodity code to the ultra-sophisticated targeted attacks, will never show up there**.

> "THE FACT OF THE MATTER IS THAT PUBLIC REPOSITORIES OF SIGNATURES ARE BY NO MEANS COMPREHENSIVE, COMPLETE, UP-TO-DATE, OR A RELIABLE RECORD OF ALL THE MALWARE THAT COULD IMPACT AN ORGANIZATION."

THE NTH DAY EXPLOIT

In addition to the increase in amount of attacks, traditional attack vectors like exploits remain popular. Attackers continue to make use of known vulnerabilities to attempt to exploit organizations. **In fact, many of the attacks we saw in 2017 were initiated by exploiting vulnerabilities that were reported more than nine months before the attack was detected and blocked**. This practice was highly visible in some of the larger, targeted campaigns discussed in the media. For example, the Patchwork and Confucius campaigns, even in the latter stages of activity, dipped into 2015 and 2016 vulnerabilities[1] , which were a year old (or older) at the time.

On a wider scale, use of older vulnerabilities has become very popular for coin-mining malware. Any vulnerability that allows full access to publicly-exposed servers (ex: web servers) is fair game. For example, in Q1 2018, there was a noticeable uptick in the use of CVE-2017-10271 for gaining access to webservers. This is just one example of a flaw (Oracle WebLogic) that allows for quick and reliable access when malicious actors need to deposit and execute their wares. Even after exploit and proof-of-concept code for this vulnerability became more well-known at the end of 2017 to early 2018, it was still being successfully used. In continuing with this trend, combining the coin miners with EternalBlue resulted in a highly spreadable and potentially profitable combination. The SMB flaws, which are still utilized heavily as of Q1 2018 and are described in CVE-2017-0144 (and related), were patched in March 2017.

Securing systems across the enterprise is already a daunting task for IT admins due to fractured technological landscapes where some devices are on-site, some are remote, and some rarely connect to infrastructure at all. Securing these systems becomes even more challenging and costly when threats slip in through the cracks due to missed patches or just win by numbers by bombarding with rapidly changing one-time-use polymorphic threats. This situation has given rise to the desire by many organizations to look for ways to mitigate attacks leveraging known vulnerability attacks, such as solutions that can detect and block zero-day payloads without a continuous connection to the cloud or requiring continuous detection signature and rule updates.

NotPetya and WannaCry's rapid movement exemplified the concerns of patch management as well as polymorphic threats, and was a wakeup call for organizations across the globe. These attacks, which we will discuss in detail later in this report, prompted many organizations to reassess their security strategy, again looking for new ways to deal with fast-moving threats. While Microsoft has since patched many of the vulnerabilities associated with the leaked NSA tools, you can bet that adversaries like lone-wolf and nation-state actors are already plotting their next attack, so now is not the time for security teams to relax. This lull in widespread outbreaks should be used by security teams to reinforce their defenses.

CASE STUDY_ BUSINESS EMAIL COMPROMISE

The situation seemed like something pulled from the Twilight Zone — a business committing fraud against itself, and no one was able to explain why. Emails showed that the appropriate parties approved each fraudulent ACH transaction. Yet, none of the approvers recalled giving their consent, or even seeing the emails that bore their names.

Cylance was asked to investigate the incident and provide insight. Our investigators examined the email system for clues. There, they discovered suspicious email handling rules on several email clients which diverted some employee communications into the Junk folder.

An attacker was impersonating everyone from the initial requestor to the approving CFO by using their Junk folders for fraudulent expenditure approvals. Further analysis by Cylance showed that the email system was not forcefully compromised. The attacker used legitimate credentials to login to the Outlook Web Access (OWA) server and implement their larcenous plan.

At the conclusion of this case, Cylance made the following recommendations:

- Implement multi-factor authentication as widely as possible, especially on remotely accessible resources and users with privileged and/or administrative accounts
- Enable auditing on Office 365 to stay informed of the activities occurring within the environment
- Centralize audit logs and create alerts for suspicious activity
- Utilize a strong password policy that favors length over complexity

[1]Confucius - CVE-2016-7193,CVE-2015-1641,CVE-2017-11882,CVE-2015-1641
Patchwork - CVE-2012-1856,CVE-2014-4114,CVE-2017-0199,CVE-2015-1641

THE BIG TEN

THE MOST PREVALENT THREATS WITHIN THE CYLANCE CUSTOMER COMMUNITY FOR 2017. IN THIS SECTION, WE EXPLORE WHAT MAKES THESE ATTACKS SO POPULAR FOR ATTACKERS.

WANNACRY

BUSINESS IMPACT:

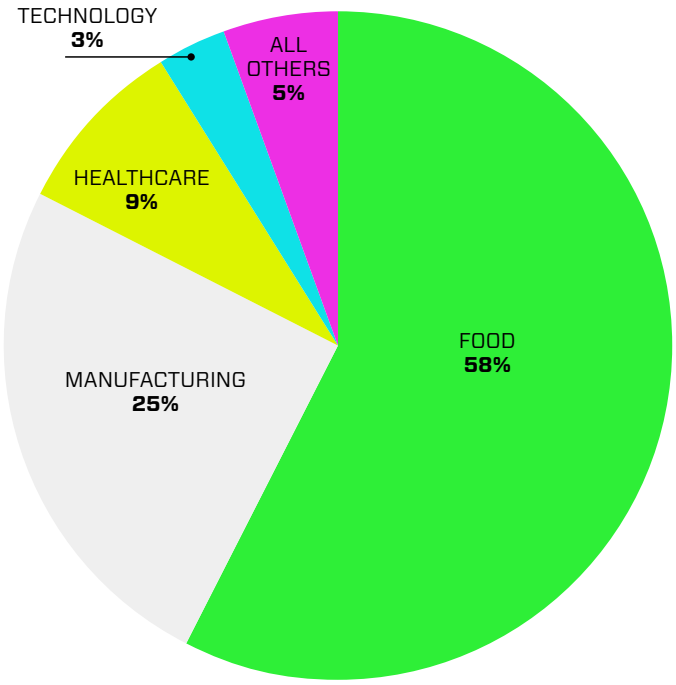
Encrypted machines that organizations were unable to decrypt, resulting in permanent loss of data, and a host of businesses reported a material impact to revenues directly caused by the WannaCry attack.

Many people have felt the impact of WannaCry — from late nights spent rebuilding infected machines to a heightened sense of insecurity. WannaCry has put many businesses on edge. Unfortunately, WannaCry will not be the last outbreak as assuredly as it wasn't the first. Complex software systems will always have bugs. However, the knowledge, skill, and time needed to ferret those bugs out and develop them into exploits has increased significantly. With WannaCry, we've witnessed what can happen if those weaponized exploits are not safeguarded and handled like the dangerous weapons they are.

As a team, we've primarily been tracking coverage of WannaCry to ensure new variants are covered by our product. As a result, we've been slogging through a surprisingly large number of variations. We wanted to get a clearer picture on the hash variance we were finding in the wild. Although there are plenty of opportunities and places to modify the wormable variant of WannaCrypt, we did not see any attempts to replace the payload of the worm or modify the functionality significantly. The repackaged ransomware appears primarily designed to introduce variability into the wild and prevent simple hash blacklists from slowing the spread.

Thankfully, the prevalence of WannaCry was severely limited owing to the discovery and sink-holing of the kill-switch domain and, to a lesser extent, due to the prevalence of another strain of malware called Adylkuzz, a bitcoin miner that appeared slightly before WannaCry that utilized the same SMB exploit to propagate. Adylkuzz, however, would modify the Windows firewall settings to close port 445 on infected systems, which would have impacted WannaCry's ability to spread.

"ADYLKUZZ, HOWEVER, WOULD MODIFY THE WINDOWS FIREWALL SETTINGS TO CLOSE PORT 445 ON INFECTED SYSTEMS, WHICH WOULD HAVE IMPACTED WANNACRY'S ABILITY TO SPREAD."



WANNACRY IMPACT ACROSS INDUSTRIES

Food	58%
Manufacturing	25%
Healthcare	9%
Technology	3%
All Others	5%

As for the modular nature of WannaCry, it would appear that in addition to the reuse of SMB exploitation code from a public repository, there is strong evidence of code reuse elsewhere, making the task of attribution very difficult from a simple code analysis perspective. The individual components also vary in terms of complexity, and although largely trivial with very little use of obfuscation, again seem to hint at the possibility of code reuse, indicating the involvement of multiple authors.

Finally, it has been widely reported that there were as many as several hundred variants found in the wild. While these reports have some credibility, the clear majority appear to have been either doctored versions of the original variant, primarily modified by researches to alter the kill-switch domain, or are subcomponents that have been extracted/carved from on-disk or in-memory images, leading to differing hash values but identical functionality.

UPATRE

BUSINESS IMPACT:

Loss of employee and customer data resulting in increased risk of identity theft.

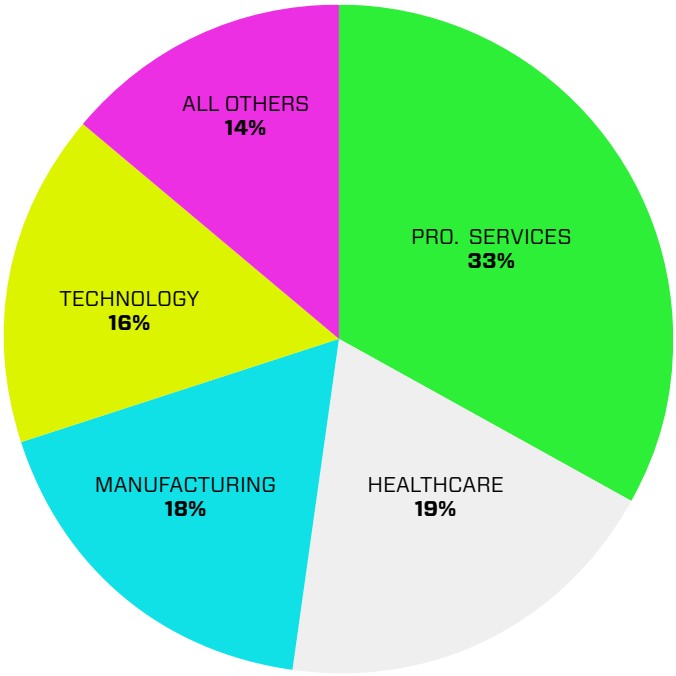
Upatre is a prolific dropper/downloader associated with the Dyre/Gozi banking trojans. Delivery is typically via malspam campaigns carrying a zip file attachment. Delivery via exploit kits has also been observed. For campaigns using malspam, the zip file will often conceal a malicious .scr or .exe. When executed by the user, a clone is dropped to %TEMP% and launched. The main banking trojan payload is then downloaded from the command and control (C2) servers, usually over HTTP, from a handful of embedded domains or IP addresses. Banking trojans steal financial and/or personally identifiable information, making the information available for purchase on the black market. This threat is applicable to individuals and businesses alike, where inadvertent disclosure of personally identifiable information or credit card data has self-evident financial and legal consequences.

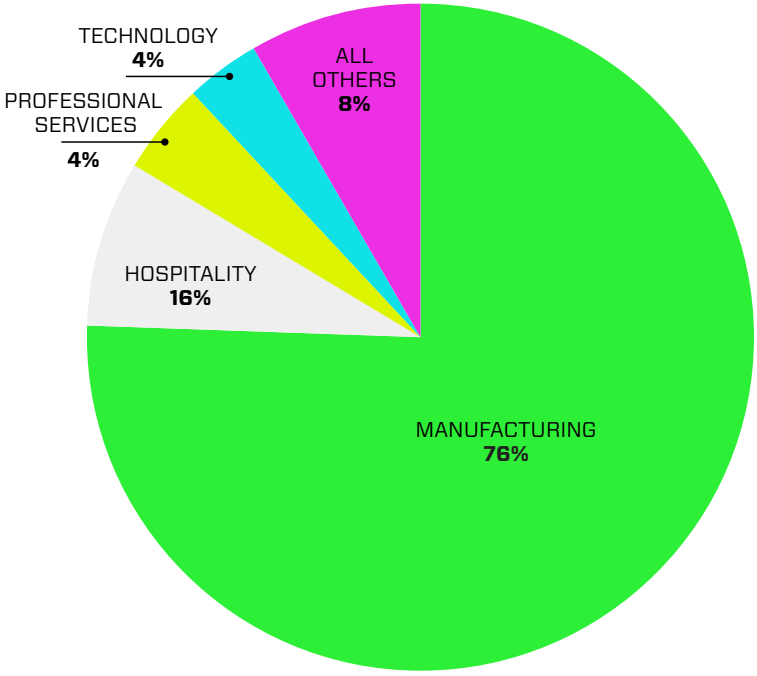
CERBER

BUSINESS IMPACT:

Impacted machines that organizations were unable to decrypt resulted in permanent loss of data.

Cerber is a malicious ransomware distributed denial of service bot that hooks into audio devices to externally speak to victims after deleting shadow copies, encrypting files, and encrypting databases using RC4 and RSA algorithms. In the past, Cerber would geo-fingerprint victims to identify if they belong to one of the following countries: Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Kazakhstan, Moldova, Russia, Turkmenistan, Tajikistan, Ukraine, or Uzbekistan, and if not, it would continue attacking.





UPATRE IMPACT ACROSS INDUSTRIES

Professional Services	33%
Healthcare	19%
Manufacturing	18%
Technology	16%
All Others	14%

CERBER IMPACT ACROSS INDUSTRIES

Manufacturing	76%
Hospitality	16%
Professional Services	4%
Technology	4%
All Others	8%

"OVER THE YEARS, CERBER HAS INCORPORATED ANTI-AV EVASION TECHNIQUES, SUCH AS EMPLOYING THE USE OF A HASH FACTORY SERVER"

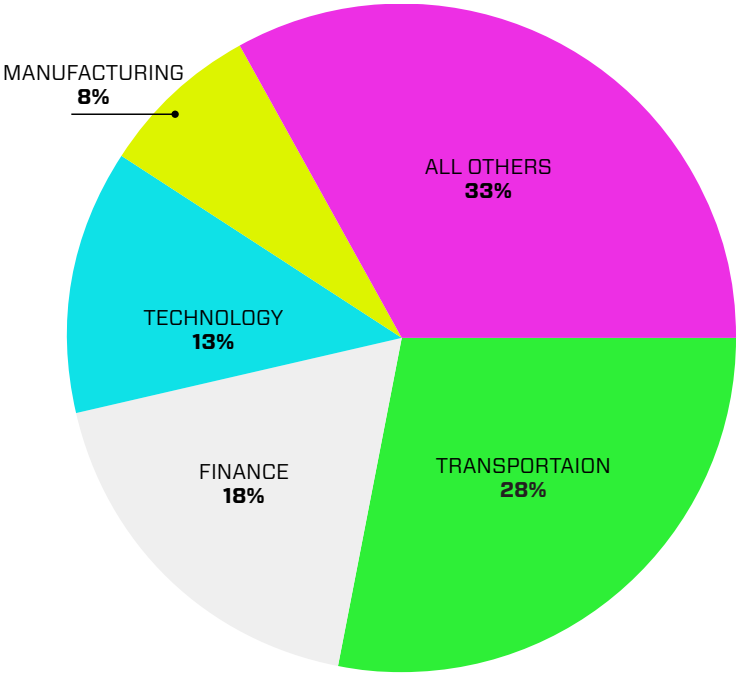
Over the years, Cerber has incorporated anti-AV evasion techniques, such as employing the use of a Hash Factory server, where its hash gets randomly generated every 15 seconds, hiding in encrypted files and using an NSIS plugin called system.dll to load itself into memory, or using a custom DLL decoder to load and decrypt its contents into memory. Another novel feature included in Cerber is the ability to work offline. Cerber is sometimes included as an example of a fileless attack. This is only partially true, or at the very least depends on the stage of the attack to which is being referred. More recent campaigns have relied on multiple layers of JavaScript and PowerShell to either download and execute payloads directly, or delay execution and download/execute the full payload at a determined time or state. Burying the final payload across layers of obfuscated JavaScript and PowerShell commands does allow for better evasion and persistence, but at the end of the day, there are still files involved, there are scripts/command being run, and there are multiple points of prevention prior to the final payload.

EMOTET

BUSINESS IMPACT:

Loss of sensitive employee and customer data.

Emotet is a variant of the Feodo trojan family. It first emerged in 2014 as a trojan designed to steal banking credentials and other sensitive information and is most often propagated by way of phishing emails containing a tainted document or URL. The first step of this attack arrives in the form of a malicious Microsoft Word file that contains a macro which requires the target to manually enable functionality. The script can have different obfuscator techniques, but at the end, the base code is the same. This obfuscated code is saved in the properties comments section, and the macro has the instruction *ActiveDocument.BuiltInDocumentProperties* in the middle of a lot of garbage code. The script leverages PowerShell to download and execute the Emotet malware payload as certproc.exe. This threat creates a copy in the folder *\%AppData%\local\microsoft\windows\certproc.exe* that is then persistent in the registry. The Emotet malware proceeds to search the infected system for sensitive information. Once it has located information of interest to the attacker, it proceeds to exfiltrate the data to a C2 server.



EMOTET IMPACT ACROSS INDUSTRIES

Transportation	28%
Finance	18%
Technology	13%
Manufacturing	8%
All Others	33%

LOCKY

BUSINESS IMPACT:

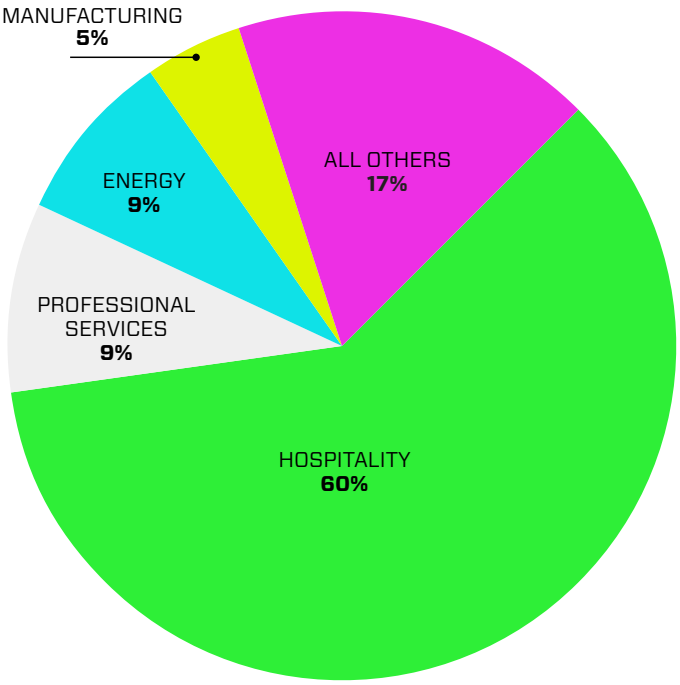
Loss of sensitive data and employee productivity due to unusable encrypted machines.

Locky ransomware affected more than 400,000 victims in the very first week of its detection. Locky caused particularly noteworthy trouble in the healthcare industry during February 2016 by attacking the system of Hollywood Presbyterian Medical Center, which paid the largest publicly-admitted ransom of $17,000 in bitcoin. A number of other large hospitals also paid hefty ransoms during this wave of attacks. Since then, we have seen a lot of variants of the Locky ransomware — Zepto, Thor, Osiris, and Diablo6 to name a few. This old malware didn't need to take a new approach. The authors behind Locky just had to tweak the only part of the process that can never be fixed — the end-user.

Some of the 2016-era Locky campaigns borrowed a page from Dridex malware's book on distribution/delivery and became more reliant on PowerShell scripts to both download and execute the final payload. The most recent change for Locky came as one of the most popular ways to spread malware: spear phishing emails. The attack happens in two stages. The first stage is the spear phishing email that has a zip archive attached. Inside the archive is a VBS file with the same name as the archive. When the victim decompresses the archive and

> "THIS OLD MALWARE DIDN'T NEED TO TAKE A NEW APPROACH. THE AUTHORS BEHIND LOCKY JUST HAD TO TWEAK THE ONLY PART OF THE PROCESS THAT CAN NEVER BE FIXED- THE END-USER."

clicks on the file, the VBS script starts to run. The script tries to connect to the C2 server and download the file *y872ff2f*. The script saves this second stage payload in the *%AppData%/Local/Temp* folder with a different name (GlNPcFUJR.exe) then runs the malware. The domain *dbr663dnbssfrodison[dot]net* was created on August 1, 2017 using the registrant email: *jenniemarc(at)mail(dot)com*. A reverse WhoIs Lookup on that account shows that 333 domains were registered by this email starting in 2016 and as recently as October 2017. Some of those domains are known to be serving other families of ransomware.



LOCKY IMPACT ACROSS INDUSTRIES

Hospitality	60%
Energy	9%
Professional Services	9%
Manufacturing	5%
All Others	17%

PETYA

BUSINESS IMPACT:

Destruction of sensitive data until recently when a decryption tool was made available.

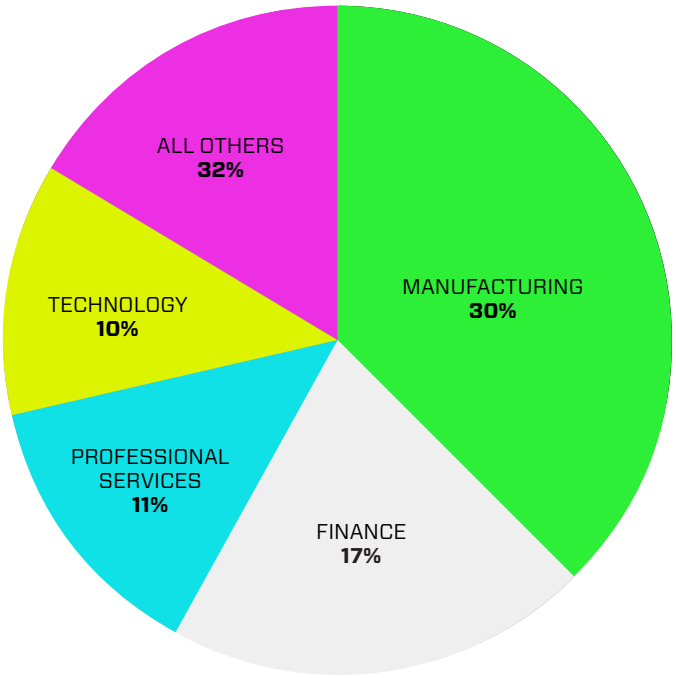
Petya is a highly-effective ransomware with multiple variants and sophisticated attack vectors, originally making its appearance in March 2016. The infection became widely known due to high-profile targets, attacks in the Ukraine, and the trademark flashing skull the malware displayed. Basic variants are known for a boot loader that encrypts the MFT, a dropper that installs the bootloader, and a flashing red skull that appears before the ransom note. With the MFT encrypted, the whole disk is at risk rather than just specific files. A variant known as Mischa acts as a more conventional ransomware, encrypting files and executables in usermode if Petya is denied administrative privileges. A further refinement labeled Goldeneye advanced the encryption and disk locking routines. While decryptors were developed for Petya and Mischa, Goldeneye does not seem to be decryptable. A further wiper variant, NotPetya, erases a user's data forever as the public key used for encryption is erased. As of July 2017, the author published the private key, which has been used to make a decryption tool available for those affected.

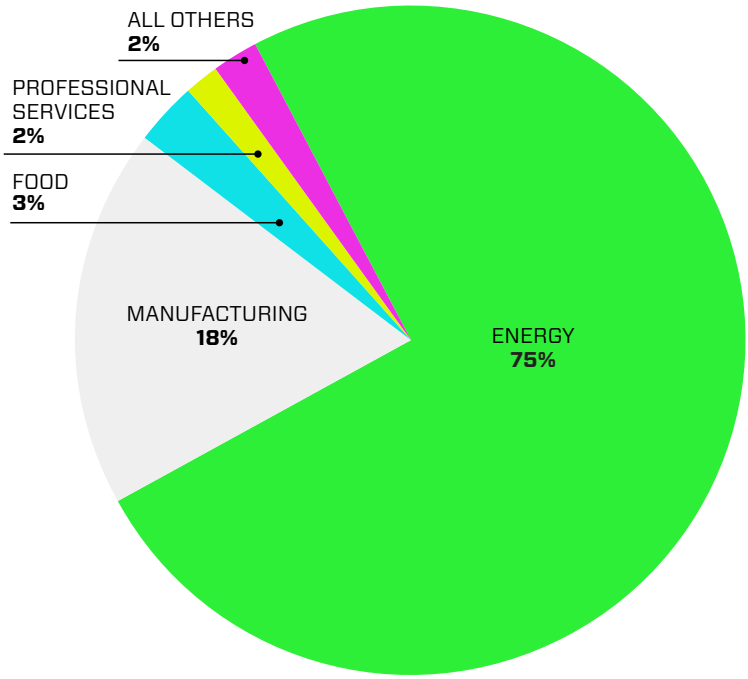
RAMNIT

BUSINESS IMPACT:

Loss of sensitive customer and employee information.

Ramnit is a parasitic virus that infects Windows PE executable files. It also has a worm capability to spread to removable media with shortcut files pointing to copies of the malware. Ramnit also infects HTML files by injecting a VBS code. Users who access those HTML files would be infected with this virus. Ramnit is designed to function as a banking trojan as well as remote access trojan. In February 2015, European authorities took down the Ramnit botnet that had infected 3.2 million machines, however, in spite of the take down, Ramint resurfaced in December 2015. New variants of Ramnit targeted major banks in the U.K. in 2016. Some Ramnit campaigns/attacks operate in a truly fileless manner, that is, without reliance on the direct running of PowerShell or JavaScript code pieces. Ramnit is known to store XOR-encrypted payload data in the registry acquired via SSL. Ramnit's loader thread is then able to parse and decrypt the blob from the registry and perform injection at that stage.





PETYA IMPACT ACROSS INDUSTRIES

Manufacturing	30%
Finance	17%
Professional Services	11%
Technology	10%
All Others	32%

RAMNIT IMPACT ACROSS INDUSTRIES

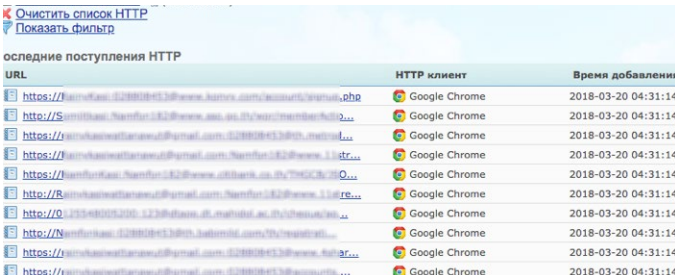
Energy	75%
Manufacturing	18%
Food	3%
Professional Services	2%
All Others	2%

FAREIT

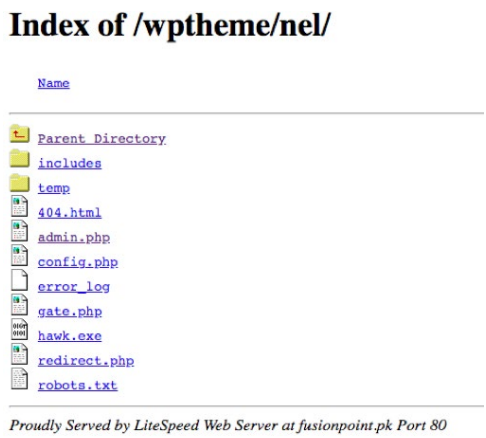
BUSINESS IMPACT:

Compromised user credentials.

Fareit (aka: Pony/Pony Loader) is an extremely popular credential-harvesting malware that also has a few other tricks up its sleeve. Fareit has been in use in various forms since 2011. Its primary purpose is to harvest credentials (username/password data) from a defined set of applications and protocols. Just about every client application is represented and supported in Fareit from the most popular, such as Chrome, Firefox, and Thunderbird, to more obscure and legacy applications like bisonFTP, Incredimail, and Flock, among others.

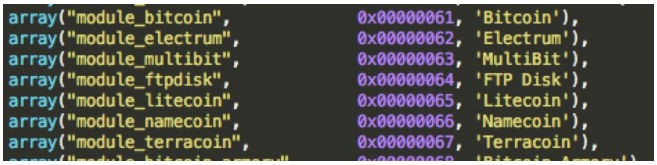


In addition to pulling valuable login data, Fareit can also be used to call and launch additional malware. There are multiple reasons why this simple tool is still used in such great volume. The primary drivers are ease of use and the fact that it's available for free. Setting up Fareit requires little to no expertise in that it is a simple Panel + Builder combo. Just place the relevant configuration files on the webserver of your choice, and you are ready to go (provided MySQL and PHP and other standards are in place). This part is frequently taken care of beforehand, as we primarily observe Fareit being hosted/managed from compromised servers that are otherwise legitimate.



That is to say, attackers will find a way to gain write access to the file system of the public-facing web server (exploits, etc.) and host it as long as possible without the true owners of the host catching on. That's not to say there are not dedicated Fareit/Pony hosts, but it is far more common to see the hosting appear on otherwise clean/safe hosts. Beyond the ease of installation and management, Fareit is essentially free and has been for years. Various cracks and source code leaks have found their way into the hands of malicious users over the years spanning every version of Fareit. The most popular versions are post-2.0 (2.2/2.3) and it is not uncommon to see malicious actors continuing to leverage very old cracks from the likes of TrojanForge and Fudtool.

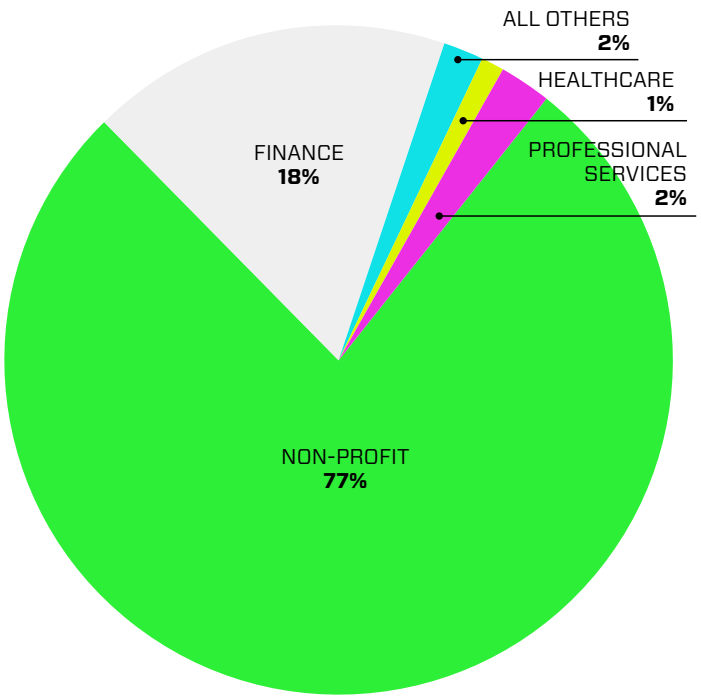
As for functionality, Fareit excels at its primary goal of harvesting credentials and transmitting them to malicious actors. Later versions also added functionality to harvest login data for cryptocurrency wallet services and currency exchanges. This applies to the most popular cryptocurrencies, such as Bitcoin and Litecoin, as well as less popular options like NovaCoin, Primecoin, and Frankocoin, among others.



Fareit has proven to be a useful tool for early attack stages. We often see it delivered via phishing and spear phishing attacks as a means to gather credentials for later phases of attack.

Long-term Fareit campaigns are typically managed and manipulated by mid-level, low-skilled, actors. The setup and configuration can be automated so that the server installation/set up and initial configuration can be handled with little to no intervention by individuals lacking in development/scripting language/server internal skills and the like. It is also very common to see multiple instances of Fareit being managed on the same host and separated by working directories. Running other similar, turnkey tools on the same host is also very common. We frequently observe single servers/hosts running instances of Fareit alongside Lokibot, Azorult, and various phishing kits/pages. The image on the next page shows a typical multi-threat setup where Fareit is being hosted alongside a ready-baked phishing kit.

Despite its age and exposure, Fareit/Pony continues to be a present and popular tool amongst malicious actors at various levels. This includes inclusion/delivery via common exploit kits (ex: RIG). There is nearly no barrier of entry to get up and running.



FAREIT IMPACT ACROSS INDUSTRIES

Non-Profit	77%
Finance	18%
Professional Services	2%
Healthcare	1%
All Others	2%

POLYRANSOM

BUSINESS IMPACT:

Loss of business-critical data due to encrypted machines.

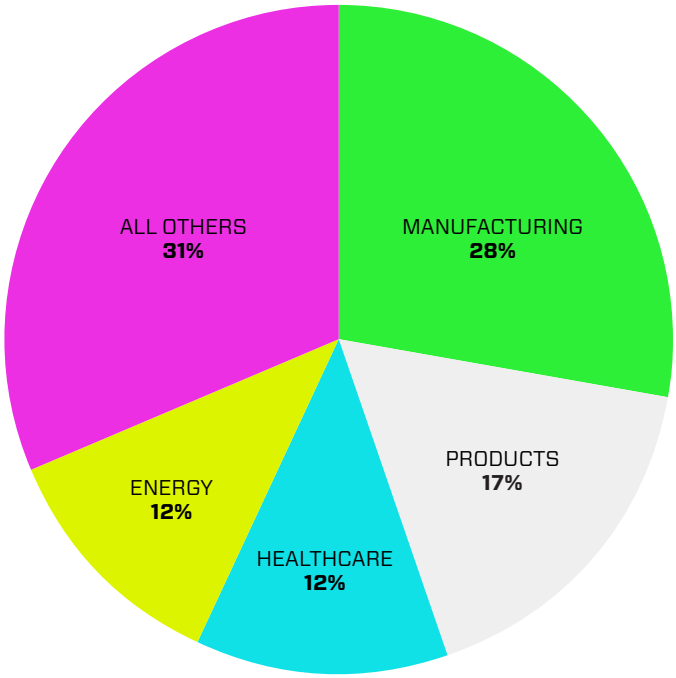
PolyRansom (aka Virlock/Nabucur) continually shows that it is not only one of the more prolific and successful ransomware families, but also one of the most complex. First observed in 2014, Virlock was the first example of ransomware that is also a parasitic infector with screen-locking functionality.

PolyRansom is able to continually generate new copies of itself, which dramatically complicates the process of analyzing/reverse engineering it. Decryption tools, when possible or feasible, are more complex to code, as the parasitic side of the malware must be taken into account. That being said, the quality/accuracy of PolyRansom's implementation of these encrypting methods is not consistent. There are examples where the encryption layers are easily reversible. PolyRansom has the capability to decrypt only the smallest portions of code that it needs at a given point, subsequently re-encrypting those code chunks after use and before continuing its routine. This re-encryption of its own code alters the original binary image. As with any polymorphic scenario, this quickly evades simple/rudimentary detective controls (ex: signature-based AV), particularly in situations where the detective control is relying on a specific hash/checksum/cloud-lookup to handle convictions.

PolyRansom processes files by adding its own code into said files (parasitic component) and then outputting an executable package/wrapper, often in the form of a straight executable, or self-extracting RAR. Upon infection/wrapping of files, said individual files are in essence weaponized/live copies of the infector. This feature is part of what allows PolyRansom to spread without being a true worm. If files that happen to reside on a shared storage location (fileshares, cloud-based service, etc.) are infected, that infection can be spread via that share/service as users will unknowingly attempt to open/manipulate the files.

In addition to the standard ransomware features, PolyRansom contains other robust mechanisms for anti-analysis. These include anti-VM features, the use of a custom-developed packer, and the subsequent use of multiple packed/crypted layers. The encryption routine for the actual file encryption is a minor deviation as well. In most observed campaigns, the encryption is handled across two basic stages. Files are first encrypted via XOR+Rotate on Left(ROL), followed by an additional XOR layer.

Virlock/PolyRansom has been associated with Carbanak and other large-scale campaigns, but it is not exclusive to large or targeted events. This family has been delivered via standard methods such as phishing and web-based attacks.



POLYRANSOM IMPACT ACROSS INDUSTRIES

Manufacturing	28%
Products	17%
Healthcare	12%
Energy	12%
All Others	31%

TERDOT/ZLOADER

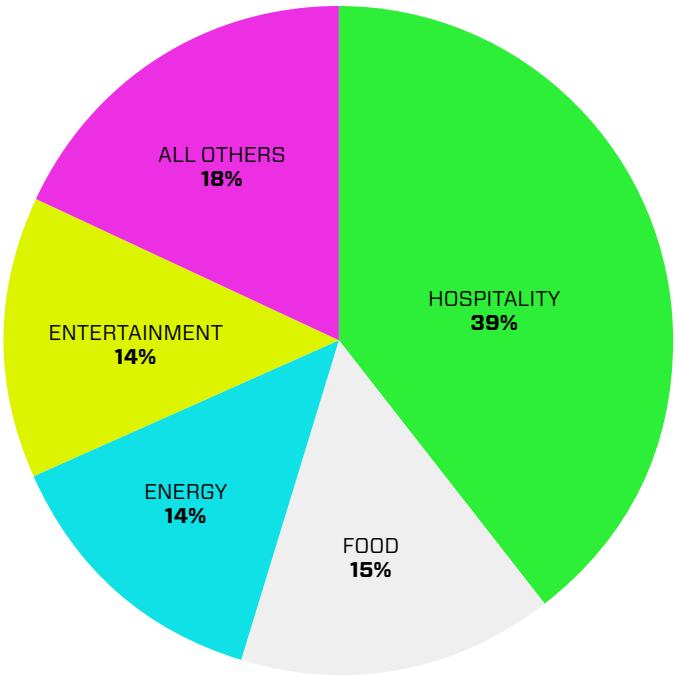
BUSINESS IMPACT:

Theft of sensitive banking and personal data, and the modification of traffic and page data.

Terdot came into prominence in 2016 and continued to flourish in various forms though 2017. Terdot's heritage lies in the source of the well-known Zeus banking trojan. The source code for Zeus was very publicly leaked in 2011. The primary goal of Terdot/Zloader is to download and spread the Zbot data stealer and, while not exclusively, is typically used to target banks and other financial institutions. Backdoor (VNC) functionality is included in many observed variants as well. Terdot is distributed via malicious email message, as well as via common exploit kits like Terror and Sundown. The Terdot/Zbot combination is particularly dangerous given its ability to circumvent the SSL trust model. The malware can inject the preferred browser and utilize its own fake SSL certs in order to MITM browser sessions:

```
aData_before    db 'data_before',0Dh,0Ah,0 ; DATA XREF: sub_1002C43D+1C4E↑o
; CHAR aData_inject[]
aData_inject    db 'data_inject',0Dh,0Ah,0 ; DATA XREF: sub_1002C43D+1554↑o
; CHAR Str1[]
Str1            db 'data_after',0Dh,0Ah,0 ; DATA XREF: sub_1002C43D+1335↑o
; CHAR aData_end[]
aData_end       db 'data_end',0Dh,0Ah,0 ; DATA XREF: sub_1002C43D+1CA3↑o
; CHAR aWebfakes[]
aWebfakes       db 'webfakes',0         ; DATA XREF: sub_1002F0CF+14C↑o
; CHAR aWebfilters[]
aWebfilters     db 'webfilters',0       ; DATA XREF: WebFilters_1002F3A0+14↑o
```

The legitimate Certutil tool is used to facilitate the signing of the fake SSL certs. This can result in theft of sensitive banking/personal data, but also the modification of traffic/page data. Some variants in late 2017 were observed manipulating social network account data, slurping data, and posting links to executable versions of itself to facilitate further spreading. Terdot/Zloader has also been shown to discriminate targets (geo-fencing) in the form of avoiding Russian victims in campaigns. Similarly, when targeting social networks, the Russian VK service is typically excluded, while Google+, YouTube, Facebook, Twitter, and other platforms are fair game.



TERDOT/ZLOADER IMPACT ACROSS INDUSTRIES

Hospitality	39%
Food	15%
Energy	14%
Entertainment	14%
All Others	18%

TRENDS BEYOND MALWARE FAMILIES

IT IS IMPORTANT TO UNDERSTAND WHERE THE BULK OF ATTACKS LIE SO THAT WE CAN CAREFULLY ADDRESS THOSE, BUT IT IS EQUALLY IMPORTANT TO PLAN FOR AND FORESEE THE ATTACKS THAT MAY BE UNIQUE TO SPECIFIC ENVIRONMENTS OR ARE TARGETED IN NATURE.

TO UNDERSTAND HOW EVENTS OF TODAY MAY IMPACT SECURITY EVENTS OF TOMORROW, HERE ARE SOME OF THE BIGGER TRENDS THAT EMERGED FROM ALL THE CHAOS OF SECURITY EVENTS AND ATTACKS IN THE PAST THREE YEARS.

KINKS IN THE LINKS: YANKING THE SUPPLY CHAIN

Laser-focused attacks, directed at the core of our long-standing trust models, have become both more visible and more impactful within the last two years. Integrity is paramount to a safe and secure environment, and campaigns against integrity of data and transactions, along with the assurances associated with those interactions, are becoming more and more accessible to sophisticated attackers. Attacks on the supply chain can take on many forms.

The most prolific and damaging attacks have been delivered in the form of maliciously-modified code delivered though seemingly official channels, where one or more steps in the process are under the control of the malicious actor. Often, attackers are going to great lengths to identify the weak link in the supply chain, taking months or years conducting appropriate and thorough reconnaissance. Once they identify a smaller-route (third party) into a larger and final target, they will continue to the next phase of the campaign. The path of least resistance will always be the most attractive path. Targeting developers via external collaborative systems, external update/patching mechanisms, and more, are quite often a more rapid path into a target organization.

In 2016 and 2017, we saw three major publicly-disclosed supply chain compromises, CCleaner, Shadowpad, and NotPetya. We consider these compromises to be trend-setters that have raised the bar. These three more recent supply chain compromises can be better explained by first looking at one that came before them, Kingslayer.

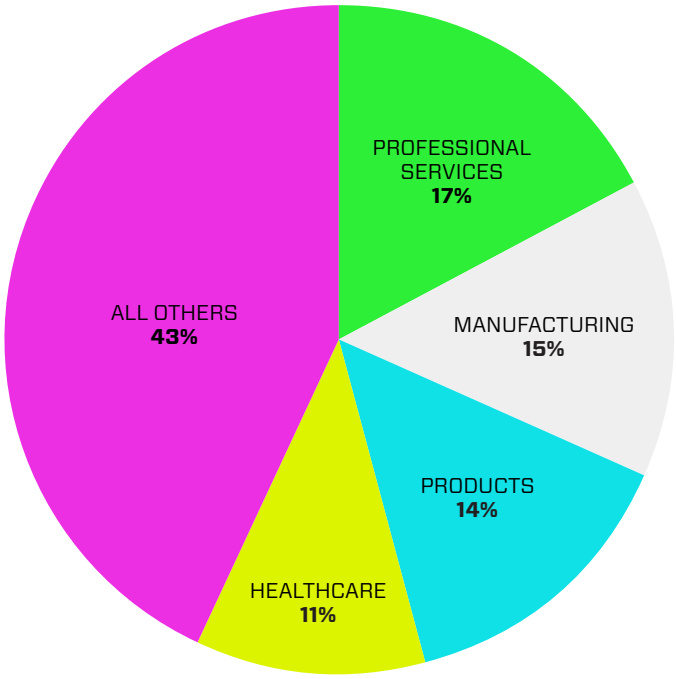
Kingslayer goes back to 2015, but it sets a good stage for discussing more recent events like CCleaner and Shadowpad. Even with the small delivery window between April 9 – 25, 2015, this attack illustrates the sophistication and resources available to modern, highly-determined attackers. The Kingslayer backdoor came in the form of trojanized binaries and installers from a popular Windows Event Log analysis tool. The actors behind this campaign setup their C2 and support infrastructure relatively quickly. During this process, a few things occurred which shattered any perceived trust in the assumed legitimate applications that were weaponized. In order to trojanize and deliver the modified binaries, the attackers had to have direct access to the source code of the compromised application. With that in place, it is also known that the attackers signed the binaries and installers with valid code signing keys. This indicates that the attackers had source code as well as code build/signing systems under their control. The remaining piece would be access to the legitimate delivery channel (ex: websites). Kingslayer had targets all across the spectrum, including manufacturing, government, financial, educational, and telecommunications entities. This level of deep compromise and control, removing any assurance of integrity, would be echoed in other high-profile attacks in 2016 and 2017, namely CCleaner and Shadowpad.

CCleaner was one of the most significant attacks of 2017 with regards to volume, which also happened to involve a supply chain compromise. Between August and September 2017, trojanized versions of CCleaner and CCleaner Cloud (from AVAST/ Piriform) were distributed via channels that were believed to be official, compromising approximately 2.5 million hosts. The weaponized versions of CCleaner contained a multi-functional backdoor. The malicious code was able to download/install additional malware, as well as facilitate the harvesting and transfer of sensitive information from infected hosts. While the overall infection footprint was large (over two million), there is some indication via analysis of secondary payloads on certain infected hosts that the attackers were also interested in specific information or data from specific companies. This makes perfect sense if we consider the apparent actor(s) behind the campaign. To date, the reliable and observable evidence indicates that a well-known and highly prolific Chinese APT group is responsible for this compromise. The group, APT17, which is also known as Aurora/DeputyDog, has been active for many years and is responsible for numerous other critical and notable attacks, including Operation Aurora, Operation DeputyDog, Operation Ephemeral Hydra, and many more. Given the requirements to carry out the CCleaner attack, it makes sense that a group as established as APT17 would be responsible. Upon discovery of the targeted, secondary payloads, AVAST issued the following, telling, statement:

“Finally, it is extremely important to us to resolve the issue on customer machines. For consumers, we stand by the recommendation to upgrade CCleaner to the latest version (now 5.35, after we have revoked the signing certificate used to sign the impacted version 5.33) and use a quality antivirus product, such as Avast Antivirus. For corporate users, the decision may be different and will likely depend on corporate IT policies. At this stage, we cannot state that the corporate machines could not be compromised, even though the attack was highly targeted.”

Ultimately. there are many victims in this level of attack, and beyond the infected hosts/users, organizations that have to reestablish trust in their manufacturing, distribution, and verification processes are often damaged as well. If they are able to resolve the issue, plug the holes that were exposed, restore trust within their user/partner/connected communities, and recover all associated costs, it could take years. Not all affected entities are able to come back after events of this magnitude. Public discourse and thorough education on how to prevent these matters is increasingly necessary.

Not surprisingly, many industries were impacted by CCleaner, but within Cylance ecosystem, professional services, manufacturing, products, and technology were highly targeted.



CCLEANER IMPACT ACROSS INDUSTRIES

Professional Services	17%
Manufacturing	15%
Products	14%
Healthcare	11%
All Others	43%

Shadowpad was delivered shortly before the CCleaner attack, and the campaign shares many functional traits with the previously mentioned campaigns. In July 2017, downloads of **NetSarang's Xmanager Enterprise, Xmanager, Xftp, XShell, Xlpd, and Xftpd** contained a trojanized library. The affected DLL (nssock2.dll) contained a sophisticated backdoor which was remotely available to the attackers via numerous layers of complex encryption. The backdoor is highly modular in nature, allowing for remote maintenance/updates, distribution, and execution of arbitrary code by way of an actively paired C2 server. The payload is also able to generate and obfuscate code via a registry-based virtual file system.

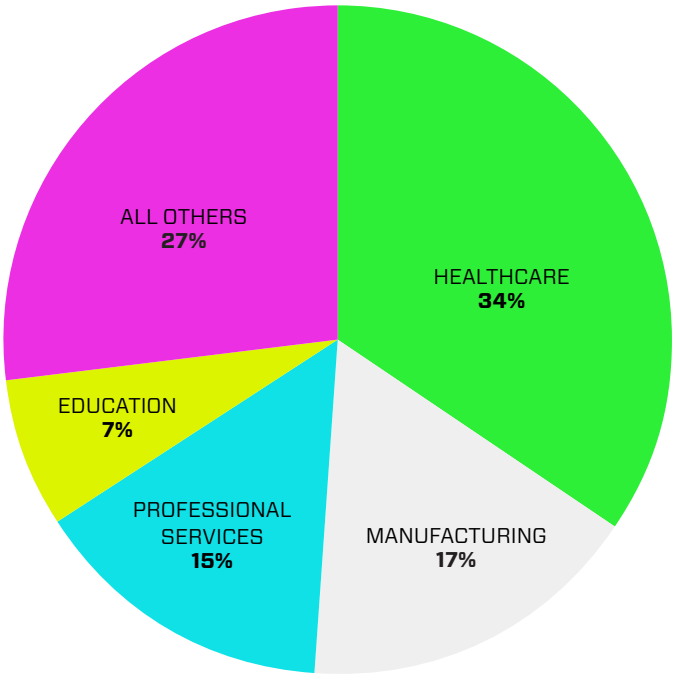
The weaponized versions of NetSarang's management software were live from July 17 to August 4, 2017, at which point the issue was reported to NetSarang, resulting in their corrective action. Similar to CCleaner, the actors behind Shadowpad (CN group Winnti/Axiom) had working access to source code and valid signing certificates. The weaponized binaries were signed using NetSarang's valid cert. It is apparent that the intent behind Shadowpad was long-term, highly covert data/information monitoring and theft. The communications between hosts and the C2s were well obfuscated through multiple layers, and were both encryption- and transactional-based. This helped to ensure both persistence and success as the malicious communications were more difficult to observe though standard analysis methods.

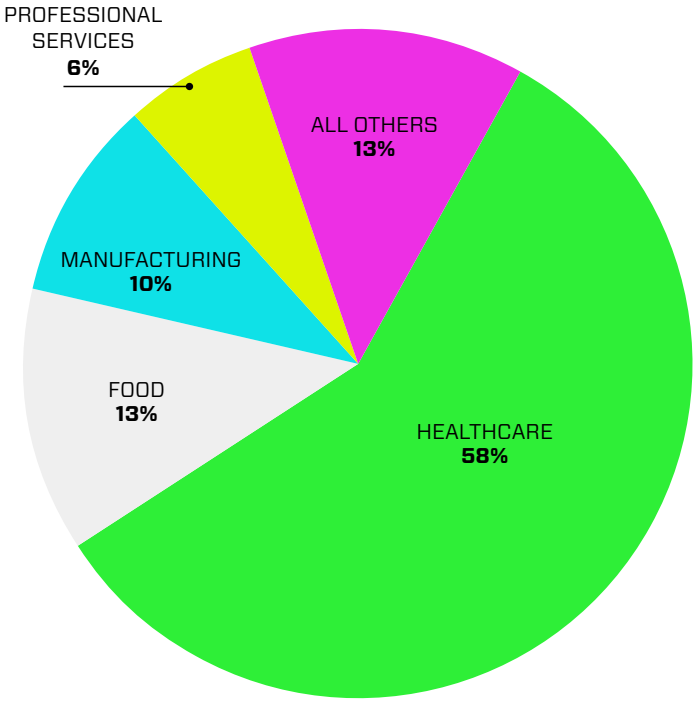
Shadowpad targeted industries of various types, including healthcare organizations, energy and power companies, and financial institutions.

NotPetya hit in July 2017 and proved to be a rapid-moving, and highly-destructive threat. It was able to spread quickly by leveraging the EternalBlue + DoublePulsar vulnerabilities, and it contained an MBR replacement/overwrite functionality similar to Petya, although they are not directly related. With this particular threat, destruction instead of financial gain was the primary motive. It is, however, important to note that NotPetya can also be viewed as a highly-successful supply chain compromise.The initial delivery of the threat came by way of a Ukrainian accounting software package named MeDoc. Once the first wave hit, the EternalBlue + DoublePulsar combo was able to assist with further spreading of the infection. The attackers had started backdooring MeDoc updates in the months prior to the NotPetya outbreak. These fake updates allowed the attackers to then pivot within the MeDoc infrastructure and distribute/execute the final trojan. The attackers had a foothold on the MeDoc update servers from at least April 2017 onward via both stolen credentials and webshells (PAS). It has been reported that the compromised web servers (NGINX) had not been patched since 2013. There is a lot to learn and note from NotPetya, but if we needed another reminder to keep external-facing web servers patched, up to date, and properly configured, this is a great one.

FAST AND FURIOUS: RANSOMWARE AT LUDICROUS SPEED

Ransomware is not a new or novel phenomenon. What has evolved rapidly in the last two to three years is the sheer velocity of the attacks. This volume increase can be observed in both the speed of infection/spreading as well as the fundamental encryption functionality. Ransomware attacks grew threefold during 2017 as compared to 2016. Cylance saw ransomware attacks affect users universally across over 160 countries and 16 different verticals. Ensuring viciously accelerated attacks is highly attractive to attackers for many reasons. For one, the quicker the infection spreads, the more money they stand to make — that's a given. Keeping up with attacks like these using outdated, traditional solutions can be defined by either having to wait for a signature to ensure detection, or scenarios where the solution in question is simply too slow to convict before the infection takes hold and continues on its path. This can be due to, amongst other things, slow cloud-based lookups for conviction or the lack of pre-execution controls. No matter what the nuanced reasoning is there, criminals/malware authors/attackers are well aware of this and continue to exploit it in the swath of successful ransomware attacks that make headlines each day.





RANSOMWARE 2016

IMPACTED INDUSTRIES

Healthcare	34%
Manufacturing	17%
Professional Services	15%
Education	7%
All Others	27%

RANSOMWARE 2017

IMPACTED INDUSTRIES

Healthcare	58%
Food	13%
Manufacturing	10%
Professional Services	6%
All Others	13%

It is clear that ransomware is here to stay. Over the past year, we have seen many of our customers targeted by ransomware attacks. With each new attack, we research the intent of the specific payload to identify interesting trends. Our analysis has resulted in a few conclusions.

Ransomware may not be what it seems. The WannaCry outbreak delivered a ransomware payload that rendered systems unusable around the world. That said, the ransomware itself was very ineffective when it came to generating revenue for the bad actors. Nearly every machine that was compromised could not be recovered since the bad actor's ransomware site, where the infected user could pay the bitcoin ransom, did not actually deliver the necessary encryption key to the user. So, was the point of WannaCry to generate revenue or something more nefarious? Many have theorized that WannaCry was designed to cause major business disruptions and not generate ransom payouts. Others further hypothesize that WannaCry was a proof of concept or diversion attack that spread faster than the authors expected. Either way, ransomware has become mainstream and will play a prominent role in future attacks.

LOW-LEVEL CYBERCRIME AND CRYPTO-SHENANIGANS CONTINUE

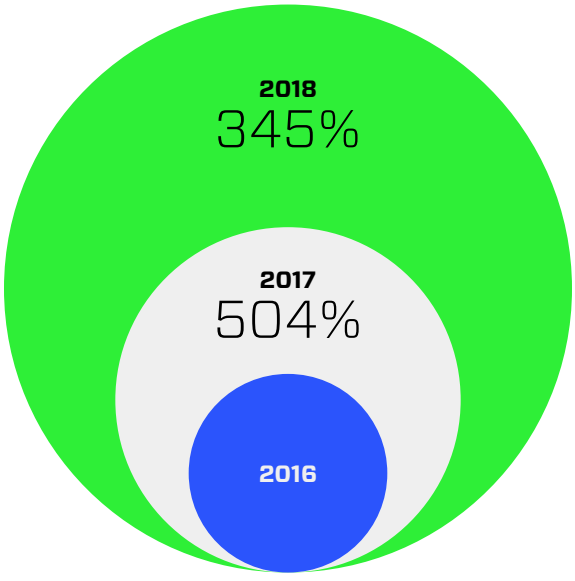
There was a great deal of low-level/entry-level cybercrime activity in 2017. A major blow was dealt to the criminal economy when law enforcement seized and shut down two of the most populous and thriving underground markets. Multiple international law enforcement agencies along with partners in the private sector targeted AlphaBay, Hansa, and several much smaller markets on the dark web. Operation Bayonette dealt a coordinated and harsh blow to a sizable portion of the low-level economy, centered around the buying and selling of drugs, weapons, personal information, stolen goods, digital services, and more. AlphaBay and Hansa were two of the top markets in terms of popularity and size. That being said, there were plenty of other markets that remained, and still exist. It took no time at all for alternatives to take up the slack as vendors and buyers adjusted their activities accordingly.

Several dark web markets continue to thrive. They persist even in a climate of wariness and distrust where criminals don't have faith in markets and sites, and assume that law enforcement could be lurking at all times. Wall Street Market, Dream, Point/T•chka, Berlusconi, and numerous others continue to thrive and survive.

We are also continuing to observe shifts in why cryptocurrencies are utilized in underground markets and for illicit transactions in general, and how they are used. Bitcoins are not inherently secure, nor are they truly anonymous. An entire industry has sprouted up to complement and assist standard law enforcement methodologies to track transactions via cryptocurrencies. Firms like Chainalysis, Blockchain Alliance, BlockSci, and Elliptic make it their business to monitor and analyze cryptocurrency activity and transactions. Cybercriminals are well aware of the ever-growing microscope that they are under and they continue to shift and innovate in order to reduce the exposure of their transactions. Cryptocurrency is not inherently bad, nor would anyone following this technology want to infer such. Likewise, cryptocurrency and cybercrime are exclusive and independent. That being said, you can track innovation around cryptocurrencies through their utilization and adoption rates amongst criminal entities.

One glowing example of this movement and innovation is the slow adoption of alternative currencies such as Monero, Dash, Ethereum, and a select handful of others. Monero is particularly attractive to the criminal world, as it has been shown to be the only option for truly decentralized, secure, and untraceable transactions. For this very reason, multiple markets, including AlphaBay before its demise, supported Monero (XMR) alongside Bitcoin. At the very least, independent vendors participating in markets allow for side-support of Monero, where support is not inherent to the wallet/escrow system of the market. There are also some markets that support Monero only, such as Libertas.

Even with all the extra attention and shifts in infrastructure, these markets continue to thrive and offer a wide variety of goods and services to low-level criminals looking for immediate gratification. These markets are still a reliable source of data (stolen, fraudulent, personal, financial, and beyond) as well as the requisite weapons, drugs, software (malware, cracks, exploits, and more), and anything else you can imagine.



GROWTH OF CRYPTO-MINERS

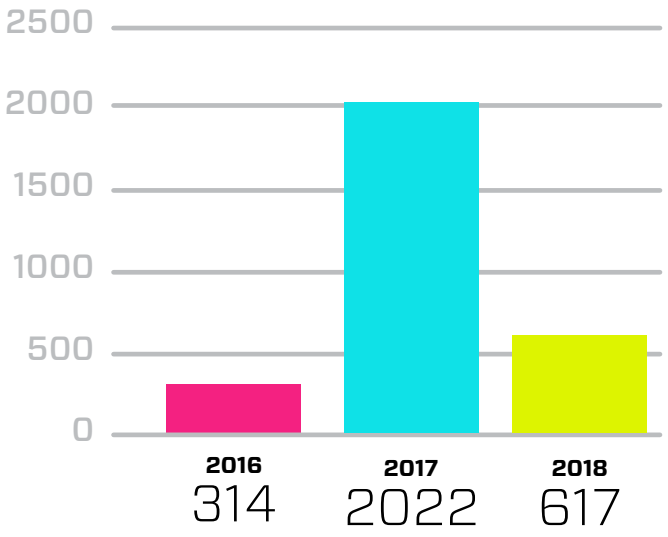
LAUNDERING

Laundering money resulting from illegal activity, along with cashing-out proceeds overall, are very real issues in the cybercrime world. We frequently see novel approaches to dealing with this. Criminals are constantly having to shift their approach, particularly in the last year, as the visibility into Bitcoin transactions has become more of an issue for them. Some enterprising criminals have gone to the extent of pretending to be professional musicians in order to filter their profits though the Apple iTunes ecosystem.[2] For example, an individual can create their own music and via a service of their choice, get the music posted and available for purchase via the iTunes store. Once the music is available for purchase, they can trade Bitcoin profits from criminal activity for iTunes gift cards, which are widely available and allow for a level of pseudo-anonymity, or themselves can be fraudulent as well. They can then purchase their own music via these gift cards and get paid in clean money from Apple. This roundabout method translates to other online services as well, and we are starting see these methods pop up more and more in criminal-authored cash-out guides and laundering how-to documents. Needless to say, if a fraudster is not confident in their own ability to properly launder illegally acquired funds, there is help readily available to them.

"THE RELATIONSHIP BETWEEN CRYPTOCURRENCIES AND THE CYBERCRIME ECONOMY IS IN A STATE OF NON-STOP FLUX AND EVOLUTION."

WALLET-SWIPING TROJANS

When thinking of cryptocurrency and malware, our minds tend to jump to ransomware first and foremost. However, there are families of malware that fit into other layers of cryptocurrency transactions. Trojans like Bitswiper and CryptoShuffler are designed to monitor victims' clipboards. When the infected user pastes a destination wallet for payment to a web form for paying or transferring funds, the intended paste is swapped for the attacker's wallet of choice. The victim has then unknowingly transferred funds to the attacker's wallet directly and transparently. These and similar threats are readily available, often for free for criminal use.



COINSTEALER GROWTH

[2] https://www.consumer.ftc.gov/blog/2016/05/scammers-push-people-pay-itunes-gift-cards
https://www.thedailybeast.com/want-to-launder-bitcoins-how-crooks-are-hacking-itunes-and-getting-paid-by-apple

MULTI-PRONGED ATTACKS

The hallmark of multi-pronged attacks is the use of multiple tools, methods, and strategies to establish and maintain persistence and stealth. When well-planned and resourced, attack campaigns achieve their own sort of fault tolerance as well as improve obfuscation of their activities. They also tend to spread out the resources and focus of those investigating them, either by design or via purposeful deceit with red herring strings and artifacts, or the reuse of well-known infrastructure from other groups.

The closer the attackers can stay to standard OS tools and functionality, the better. The more they deviate/append, the more visible they become. Sticking to tools like PowerShell, Netsh, SC, WMI, and various automatic update/certification mechanisms all fit this model.

The APT34 Group, believed to be based in Iran, is known, like many others, for their heavy reliance on external tools while still employing internal tools when needed. Here is an example:

- Start with a malicious RTF (CVE-2017-11882)
- Upon execution/open of the RTF, an additional txt file/ script is downloaded from a staging server (allowed via the RTF exploit)
- **Script/txt downloaded in Step 2 uses standard system utilities to download and decode additional components (ex:** encoded PowerShell scripts/commands)
- **Scripts/commands run in Step 3 include the creation of scheduled tasks or other methods of establishing persistence (ex:** registry)
- Components established in Step 4 are final stage payloads that run at prescribed intervals and launch desired payloads/code, and as such, full malicious realization is established at this point

By some definitions, the above attack is all fileless, as we are only dealing with system functionality, PowerShell, and an RTF document to start it off. While we would disagree that it is not all fileless (the RTF is a file, and often the attackers write the PS to disk as files — not always, but often), it still illustrates the point. There is no obvious PE malware binary floating around here.

ATTACKING FIRMWARE AND HARDWARE VULNERABILITIES

Similar to platform agnostic attacks, another lucrative target is to attack the firmware/bios and hardware vulnerabilities of a device. These types of attacks are costly to build, however can grant longer-term persistence as well as cross-operating-system attacks. Attacks using firmware or hardware vulnerabilities are also worrisome for cloud service providers as they enable the compromise of machines that may be hosting more than one client instance, potentially leading to leakage and cross-contamination of data present on the cloud infrastructure. We are already seeing an increase in reports of firmware and hardware vulnerabilities and expect to see these low-level attacks gain popularity in the coming year.

Intel announced multiple firmware vulnerabilities in 2017. These vulnerabilities were present in low-level firmware components like Management Engine and Trusted Execution Engine. Some of these vulnerabilities enable bad actors to launch attacks, crash systems, and load and execute code outside OS visibility. So far, no known attacks have been found in the wild and updated firmware is available for download, however the firmware patch management within the enterprise environment is difficult and adoption is slow.

Recent analysis of firmware manufactures found that even the most basic firmware protections are lacking. It was found that over 3,000 firmware images across multiple hardware vendors were lacking firmware protections, leaving them open to attacks.

Also, in March 2017, Wikileaks exposed a description of the Der Starke implant which is a diskless EFI-persistent attack for MAC firmware. Der Starke enables covert network communications. Similarly, the Weeping Angel attacks, which target IoT devices like TVs, are within the realm of possibility for nation-state actors.

We anticipate that 2018 may present more real-world proof that attackers are looking to infect firmware and hardware vulnerabilities in order to gain persistence or breach data.

CASE STUDY_ RANSOMWARE

The company was in dire straits. Their environment was encrypted by ransomware. Sensitive information had been hijacked by cybercriminals. The hostile actors made no bones about their unsavory demands: *pay $3.2million in bitcoin or the stolen data hits the Dark Web and your company is ruined*. With no backups of the seized data and no reasonable way to meet the ransom demand, the company turned to Cylance for guidance.

The Cylance Incident Response team assessed the organization's technical environment then analyzed the tools, techniques, and procedures of their adversaries. Identifying how the attack succeeded and studying the threat group's processes gave the Cylance team valuable information. The responders used this knowledge to negotiate the ransom down by 75%. With the ransom reduced, Cylance turned its attention to the multiple vulnerabilities still present within the company's infrastructure. The ransomware attack used an exposed RDP connection, but there were other opportunities for improving system integrity as well.

At the conclusion of this case, Cylance made the following recommendations:

- Implement a regularly-scheduled backup plan
- Remove all RDP connections accessible from the Internet
- Conduct internal annual threat assessments

FILELESS VS. SCRIPT HEAVY ATTACKS

The definition of a fileless attack has been somewhat stretched over the last few years. From the purist perspective, there are true fileless attacks (Code Red, SQL Slammer), pseudo-fileless (Ramnit), and then what would really be script-heavy or script-reliant attacks. These days, all these subcategories tend to get lumped into one large fileless pile, which can be misleading.

Malware that stays fully memory-resident and does not rely on additional script execution would be completely fileless, however, the use of additional scripts (JavaScript, PowerShell, etc.) to enhance evasion and persistence enter the an a gray area of what should be called script-heavy attacks. An example would be Cerber's use of JavaScript/VB to download final payloads, or delay payload execution by calling an additional PowerShell script to then download and detonate.

The initial stages of attack, in the Cerber scenario, are not the full malware payload, but there are still files involved during these stages. The same holds true for attacks initiated via malicious documents with Macros/VB or other forms of embedded code. Fileless attacks are attractive to malicious actors for some of those very reasons (enhanced evasion, stealth, persistence), but we need to be careful how we use the term fileless so as to accurately describe what is really occurring during these attacks[3].

[3] https://www.youtube.com/watch?v=Tiv_-NLZzkc

K.O. – NOTHING TO RECOVER

Since the release of Shamoon in 2012, hostile attacks with the goal of destruction have been consistently emerging and causing havoc. These attacks are often used by hacktivists to make political statements or by nation states against each other. Once these destructive attacks execute, the road to recovery is long and costly, often requiring manual rebuilds of infrastructure. In the case of Shamoon, for example, the systems at Saudi Aramco went offline for about five months. In 2017, we saw major destructive attacks, some of which were attributed back to nation states.

In March 2017, Stonedrill malware was reported with disk-wiping capabilities that targeted Saudi Arabia, which has often been a target of disk-wiping malware. Following that, in June 2017, NotPetya gained notoriety and spread to many devices via leaked EternalBlue exploit. The main modus operandi was gaining profit as well as making the infected systems not bootable by infecting MBR. Ukraine was worst hit with this particular malware.

GhOstRAT malware, first discovered in 2001, was also reported to be redistributed via EternalBlue exploit, and contains disk-wiping capabilities as well. Additionally, 2017 also saw attacks like Brickerbot that scanned the Internet for Linux-based routers and was designed to destroy poorly secured devices, corrupting the device storage and deleted all the files on the device.

We anticipate that in 2018, we will see more of these debilitating attacks designed to disrupt services and cause losses to the target. In February 2018, we witnessed an attack dubbed Olympic Destroyer which was designed to disrupt the opening ceremony of the PyeongChang winter Olympic games. It contained a malicious component that essentially wiped files on the network shares. This attack was distributed via the EternalRomance exploit which was also part of the NSA tools leaked last year.

ATTRIBUTION: WHERE IT IS MATTERS / SHIFTING FOCUS

Attribution has always been a hot-button issue in the security industry. All too often, attribution is used as a tool to grab headlines or sway discussion away from the core issue at hand: why an attack was successful or why the campaign succeeded for so long. Cylance believes that it is far more critical to focus on the latter than dwell on the who question.

Does attribution have a place in the discussion? Absolutely. However, we need to focus. Attribution has definite and absolute academic value. There is value in the encyclopedic knowledge that comes with trending TTPs across different geos/actors and matching them with targets and campaigns over time. Attribution also has value to law enforcement and other entities that are directly tied to investigations or litigation stemming from an attack or breach. Beyond those contexts, the value becomes less clear.

Attackers knowingly seed misinformation and doubt in order to redirect possible attribution efforts. For example, attackers will often reuse tools or infrastructure that is known to be associated with other groups — i.e.: these two attacks came from server X and therefore must both be from the same group. That's an ultra-simple scenario, but not uncommon. Attackers will also go out of their way to obfuscate or relocate infrastructure so as to direct the public attribution story any way they see fit.

Public speculation of attribution with no proof or direct knowledge muddies the data/information pool. Non-provable speculation damages real investigations and also downgrades the aforementioned academic value of attribution.

Over the last few years, there are some strikingly-blatant and highly-visible attempts by malicious actors to redirect attention, and these are usually just meant to distract more than anything. Multiple references to the WhoIs Team (Dark Seoul) and the Guardians of Peace (Sony attack) are great examples that go back a few years, many of which are the more pedestrian examples of distractions employed by certain groups operating out of North Korea. The group called Lazarus has been known to embed different language strings or command structures in malicious binaries, so as to lead others to the wrong conclusions around country of origin. In 2017, we saw Lazarus attack financial targets, including multiple Polish banks, using a Russian-language command set, as well as embedded Russian-language strings in various associated binaries. All this was meant to misdirect attempts at attribution.

More recently, we saw this sort of manipulative behavior with the Olympic Destroyer malware targeting the infrastructure of the 2018 PyeongChang Olympics. This time, we saw an attack which appears to have originated out of Russia based on thorough analysis of all evidence to date, but aimed to direct the blame at North Korea's Lazarus. When taking into account all we know historically about Lazarus and/or DPRK and their history, TTPs, and modus operandi, this makes more sense, but it's still not definitive. Having said that, this is a great example where data is still being analyzed and monitored, investigations are ongoing, and all that is known needs to be taken into account before jumping to (and over-focusing on) inaccurate conclusions.

This whole scenario can get even more complicated when you factor in the ongoing use of Hive or similar tactics. With methods like this in use already, allowing for attackers to hide within legitimate infrastructure that is supported by a good trust model (ex: forged/fake SSL Certificates), it makes it that much more difficult to see though any attribution fog.

When any notable attack or breach occurs, there is an immediate tendency for press outlets to flood the planet with speculative attribution information. When this occurs, take a moment to put it into perspective. Attribution and intent are complex. The real focus should be on preventing these attacks, regardless of their origin.

As Malcolm Harkins, Cylance Chief Security and Trust Officer, stated, "In order to move forward and refocus our industry's energies on making attacks more difficult for malicious actors, we need to break free from our own obsessive infatuation with attribution. By investing all of our resources into finding out 'whodunnit', we get to play the victim card to minimize our own responsibilities and limit our liabilities. None of that helps the organizations that have been breached or the customers and clients who trusted those companies with their private information. Instead, we need to focus on WHY those intrusions were successful, so we can give attribution to the real source of the intrusion — the controls that failed which were sold to the breached parties by the security industry."

"WE NEED TO REFOCUS OUR INDUSTRY'S ENERGIES ON MAKING ATTACKS MORE DIFFICULT FOR MALICIOUS ACTORS RATHER THAN CHASING ATTRIBUTION."

CONCLUSION

The past year served as a stark reminder of the innovative prowess and destructive capabilities of global threat actors. Their tireless dedication to technical theft, inventive exploits, and creative methodology paid big dividends in 2017. Backed by state funding and armed with the latest knowledge and tools for compromising technology, threat actors are well positioned for continued success.

Cylance's examination of the attacks of 2017 provides an opportunity to reassess which security practices remain effective and which are no longer relevant. Many reliable security standbys still hold tremendous value, including:

- Keeping hardware and software updated
- Wisely managing access and permissions within the environment
- Strictly limiting and monitoring remote access
- Training personnel to identify attempts at social engineering and phishing
- Maintaining strong physical security over vulnerable infrastructure

Other security practices have been rendered obsolete by threat attributes like polymorphism and tactics utilized by fileless malware. These include signature-based antivirus solutions and blacklisting.

While 2017 highlighted the downfall of many time-honored security approaches, great advancements continue to be made throughout the cybersecurity industry. When threats go fileless, forward-looking threat responders turn to script controls and memory management to shut them down. When malware circumvents signature-based detection, visionary companies use artificial intelligence and machine learning to predict and prevent compromises.

As with all battles, knowledge is a key factor in achieving success. By sharing our knowledge and key findings for 2017, it is our hope that your organization may better prepare for the threats throughout 2018 and beyond.

CONTRIBUTORS

DATA ANALYSTS

Srinivasa Kanamatha
Danny Wu

THREAT RESEARCHERS/AUTHORS

Thom Ables
Steve Barnes
Bronson Boersma
Tom Bonner
Alex Hegyi
Shinsuke Honjo
Marta Janus
Aditya Kapoor
Tom Pace
Carolina Regalado
Jim Walter

EDITORS

Dan Ballmer
Brigitte Engel
Sally Feller
Anthony Freed
Natasha Rhodes
Steve Salinas
William L. Savastano
Jessica Vose

DESIGN

Sheri K. Audette
Drew Hoffman

CONTACT

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

20180427-0398