CYLANCE

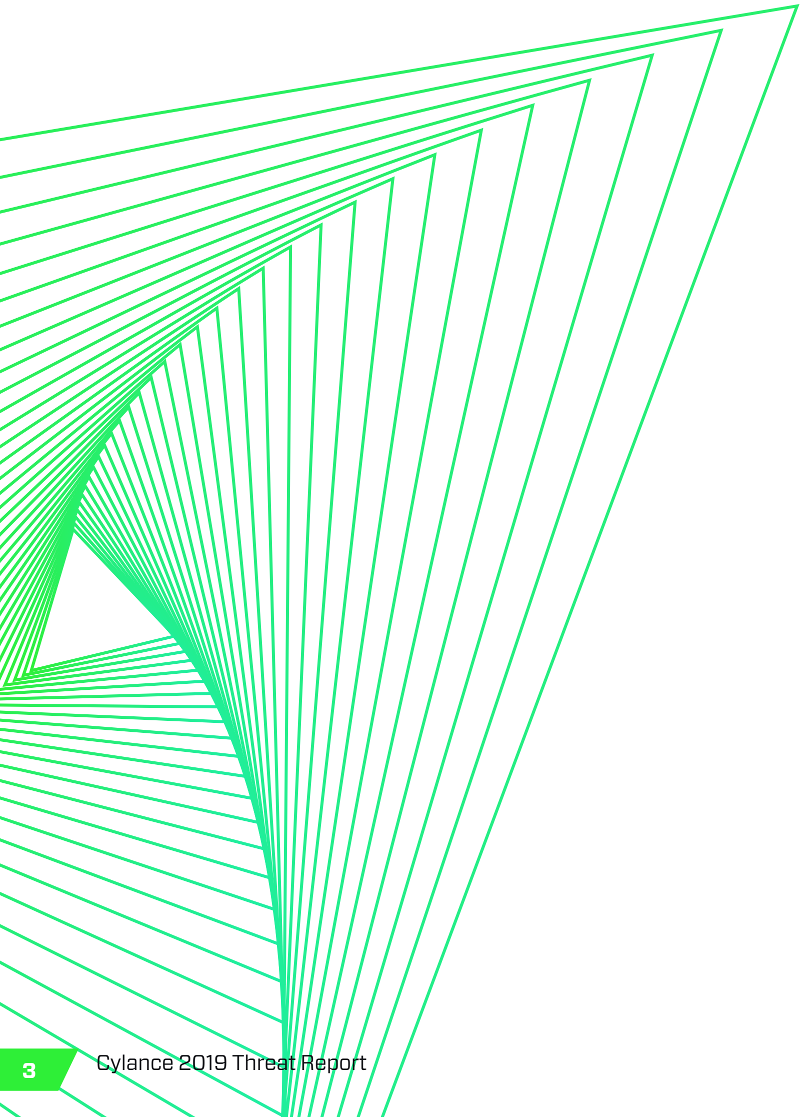
2019 THREAT REPORT

Contents

Executive Summary

In 2018, Cylance® observed a decline in overall ransomware attacks, an increase in malicious coinminers, and a marked evolution of popular threats like Emotet. Overall malware attacks rose by 10% as attackers continued to hone their tools, skills, and tactics to threaten Windows, macOS, and various IoT platforms.

Coinminers offer profit-driven threat actors certain advantages over ransomware, which Cylance believes were leading factors in their increase in popularity. First, they operate quietly by hijacking system processing resources for mining cryptocurrencies like Bitcoin, often without alerting the victim. Second, attackers can repurpose Coinhive – a tool intended to create alternative revenue streams for website owners – to install coinminers on victims' browsers without consent. This year's report offers some insight into why the combination of readily available tools, the ability to conduct discreet operations, and the chance to reap the benefits of hassle-free payouts made coinmining very popular among threat actors in 2018.



While ransomware attacks declined in popularity, and therefore in overall volume in 2018, they did remain a significant threat to the technology, consumer goods, and manufacturing industries according to Cylance data. Both PolyRansom and GandCrab ransomware ranked in Cylance's top ten Windows-based threats. Additionally, there is still ample room for improvement in technology and tactics to respond to ransomware as the data tells us the average industry ransomware response clocked in at 25 days in 2018. It's worth noting that though ransomware attack volume may have decreased in 2018, ransomware attack sophistication increased last year. You'll see this evidenced in Cylance's accounts of how ransomware played a role in the high-profile Lazarus Group attacks against Banco de Chile, and how ransomware families like Ryuk and UmbreCrypt were deployed by Emotet in 2018.

A heavily upgraded version of the Emotet banking trojan made a significant impact on the threat landscape in 2018. Threat actors implemented analysis awareness, multi-layered command-and-control (C2) encryption, brute-force credential attacks, and full-body email harvesting capabilities into Emotet. Upgraded Emotet also leverages DKIM controls to bypass spam controls, uses PDFs to trigger malicious links, and functions as a modular attack platform. The Emotet threat platform uses a dynamic infrastructure that regularly updates malicious documents and rotates encryption keys. Cylance dedicated a section of this year's report to Emotet, in part to outline how Emotet acts as a delivery agent for IcedID, Trickbot, Qakbot, and other threats in 2018.

In 2018, advanced persistent threat (APT) actors actively embraced tools and malware based on open source code like Mimikatz and HTran. The OceanLotus Group used customized backdoors and trojans like Remy, Roland, and Splinter in their campaigns against specific targets. They also used custom encryption keys to obfuscate communications with their C2 servers and to complicate analysis of their activities. Meanwhile, other threat groups like The White Company carried out complex and sustained attacks against the Pakastani Air Force. This year's report covers some of the basics you need to be aware of related to the new tactics and strategies deployed by these threat actors.

The Cylance 2019 Threat Report represents the company's piece of the overall cybersecurity puzzle. It details the trends observed and the insights gained, and the threats Cylance's consulting team, research team, and customers encountered over the past year. Cylance shares this report in the hope that you will put it to good use in our collective fight against the rising tide of cyber attacks worldwide.

A Look Back at Cylance's Successful Predictions from Last Year's Report

Firmware and Hardware Vulnerabilities: Last year's threat report stated: *"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."*

> On September 27, 2018, Lojax[1], the first UEFI rootkit was discovered in the wild.

Destructive Attacks: Last year's threat report stated: *"Since the release of Shamoon in 2012, hostile attacks with the goal of destruction have been consistently emerging and causing havoc . . . We anticipate that in 2018, we will see more of these debilitating attacks designed to disrupt services and cause losses to the target."*

> On December 12, 2018, a Shamoon variant attacked Italian oil services[2].

Methodology

Cylance provides security solutions that are focused on protecting endpoints and servers from being compromised by advanced threats. Using a lightweight agent on the endpoint, when a threat is detected, information about the event – including telemetry data – is transmitted through encrypted channels 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 and December 31, 2018.

What is Predictive Advantage (PA)?

Predictive Advantage is a unit of measurement applied to security solutions that measures *"how far into the future its protection is seen to reach. For example, if it protected against a threat that was created one year after the product was built, then it would have a predictive advantage (PA) of 12 months."*[3] Cylance's malware PA scores reflect the time elapsed between the creation of a Cylance security model and the first documented emergence of that detected threat type.

Why does PA matter? The PA unit of measurement provides insight into how advanced the machine learning training was for a particular security solution model. A model that can block a threat that arrives on the scene 24 to 30 months after that model was introduced can be considered a very robust and expertly trained model. Cylance invites you to learn more about this important method for evaluating AI-driven security solutions by reading the SE Labs test and report on the topic.

[1] https://arstechnica.com/information-technology/2018/10/first-uefi-malware-discovered-in-wild-is-laptop-security-software-hijacked-by-russians/

[2] https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA

[3] https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SELabsPredictiveMalwareResponseTestMarch2018Report.pdf?kui=kMzpDSif2OljDv7c6GwpIA

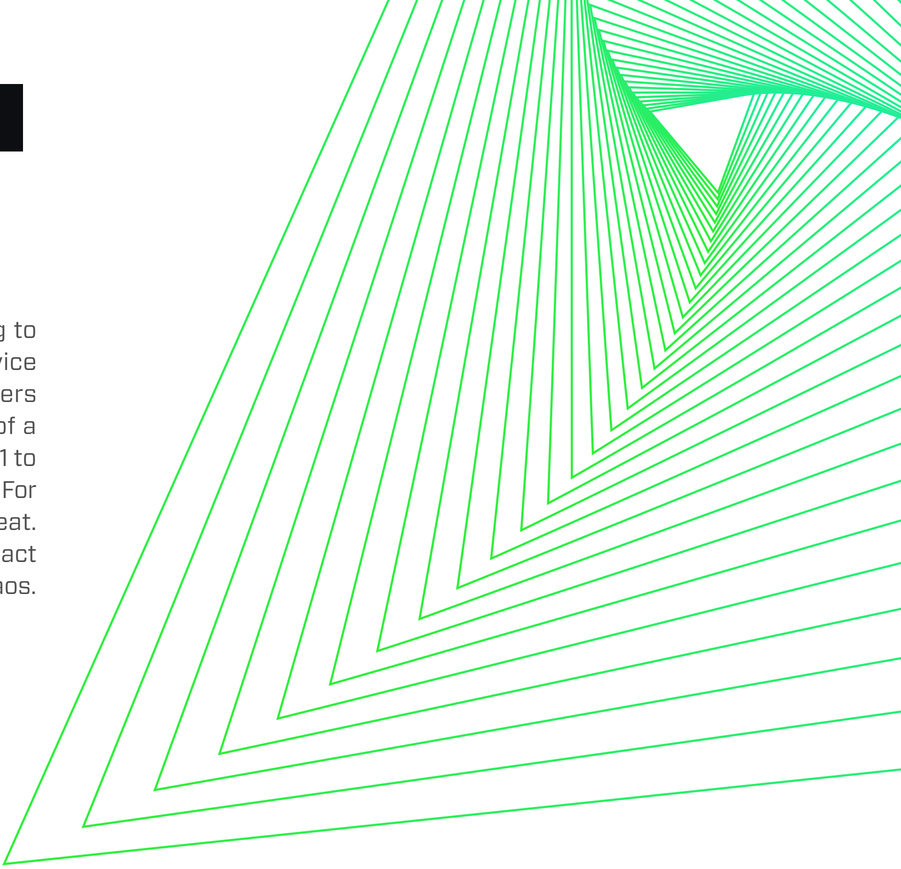
New To This Year's Report: Execution, Identity, and DoS (E:I:D) Ratings

In our 2019 Report, Cylance rates each threat according to three categories: execution, identity, and denial of service (availability). The E:I:D rating is intended to assist readers with quickly identifying and understanding the severity of a threat. The cumulative rating for each threat ranges from 1 to 10 with higher numbers representing more serious threats. For example, an E:I:D rating of 1 represents a low severity threat. An E:I:D rating of 10 would signify a high severity, high impact threat that can lead to system failures and widespread chaos.

Execution (Integrity): This rating is a qualitative measure of the overall attack execution complexity. It includes measurements like uniqueness/innovation, the level of user interaction required for the attack, and the difficulty involved in remediating a successful attack.

Identity (Confidentiality): This rating is a qualitative measure of how severely a threat impacts identity data. Threats have numerous ways of stealing identity information. Some only steal environmental artifacts while others may focus solely on harvesting PII or IP information. Some threats only impact financial data, while other threat families like backdoors or bots feature key-stroke logging capabilities that may or may not be utilized in an attack. A high identity rating indicates a threat that excels at identity-stealing activities.

Denial of Service (Availability): This rating qualitatively measures the amount of downtime a threat imposes on users and machines, primarily through resource denial resulting in lost productivity. For example, a coinminer's sole purpose is to utilize system resources to mine cryptocurrencies. Each resource stolen by the coinminer is one denied for legitimate business use. A ransomware or a disk wiper have the capability to deny data, or even an entire system, to victims. Some threats can deny network availability or participate in botnets that are used for distributed denial-of-service (DDoS) attacks. The denial of service rating indicates how likely a threat is to impact daily operations and disrupt enterprise networks.



Key Findings

- **Most popular infection vector:** Phishing/email.
- **Malware attack volume increase:** Cylance customers experienced a 10% overall increase in malware attacks in 2018.
- **Top cyber attack industry targets:** The top three targets among Cylance customers for cyber attacks were the food industry, logistics industry, and non-profit organizations.
- **Top ransomware industry targets:** The technology sector was the primary target for ransomware attacks in 2018. Consumer goods and manufacturing placed second and third.
- **The rise of coinminers:** Coinminer detections increased by 47%.
- **Coinminer industry targets:** The top three targets of coinminers were the food industry, technology sector, and professional services.
- **OS X attacks:** OS X was targeted by coinminers, adware, ransomware, and trojans.
- **IoT Attacks:** The Mirai codebase is still being leveraged to launch attacks against IoT devices.

TOP MALWARE

This section provides a short summary of the top threats reported by Cylance customers in 2018. Additionally, Cylance provides a risk analysis of each threat, lists the industries they impacted the most, and references the number of variants Cylance products prevented from running as the activity measurement of a threat family.

Top 10 Windows Threats

The top 10 Windows threats reported by Cylance customers in 2018 were:

1. MyWebSearch
2. InstallCore
3. PolyRansom
4. Neshta
5. Upatre
6. Ramnit
7. Emotet
8. GandCrab
9. Qukart
10. Ludbaruma

MyWebSearch

Number of Variants:	High
Cylance Predictive Advantage:	782 days
EID Rating:	1 (E:1 I:0 D:0)
Top Industries Impacted:	Healthcare, manufacturing, and professional services

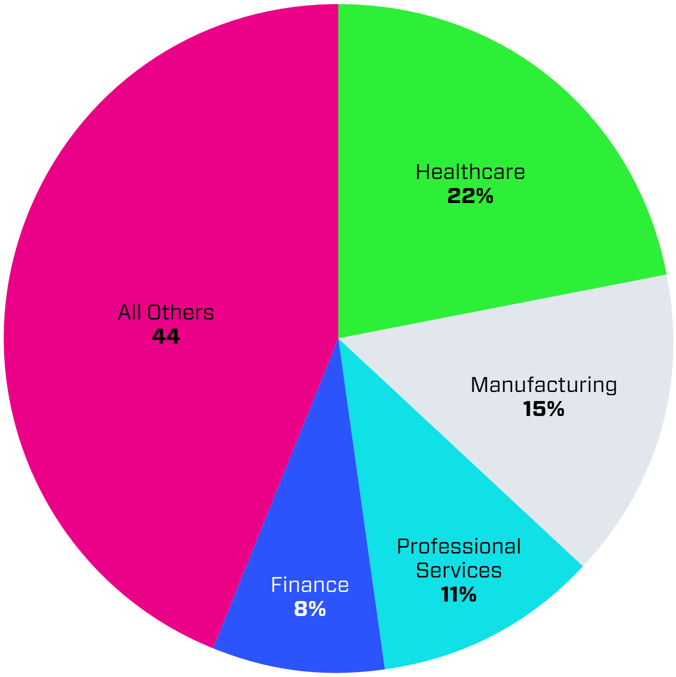
MyWebSearch is a prolific nuisance that poses only marginal risks to infrastructure. It is a browser hijacker that typically modifies default browser settings without requiring human interaction.

The browser modifications generally display advertisements or influence search operations. Obvious signs of a MyWebSearch infection include the changing of a browser's default home page or preferred search engine. MyWebSearch is often bundled with freeware and may use the signature of legitimate software to bypass security checks.

MyWebSearch impacted the healthcare and manufacturing industries more than any other, though it impacted a wide swath of different industries across the board.

Cylance collected over 17,000 variants of MyWebSearch in the past year. The MyWebSearch family likes to rotate the hashes to avoid detection. More than 88% of the hashes found infected 10 or fewer devices. This makes this threat a prime candidate for prevention. In calculations across a random sampling of the MyWebSearch data, Cylance was able to prevent this family at least 782 days in advance.

MyWebSearch Target Breakdown By Industry



InstallCore

Number of Variants:	Medium
Cylance Predictive Advantage:	717 days
EID Rating:	1 (E:1 I:0 D:0)
Top Industries Impacted:	Consumer goods, education, and government

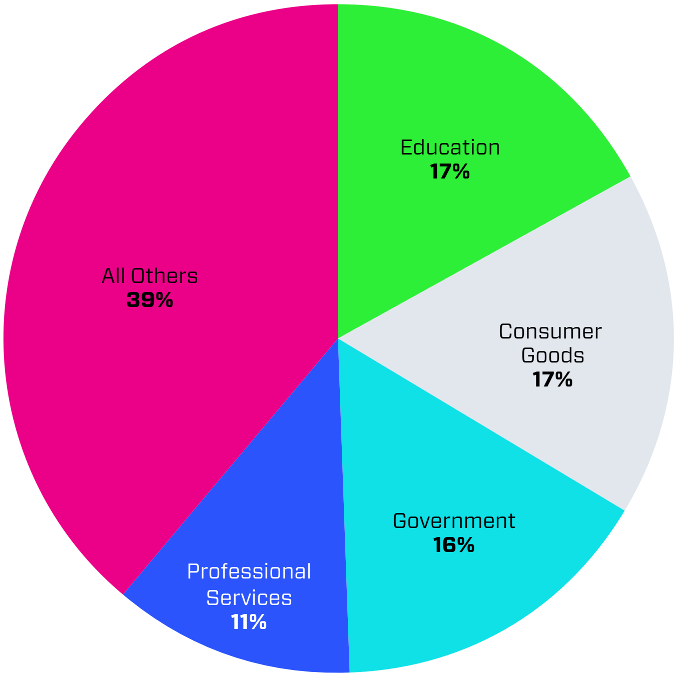
InstallCore bundles legitimate software with unwanted products from their advertising partners.

InstallCore primarily affected the consumer goods, education, and government sectors in 2018.

InstallCore may use a legitimate signature from whichever primary software it installs. This signature borrowing allows InstallCore to operate without the host system raising red flags. The unrequested software will ask for user permission before installing.

Over 92% of InstallCore binaries were found on 10 devices or less, which shows that InstallCore likes to rotate its hashes with each bundled product. From a prevention standpoint, every variant that Cylance saw was prevented at least 717 days in advance, rendering them harmless to Cylance customers.

InstallCore Target Breakdown By Industry



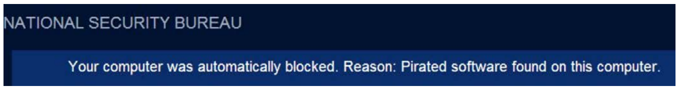
PolyRansom

Number of Variants:	High
Cylance Predictive Advantage:	862 days
EID Rating:	4 (E:2 I:0 D:2)
Top Industries Impacted:	Technology, government, finance, and manufacturing

PolyRansom, also known as Virlock and Nabucur, was a major threat by volume in 2018 and shows no signs of slowing down. It is one of the more prolific ransomware families and one of the most complex.

PolyRansom primarily targeted the technology industry. Government organizations were also a secondary, but significant, target of this malware.

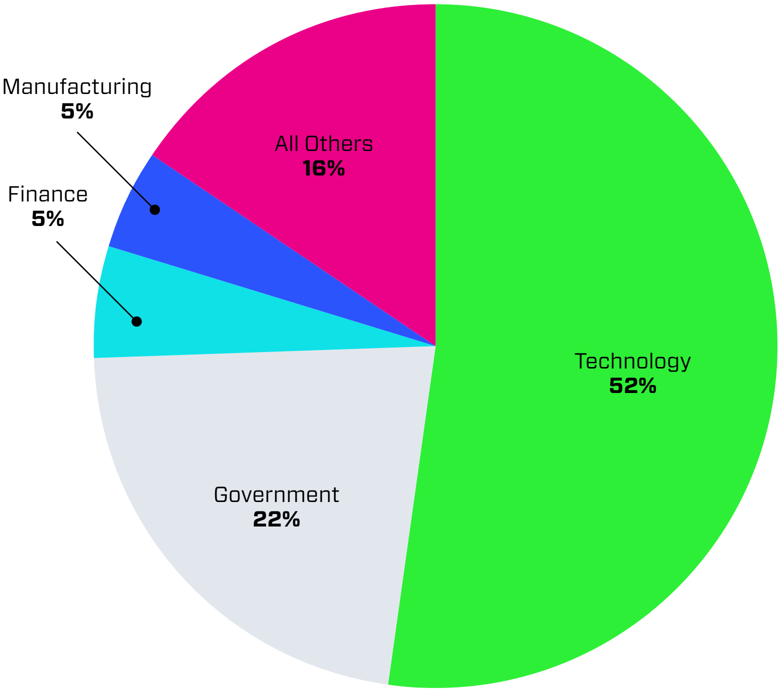
First observed in 2014 as Virlock, PolyRansom debuted a screen-locking functionality.


NATIONAL SECURITY BUREAU

Your computer was automatically blocked. Reason: Pirated software found on this computer.

PolyRansom displays a message falsely claiming to be authored by the "National Security Bureau". It directs users to make a bitcoin payment to avoid a warrant being issued for their arrest and possible imprisonment.

PolyRansom Target Breakdown By Industry



The malware generates new copies of itself, dramatically complicating the process of analysis and reverse engineering. Fortunately, the quality of PolyRansom's encryption methods is inconsistent. Decryption tools have had some success recovering files from infected systems.

PolyRansom decrypts the minimal amount of code needed to operate, subsequently re-encrypting these code chunks as it continues its routine. This re-encryption of code alters the malware's original binary image thereby changing its file hash. This technique, called polymorphism, allows PolyRansom to evade signature-based threat detection.

To propagate, PolyRansom injects itself into other files then creates a weaponized executable or self-extracting RAR. This process allows PolyRansom to spread without being a true worm. Users launching the infected executables will cause the process to repeat, thereby spreading the malware across file shares, cloud-based services, and other collaborative venues.

PolyRansom contains other robust mechanisms for anti-analysis. These include anti-VM features, a customized packer, and the use of multiple packed/encrypted layers. PolyRansom sets the hidden attribute on files and directories and uses .bat, .vbs, and .js scripting to avoid detection.

PolyRansom is delivered via standard methods such as phishing and web-based attacks.

Neshta

Number of Variants:	Medium
Cylance Predictive Advantage:	874 days
EID Rating:	6 (E:2 I:3 D:1)
Top Industries Impacted:	Manufacturing, finance, and consumer goods

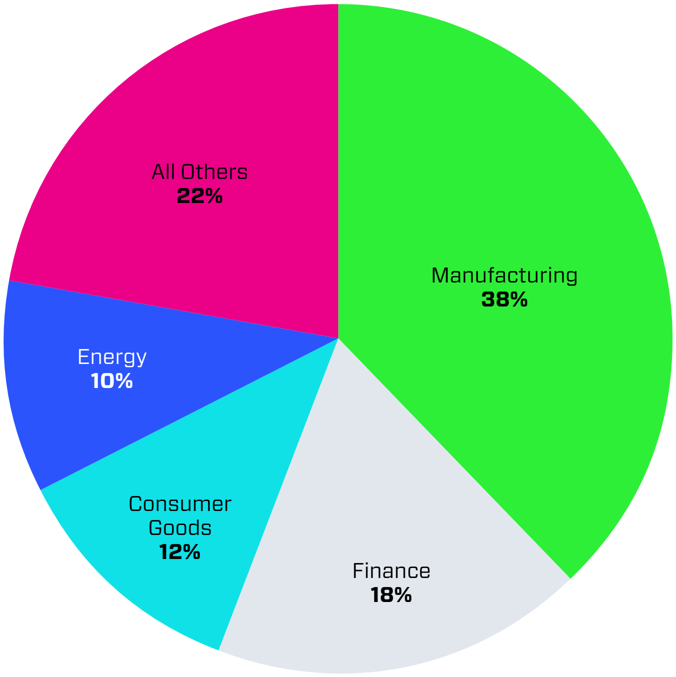
Neshta is an older file infector that is still prevalent in the wild. It prepends malicious code to infected files.

Neshta predominantly targeted the manufacturing industry. The finance, consumer goods, and energy sectors were also significant targets of this malware in 2018.

Neshta has been observed since 2003, and has been previously associated with BlackPOS malware[4]. This threat is commonly introduced into the environment by being unintentionally downloaded or dropped by other malware. It infects Windows executable files and may attack network shares and removable storage devices.

To achieve persistence, Neshta renames itself to svchost.com then modifies the registry so it runs each time an .exe file is launched. Neshta is known to collect system information and use POST requests to exfiltrate data to attacker-controlled servers.

Neshta Target Breakdown By Industry



[4] https://threatvector.cylance.com/en_us/home/the-abcs-of-apts.html

Upatre

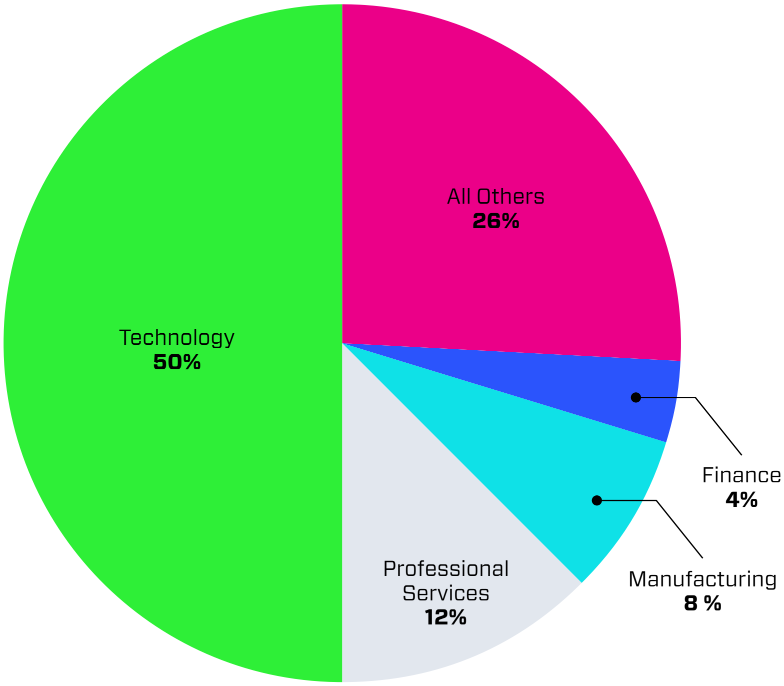
Number of Variants	Medium
Cylance Predictive Advantage:	875 days
EID Rating:	4 (E:1 I:2 D:1)
Top Industries Impacted:	Technology, professional services, and manufacturing

Upatre is a malicious downloader capable of delivering destructive payloads like Dyre and Zbot/Zeus to target systems.

Upatre overwhelmingly targeted technology organizations in 2018. Professional services were also selected for Upatre attacks, though they ranked a distant second.

Upatre often arrives as a malicious email attachment. It has been associated with several botnets and exploit kits. Upatre may display the icon of a recognized file or application to lure users into clicking on it, and can update itself or expand its functionality by connecting to C2 servers and downloading additional code.

Upatre Target Breakdown By Industry



Ramnit

Number of Variants:	High
Cylance Predictive Advantage:	858 days
EID Rating:	6 (E:2 I:3 D:1)
Top Industries Impacted:	Manufacturing, professional services, and media

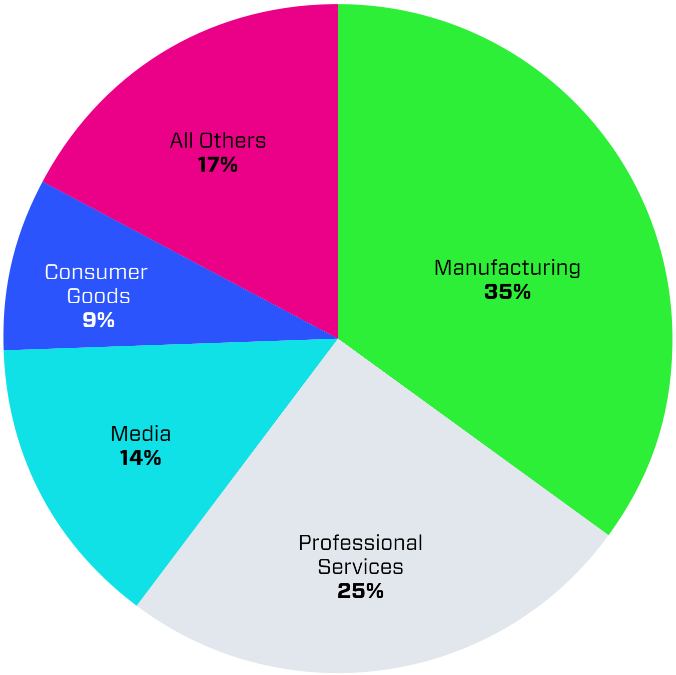
First discovered in 2010, Ramnit was originally known for infecting Windows Portable Executables such as .exe, .scr, .dll files, and HTML documents.

The manufacturing and professional service industries were both significant targets of Ramnit in 2018. Media companies also received heavy attention from this malware.

Ramnit historically spreads through removable devices such as USB keys and across shared locations such as network drives. A new variant of Ramnit has borrowed multiple capabilities from the leaked source code of the Zeus banking trojan, allowing it to use exploits to propagate via networks. The upgraded Ramnit can steal sensitive information and more closely resembles a full-blown banking trojan.

The Ramnit framework has recently been in the news as it was reportedly involved in proliferating another malware called Ngioweb. Additionally, early in 2018, Ramnit was involved in data stealing operations outside pure banking attacks. It was discovered trying to steal sensitive information from the users visiting e-commerce sites.

Ramnit Target Breakdown By Industry



Emotet

Number of Variants:	High
Cylance Predictive Advantage:	816 days
EID Rating:	5 (E:1 I:3 D:1)
Top Industries Impacted:	Government, healthcare, and non-profit

Emotet, a variant of the Feodo trojan family, first emerged in 2014 as a threat designed to steal banking credentials and other sensitive information. It is most often propagated by phishing emails containing an infected document or malicious website link.

If a malware can be described as egalitarian in its selection of targets, Emotet qualifies. The utility and effectiveness of Emotet is such that it was leveraged widely against government, non-profits, healthcare, and logistics organizations.

Emotet is usually delivered by a Microsoft Word file embedded with malicious macros. These malicious macros are heavily obfuscated. When executed, the malicious code runs PowerShell commands to download a malware payload from one of several preconfigured websites.

Once Emotet is active, it copies itself to a local file directory and implements its persistence mechanisms. Cylance invites you to take advantage of the wealth of further detail on the expanded capabilities and recent activity of Emotet in The Year of Emotet section further on in this year's report.

GandCrab

Number of Variants:	Medium
Cylance Predictive Advantage:	795 days
EID Rating:	3 (E:1 I:0 D:2)
Top Industries Impacted:	Construction, finance, manufacturing, and technology

GandCrab is an actively maintained ransomware. It is offered by ransomware-as-a-service providers and saw at least five major version releases in 2018.

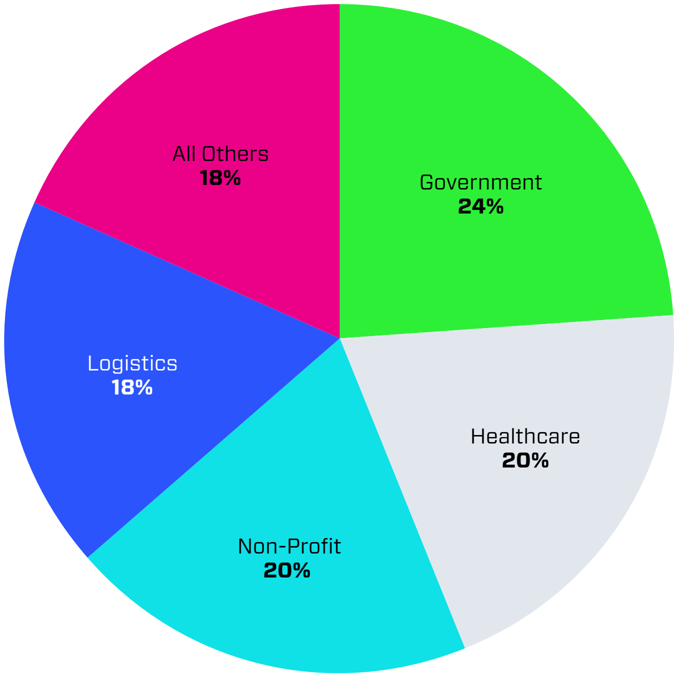
GandCrab primarily targeted the construction, finance, manufacturing, and technology sectors in 2018.

GandCrab versions may be identified by the file extensions appended to encrypted files:

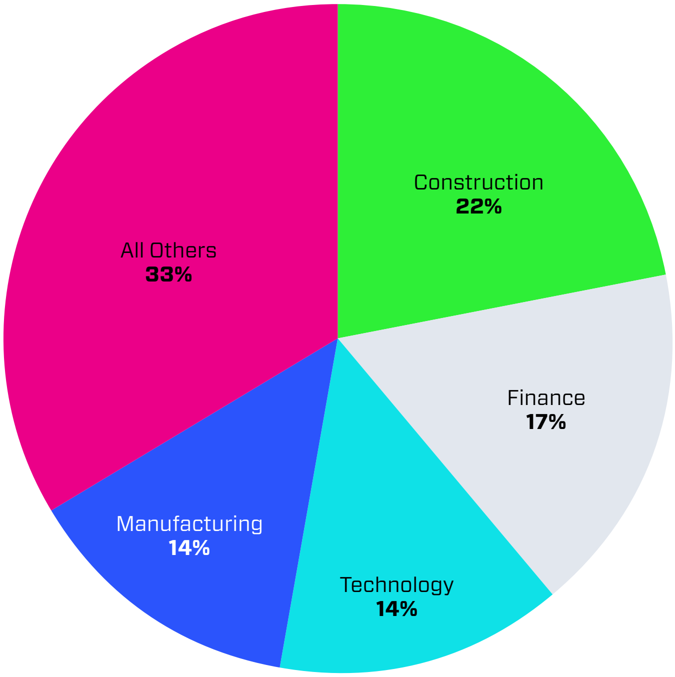
- Version 1 – filename.GDCB
- Version 2 – filename.CRAB
- Version 3 – filename.CRAB
- Version 4 – filename.KRAB
- Version 5 – filename.<random>

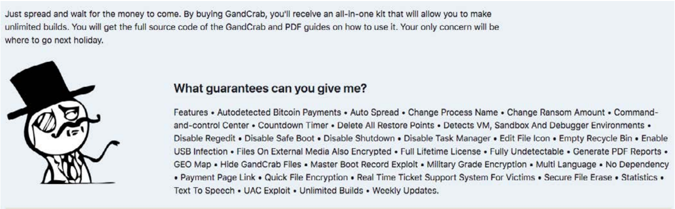
As of the release date of this report, pricing for GandCrab ranges between $500 (Standard) and $1,200 (Premium). Subscriptions include unlimited builds of ransomware binaries, weekly updates, and unique management panel access.

Emotet Target Breakdown By Industry



GandCrab Target Breakdown By Industry

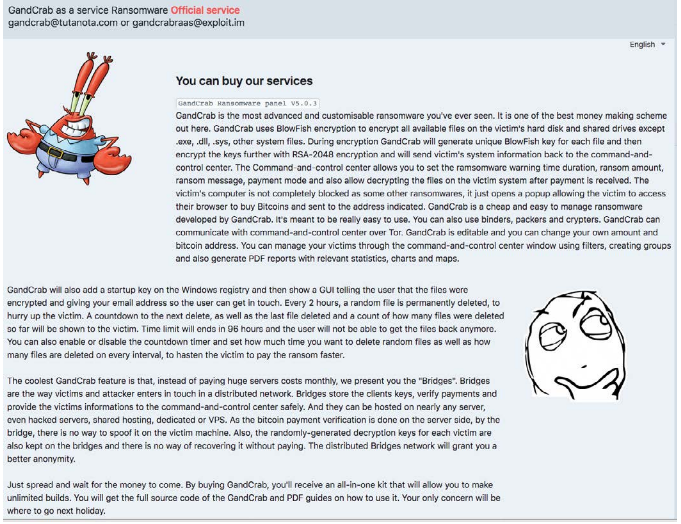




Just spread and wait for the money to come. By buying GandCrab, you'll receive an all-in-one kit that will allow you to make unlimited builds. You will get the full source code of the GandCrab and PDF guides on how to use it. Your only concern will be where to go next holiday.

What guarantees can you give me?

Features • Autodetected Bitcoin Payments • Auto Spread • Change Process Name • Change Ransom Amount • Command-and-control Center • Countdown Timer • Delete All Restore Points • Detects VM, Sandbox And Debugger Environments • Disable Regedit • Disable Safe Boot • Disable Shutdown • Disable Task Manager • Edit File Icon • Empty Recycle Bin • Enable USB Infection • Files On External Media Also Encrypted • Full Lifetime License • Fully Undetectable • Generate PDF Reports • GEO Map • Hide GandCrab Files • Master Boot Record Exploit • Military Grade Encryption • Multi Language • No Dependency • Payment Page Link • Quick File Encryption • Real Time Ticket Support System For Victims • Secure File Erase • Statistics • Text To Speech • UAC Exploit • Unlimited Builds • Weekly Updates.



GandCrab as a service Ransomware Official service
gandcrab@tutanota.com or gandcrabraas@exploit.im

You can buy our services

`GandCrab Ransomware panel V5.0.3`

GandCrab is the most advanced and customisable ransomware you've ever seen. It is one of the best money making scheme out here. GandCrab uses BlowFish encryption to encrypt all available files on the victim's hard disk and shared drives except .exe, .dll, .sys, other system files. During encryption GandCrab will generate unique BlowFish key for each file and then encrypt the keys further with RSA-2048 encryption and will send victim's system information back to the command-and-control center. The Command-and-control center allows you to set the ramsomware warning time duration, ransom amount, ransom message, payment mode and also allow decrypting the files on the victim system after payment is received. The victim's computer is not completely blocked as some other ransomwares, it just opens a popup allowing the victim to access their browser to buy Bitcoins and sent to the address indicated. GandCrab is a cheap and easy to manage ransomware developed by GandCrab. It's meant to be really easy to use. You can also use binders, packers and crypters. GandCrab can communicate with command-and-control center over Tor. GandCrab is editable and you can change your own amount and bitcoin address. You can manage your victims through the command-and-control center window using filters, creating groups and also generate PDF reports with relevant statistics, charts and maps.

GandCrab will also add a startup key on the Windows registry and then show a GUI telling the user that the files were encrypted and giving your email address so the user can get in touch. Every 2 hours, a random file is permanently deleted, to hurry up the victim. A countdown to the next delete, as well as the last file deleted and a count of how many files were deleted so far will be shown to the victim. Time limit will ends in 96 hours and the user will not be able to get the files back anymore. You can also enable or disable the countdown timer and set how much time you want to delete random files as well as how many files are deleted on every interval, to hasten the victim to pay the ransom faster.

The coolest GandCrab feature is that, instead of paying huge servers costs monthly, we present you the "Bridges". Bridges are the way victims and attacker enters in touch in a distributed network. Bridges store the clients keys, verify payments and provide the victims informations to the command-and-control center safely. And they can be hosted on nearly any server, even hacked servers, shared hosting, dedicated or VPS. As the bitcoin payment verification is done on the server side, by the bridge, there is no way to spoof it on the victim machine. Also, the randomly-generated decryption keys for each victim are also kept on the bridges and there is no way of recovering it without paying. The distributed Bridges network will grant you a better anonymity.

Just spread and wait for the money to come. By buying GandCrab, you'll receive an all-in-one kit that will allow you to make unlimited builds. You will get the full source code of the GandCrab and PDF guides on how to use it. Your only concern will be where to go next holiday.

GandCrab often arrives as a malicious email attachment. It is also distributed by a number of exploit kits including GrandSoft EK and RIG EK[5].

QUKART

Number of Variants:	Low
Cylance Predictive Advantage:	801 days
EID Rating:	7 (E:2 I:3 D:2)
Top Industries Impacted:	Technology, professional services, and healthcare

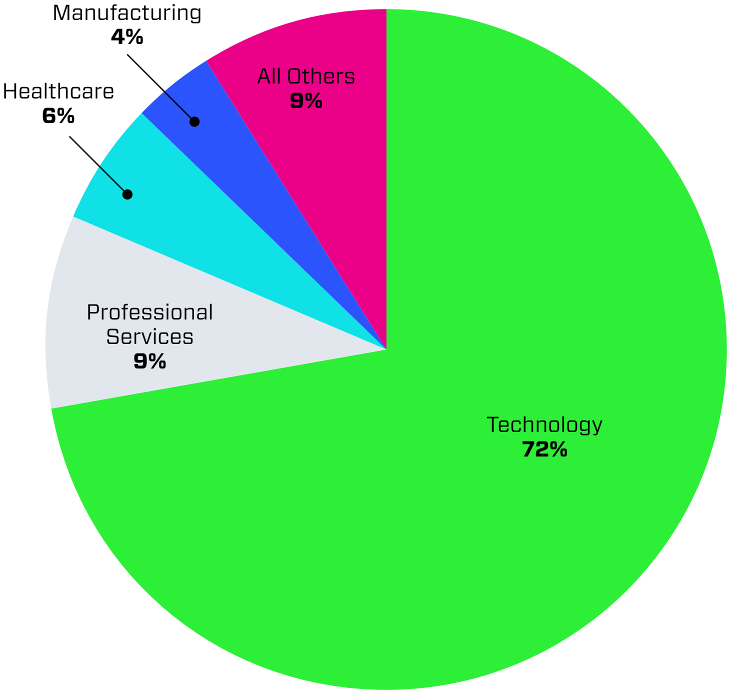
QUKART, also known as BERBEW and PADODOR, is a password-stealing trojan. It is designed to monitor web browsers and harvest credential information when victims access login pages.

QUKART malware largely affected the technology sector, which accounted for 72% of reported attacks. No other industry received double-digit attention from this malware, though professional services received 9% and healthcare received 6%.

QUKART is usually delivered by spam campaigns, through drive-by-downloads, through exploit kits, or via downloaders.

Some variants of QUKART can inject fake fields into login pages to steal credit card information, CVV, PIN, and other information. The trojan creates HTML files on the victim machine to store harvested credential information. QUKART can act as a proxy server for relaying malicious traffic or to conduct denial of service attacks. This trojan is polymorphic.

Qukart Target Breakdown By Industry



[5] https://threatvector.cylance.com/en_us/home/cylance-vs-GandCrab-ransomware.html

Ludbaruma

Number of Variants:	Low
Cylance Predictive Advantage	800 days
EID Rating:	6 (E:2 I:2 D:2)
Top Industries Impacted:	Manufacturing, technology, and education

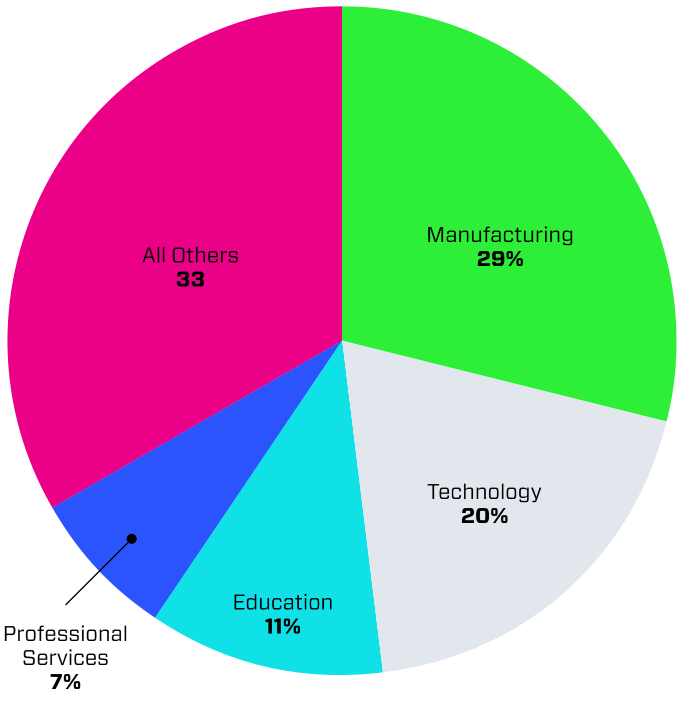
Ludbaruma, also known as Rontokbro and Brontok, is a mass mailer worm written in VisualBasic. This worm, first identified more than 10 years ago, has resurfaced through many variants over the years.

Ludbaruma primarily focused on the manufacturing and technology sectors in 2018. Educational organizations placed a distant third.

Ludbaruma harvests email accounts from address books, email messages, and certain documents on the victim's machine. The malware uses its own SMTP engine to send email messages with infected attachments to harvested addresses. Ludbaruma can also infect removable media and network shares.

Ludbaruma disables the registry tool, task manager, command prompt, folder option, and system restore on the target machine. If the worm encounters certain strings, including names of security vendors or words suggesting it has been detected, it will reboot the system. Ludbaruma was less active in 2018 than in past years, but still ranks as a top ten threat within the Cylance ecosystem.

Ludbaruma Target Breakdown By Industry



Top 5 OS X Threats

This year, Cylance's report also includes OS-X-specific threats encountered by a significant portion of users. The top five OS X malwares are:

- Cimpli
- Coinminer
- Flashback
- KeyRanger
- MacKontrol

Cimpli

EID Rating:	1 (E:1 I:0 D:0)

Cimpli is adware written for OS X that automatically displays unwanted advertisements. While adware is not particularly destructive, it is an annoyance and can impact user productivity. Cimpli installs in the Application Support folder and maintains persistence via LaunchAgents. This malware may download and install other malware families like Bundlore and Vsearch. Cimpli was one of the most common OS X malware infections detected in the Cylance ecosystem in 2018.

CoinMiner

EID Rating:	3 (E:1 I:1 D:1)

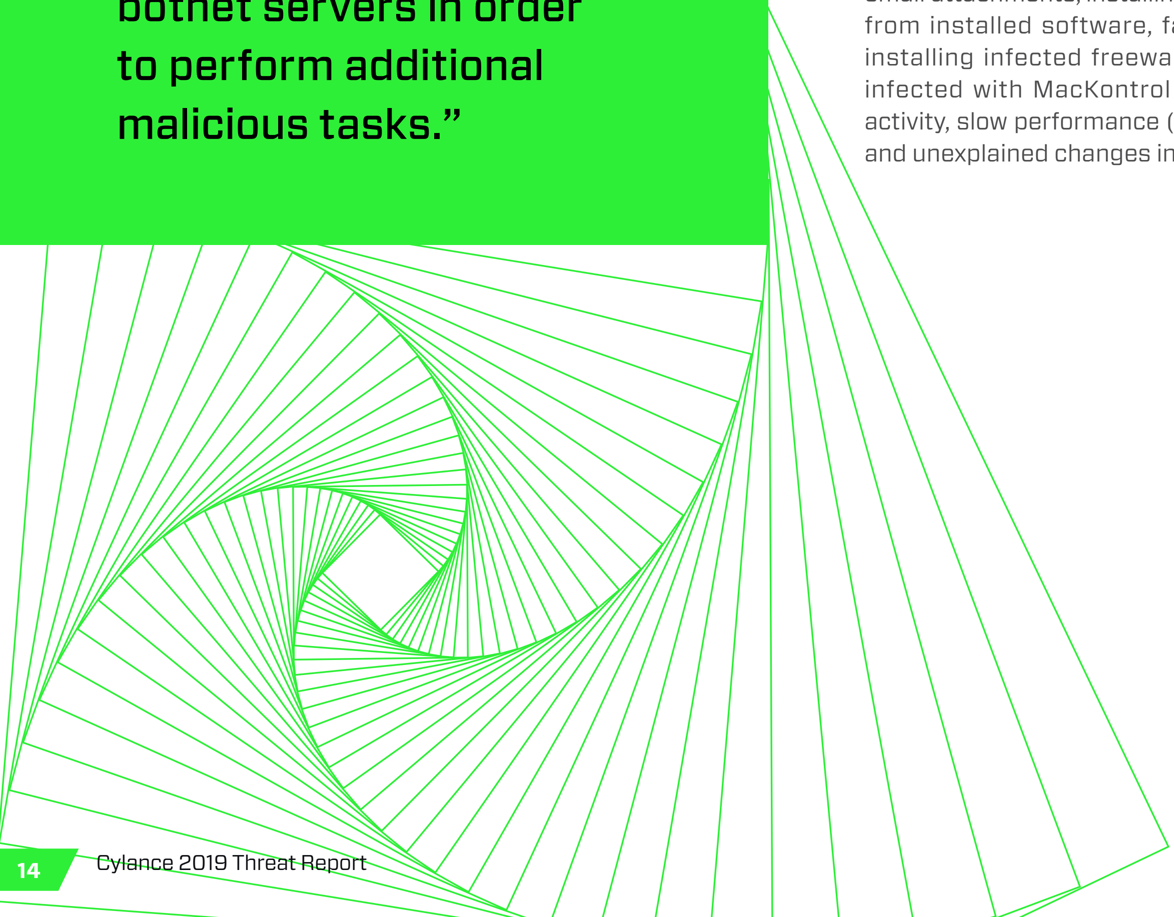
CoinMiner is installed via a dropper, like a fake flash player update. The most recent variant found in 2018 used XMRig to mine cryptocurrency. CoinMiner malware installs a launcher named pplauncher. This file is located at /Library/Application/Support/pplauncher/pplauncher. The malware uses a LaunchDaemon called *com.pplauncher.plist* to maintain persistence on the target system. The LaunchDaemon is written in Golang and compiled for MacOS. The launcher performs two simple functions, installing an older version of XMRig (version 2.5.1.) and beginning the mining process. The malicious mining process is named mshelper, a likely attempt to disguise itself as a Microsoft helper process.

Flashback

EID Rating:	3 (E:1 I:2 D:0)

The Flashback trojan targets Macs running an older version of Java Runtime. It installs from a malicious webpage. Flashback alerts victims that their flash or Java is out of date and requires updating. When users click the fake flash .dmg, which in some cases will update the software, the malware payload is installed. Flashback creates a file in /Applications/Safari.app/Contents/Info LSEnvironment or ~/.MacOSX/environment DYLD_INSERT_LIBRARIES. Once active, Flashback searches for installed antivirus applications then generates a list of botnet control servers. The malware communicates with the botnet servers in order to perform additional malicious tasks.

> “Once active, Flashback searches for installed antivirus applications then generates a list of botnet control servers. The malware communicates with the botnet servers in order to perform additional malicious tasks.”



Keyranger

EID Rating:	5 (E:2 I:1 D:2)

Keyranger is OS X ransomware that was first found in 2016 embedded in a signed Transmission torrenting application. At that time, Keyranger was available for download via hxxps://download.transmissionbt.com/files/Transmission-2.90[.]dmg. Since the malware was signed with a valid Mac app development certificate, it was able to bypass Apple’s Gatekeeper protection. Once installed, Keyranger waits three days before connecting with C2 servers over Tor. The malware is capable of encrypting roughly 300 different file types and begins the encryption process after connecting to the C2 servers. Encrypted files will have a .encrypted file extension added. To avoid detection, Keyranger disguises itself as an .RTF file named General.rtf and copies itself to the ~/Library/kernel_service directory.

MacKontrol

EID Rating:	7 (E:1 I:3 D:3)

MacKontrol is an OS X backdoor trojan with wide-ranging capabilities. It can handle remote access connections, perform DDoS attacks, capture keyboard inputs, delete files, and terminate processes. Once active, MacKontrol connects to a remote server to receive further instructions. The malware maintains persistence through the use of LaunchAgents on the infected computer. MacKontrol malware is commonly encountered through malicious websites, opening infected email attachments, installing fake updates claiming to come from installed software, fake video players and codecs, installing infected freeware, and torrent sites. Systems infected with MacKontrol may display unusual network activity, slow performance (due to high CPU or RAM usage), and unexplained changes in Safari browser settings.

APT TRENDS IN 2018

Cylance monitored a number of advanced persistent threat (APT) campaigns throughout 2018 and observed several notable trends.

Tools and Malware Based on Open Source Code

Cylance observed a visible shift among threat actors towards adapting publicly available code as an alternative to developing their own attack platforms. This approach saves attackers time and effort while protecting their anonymity by making the attribution process more difficult.

The Powersploit/Metasploit frameworks and Cobalt Strike Beacon remained popular, but Cylance noted an increase in the number of open source hacking tools used by several APTs. These tools include popular GitHub projects, such as Mimikatz (a credentials stealer) and HTran (a connection proxy tool), and lesser known tools. APTs have access to numerous utilities like port scanners, network sniffers, and password bruteforcers whose code appears on online blogs and forums.

Cylance also observed a rise in the prevalence of open source backdoors in APT campaigns. QuasarRAT, a remote administration tool written in .NET, has seemingly become a permanent part of the MenuPass/APT10 toolset. The Chinese PcShare backdoor was observed in a highly targeted campaign by another actor. These backdoors are often dropped during the early phases of the attack life cycle until a more bespoke solution can be deployed..

Bespoke Malware

Many threat actors tend to use sophisticated and customized backdoors to maintain persistence in an environment. These backdoors are often designed based on information gleaned by the threat actors during reconnaissance. They are usually deployed in the advanced stages of the attack cycle.

Backdoors may implement anti-detection tricks and bypass mechanisms tailored specifically to the software used on the targeted machine. They may also include a set of functionalities specific to the victim's profile. A good example are the backdoors used in recent OceanLotus campaigns. These backdoors use malicious DLLs to mimic the names and exports of a legitimate library found in the targeted environment. By using DLL-sideloading techniques, the backdoor binary gets loaded to the memory by one of the victim's benign applications.

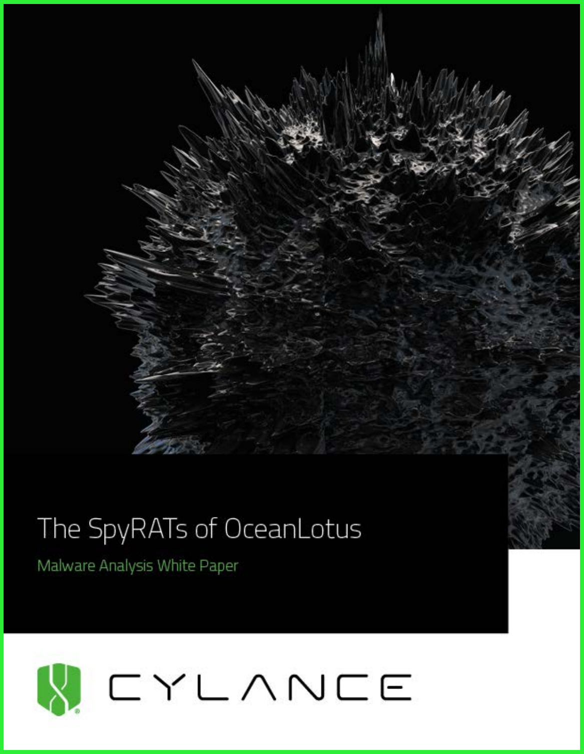
As modular architecture is becoming increasingly common, the foothold backdoors tend to be small and compact. Most of their malicious functionality relies on separate plugins, which can be immediately deleted from the system after being used. This allows the attackers to maintain basic persistence while keeping the digital footprint down to minimum.

OceanLotus Group

During an incident response investigation conducted late in 2017, Cylance threat researchers uncovered several backdoors deployed by the OceanLotus Group, which is also known as APT32 and Cobalt Kitty. Further efforts to analyze the tactics, techniques, and procedures of this threat group resulted in some significant revelations.

Cylance observed the OceanLotus Group using obfuscated Cobalt Strike Beacon payloads to perform C2 and PowerShell one-liners to download and deploy malware. They leveraged obfuscators and reflective PE/shellcode loaders from exploit kits (including MSFvenom, Veil, and DKMC) to achieve fileless attack capabilities. Their attacks were highly tailored to specific targets and included the development of remote access trojans Roland, Remy, and Splinter.

For full details read Cylance's report, The SpyRATS of OceanLotus[6]



The SpyRATs of OceanLotus

Malware Analysis White Paper

CYLANCE

[6] https://threatvector.cylance.com/en_us/home/report-the-spyrats-of-oceanlotus.html

C2 Communications

Threat actors have been trying to protect or obscure C2 communications for many years, with varying degrees of success. The RedControle backdoor was recently observed modifying C2 commands by randomly inserting characters into command directives, in an attempt to evade HIDS/NIDS signatures. Other backdoors, like those from the OceanLotus Group, utilize a range of protocols including HTTP/S, DNS, and ICMP, and employ layers of encryption/compression. Often these attacks use custom encryption keys for each target. This makes the task of decoding commands to establish how a particular threat actor has been operating significantly more complex and time consuming.

Novel and Complex Techniques Used To Fly Under the Radar

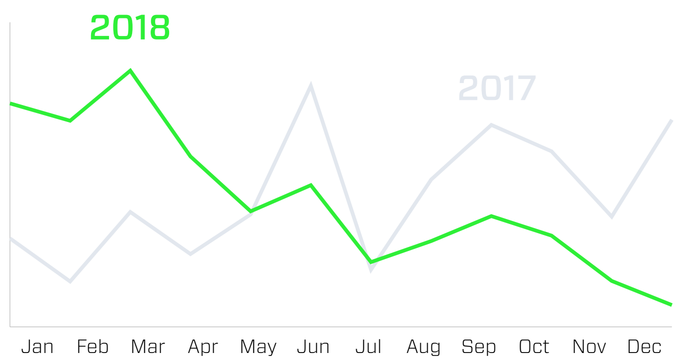
Cylance researchers uncovered a novel payload loader that utilizes steganography to read an encrypted payload concealed within a .png image file. The steganography algorithm appears to be bespoke and utilizes a least significant bit approach to minimize visual differences when compared with the original image. This approach is likely used to prevent analysis by discovery tools. Once decoded, decrypted, and executed, an obfuscated loader will load a variant of the Denes backdoor. The loader can be easily modified by threat actors to deliver other malicious payloads as well. The complexity of the shellcode and loaders shows that APTs continue to invest heavily in the development of bespoke tooling to evade detection.

> “The complexity of the shellcode and loaders shows that APTs continue to invest heavily in the development of bespoke tooling to evade detection.”

YEAR-OVER-YEAR ANALYSIS

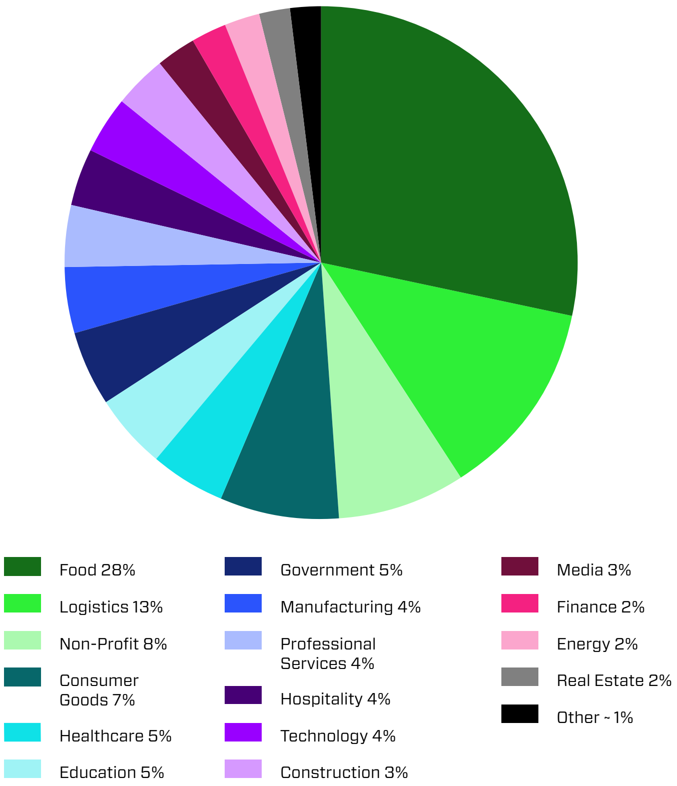
Every year, Cylance tracks the threat trends affecting customers. This provides insight into the historical progression and current state of the threat landscape by comparing the trends of a previous year with the most recent data.

Malware Sample Submissions By Year



According to Cylance customer data, the food industry was hit hardest by malware attacks, followed by the logistics sector. Non-profits and the consumer goods industry tied for third place, each suffering 8% of all malware attacks in 2018.

Malware Distribution By Industry



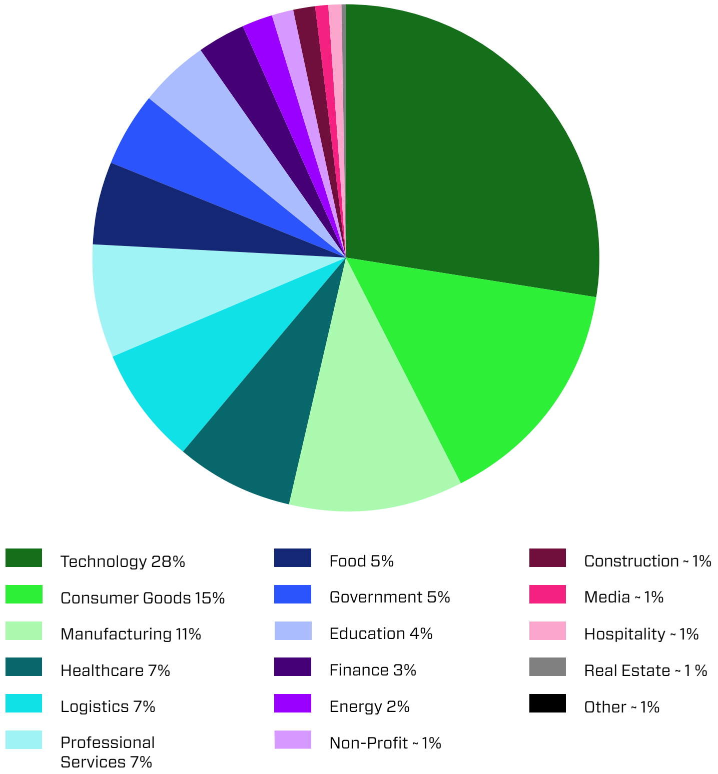
Ransomware

The technology sector, consumer goods, and manufacturing industry were hardest hit by ransomware attacks in 2018. The following chart offers a detailed breakdown of ransomware attacks within the Cylance ecosystem by industry.

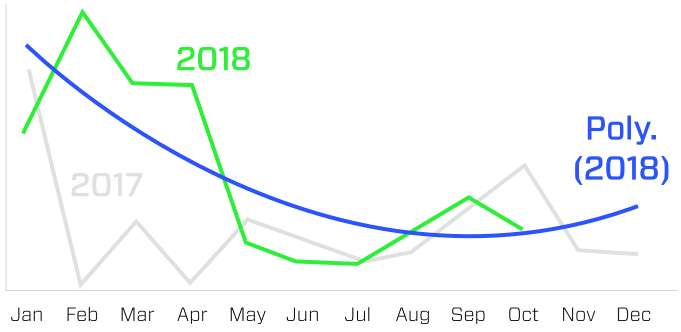
Overall, Cylance found that unique ransomware events decreased by 26% per enterprise customer in 2018.

It is important to note that for Cylance, a unique ransomware event occurs with the detection of a new threat and does not take into account the number of affected devices. Thus, the detection of a new strain of ransomware is only counted here as one event whether it attempts to affect one machine or hundreds.

Ransomware Attacks By Industry



Unique Ransomware Events By Year



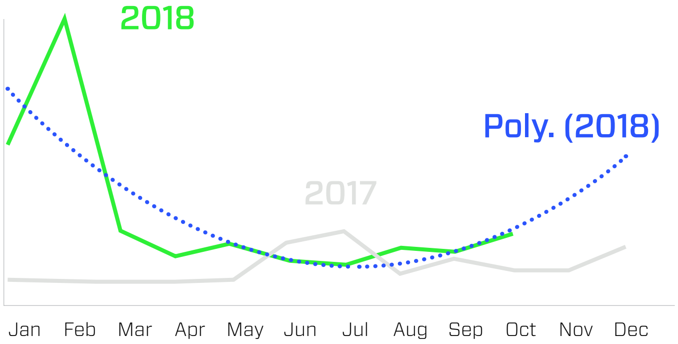
Cryptominers

Cryptominer detections increased by 47% per enterprise customer in 2018. It's no surprise that cryptomining attacks have dominated the threat landscape in 2018. It is a natural result of the rising popularity of cryptocurrencies and currency mining technologies becoming easier to use. During 2018, Cylance observed a wide range of currency mining malware using new spreading techniques and exploring novel approaches. This behavior appeared in both off-the-shelf open source solutions and sophisticated commercial botnets.

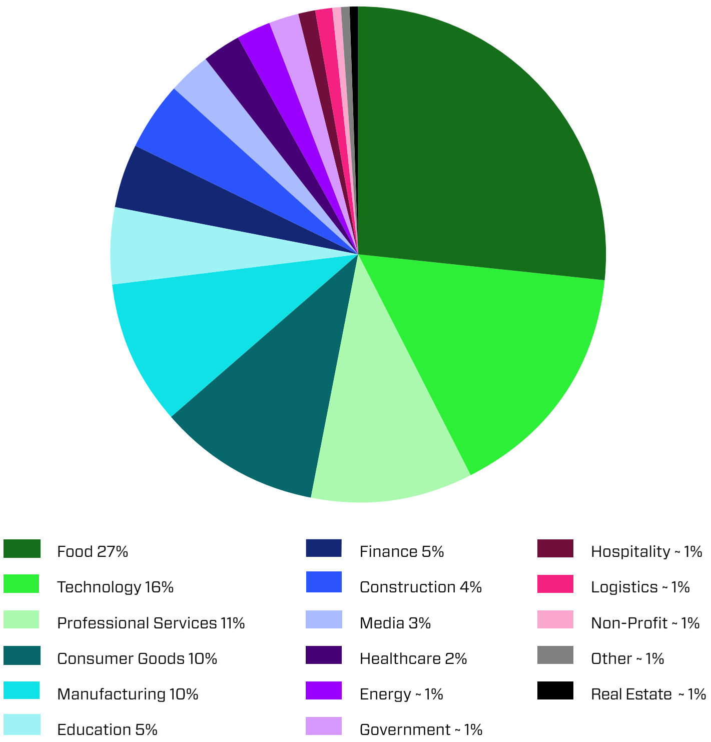
Traditional mining trojans, which execute locally on the victim's machine, comprise the majority of coinminer infections. However, there is a visible shift towards server-based solutions, which involve malware running solely from within the victim's browser.

The food sector, technology, professional services, consumer goods, and manufacturing industry were hit particularly hard by cryptominers in 2018.

Cryptominer Detections Per Year



Coinminer Attacks By Industry



File-Based Cryptominers

Most locally executed trojans are based on publicly available code with CCminer and XMRig being the most popular choices. During a typical infection, several files are dropped onto the target machine. Payloads include a loader and executables to perform the mining (both 32-bit and 64-bit versions). Text files containing pool lists and miner settings are often downloaded at a later stage to ensure up-to-date configuration. Persistence is achieved by modifying the registry, copying the loader to the Startup directory, or setting up a scheduled task.

Spam campaigns and drive-by downloads are two popular methods for delivering mining trojans. Mining trojans were also observed being dropped alongside banking malware and pulled by all-purpose downloaders such as Smokeloader. Some miner families, like Adylkuzz and MsraMiner, implement a worm functionality based on the leaked EternalBlue exploit.

Although most mining trojans are designed to run on Windows, cyber criminals did not neglect MacOS, Linux, and Android. In February 2018, a Monero mining trojan called CreativeUpdate was discovered being distributed via a compromised MacUpdate website. In May, XMRig-based MacOS trojan mshelper made headlines and a mining malware was discovered on Ubuntu's Snap Store. These entries add to a growing list of non-Windows mining trojans, including CpuMeaner (also XMRig-based) and MinerGate-based PwNet, to name a few. The Internet of things (IoT) is not immune to cryptojacking malware either. A mining botnet exploiting Android phones, tablets, and TVs was discovered in February of 2018.

Browser-Based Cryptominers

Coinhive, a service launched in September 2017, created a new approach to cryptomining. Coinhive offers a JavaScript-based solution to websites that mines Monero cryptocurrency using the browser and computing resources of visitors. The project was intended for legitimate website owners as an alternative way to monetize website traffic.

Coinhive is a ready-to-use solution that relies solely on code executed in the browser of visitors. There is no need for any software component to be installed. This approach makes the whole mining process easier to achieve, more persistent, and surreptitious. Cyber criminals quickly took notice of Coinhive's potential and put it to malicious use.

Shortly after Coinhive launched, its mining scripts were discovered on a range of rogue domains that leverage a technique called typosquatting. Typosquatting relies on users making mistakes when typing a URL into their browser. Cyber criminals later installed Coinhive scripts on compromised portals. In February 2018, Coinhive-based malware began to cause a serious uproar after a popular web plugin called Browsealoud was hijacked. The compromised plugin was used to secretly inject cryptominer code into thousands of government websites

Mitigation

Cryptominers can cause a major headache for businesses and private users alike by slowing down machines and disrupting productivity. Here are a few pointers on avoiding miners, both locally installed and browser-based:

- Run a contemporary security solution
- Keep all software up to date
- Disable the use of JavaScript in the browser
- Use browser extensions that block browser-based miners (NoCoin, minerBlock, AdBlock Plus)
- Block connections to known coin vault URLs
- Monitor or cap CPU usage

Cryptominer incidents are expected to grow through the beginning of 2019 and plateau by the end of the year. The volatile and highly-fluctuating value of bitcoin and the proliferation of competing cryptocurrencies will likely diminish the long-term appeal of malicious cryptominers. Another factor that will reduce their appeal is the unpredictable footprint on infected endpoints. Malicious cryptominers produced by less-skilled actors are often very noisy and visible.

> **"Shortly after Coinhive launched, its mining scripts were discovered on a range of rogue domains that leverage a technique called typosquatting. Typosquatting relies on users making mistakes when typing a URL into their browser."**

CYBERSECURITY INSIGHTS

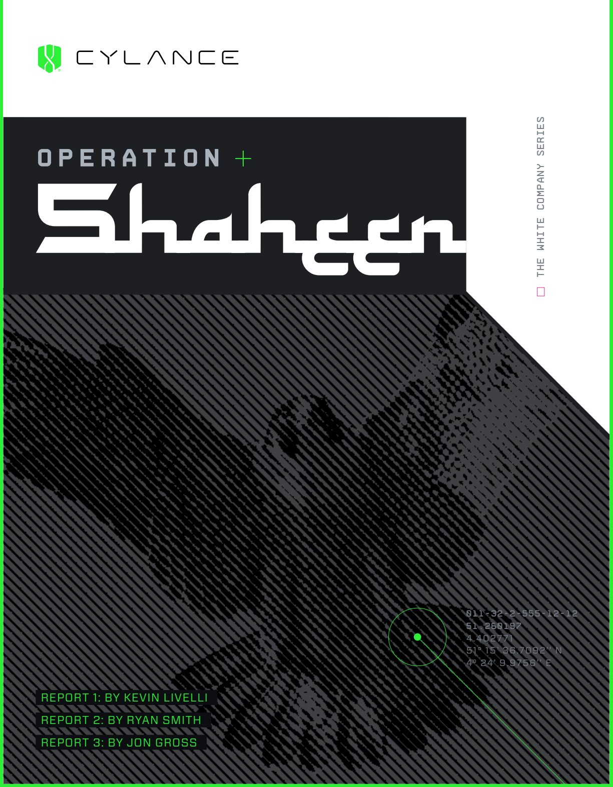
The White Company

In November 2018, Cylance released a report detailing the activities of a newly identified advanced persistent threat group, The White Company. This report offers detailed analysis of this threat actor's year-long campaign against the Pakastani Air Force (PAF). The PAF is an integral part of the Pakistani nuclear weapons program and home to the country's recently founded National Centre for Cybersecurity.

The White Company may be state-sponsored, given the considerable resources they possess including:

- Access to zero-day exploit developers and (potentially) zero-day exploits
- A complex, automated exploit build system
- The ability to modify, refine, and evolve exploits to achieve mission-specific needs
- The capacity for advanced reconnaissance of targets

For a full breakdown of this APT, read Cylance's report titled The White Company: Operation Shaheen, Inside a New Threat Actor's Espionage Campaign[7].



Virus Cleaning Conundrum

Last year, Cylance saw several parasitic infectors make its top 10 threat list. When parasitic infectors are successful in the wild, AV vendors receive a massive number of malware binary submissions. Cylance saw this happen with older threats that continue to make the rounds like PolyRansom, Ramnit, and Neshta. This infection-submission cycle also happens with classics like Elkern, Sality, and Virut.

Cylance researchers observed several files containing portions of viral code offered for public consumption in software distribution channels. This appears to be a result of certain AV solutions that clean infected files yet still leave traces of the malware infection intact. One nuance of AI-based security solutions is that they are sensitive to subtle file modifications. This sensitivity leads to files previously cleaned by competitors' AV being flagged as virally infected, due to the lingering malware artifacts. This creates a situation that could result in future embarrassment to both developers and AV vendors.

The Year of Emotet

If there is one threat that dominated 2018 in terms of propagation and persistence, it is Emotet. The Emotet of 2018 is a vastly different creature from the original 2014 version. It has evolved from a banking trojan into a robust and multi-faceted threat tool. Cylance observed numerous Emotet campaigns throughout 2018, a majority of which delivered additional (or later stage) malware payloads. Emotet has become a go-to tool for the distribution of Trickbot, IcedID, Qakbot, and many ransomware families.

Emotet campaigns are run by well-resourced private entities demonstrating an above-average level of technical skills. Revenue for Emotet comes primarily from the rental and use of its infrastructure to spread and manage other malware and threat tools. Over the last year, both the Emotet infrastructure and malware have improved their ability to evade traditional controls. Compromised servers hosting malicious documents and executable payloads are managed and dynamically cycled. Obfuscation of the malware code and scripts in malicious documents is continually altered to complicate analysis and detection.

Emotet infections generally begin with a phishing email containing a malicious document or a link to an infected document. While banking and invoice-themed lures are often used, the emails can be tailored to any subject or theme (holidays, etc.). The macros in the malicious documents are heavily obfuscated, often across multiple layers of encryption, substitution, and encoding. Emotet's Invoke-Expression layers, string replacement routines, and obfuscation can foil standard security controls and detection methods. Cylance has also observed examples of code or commands being reversed (data reading from right to left).

[7] https://pages.cylance.com/en-us-2018-11-operation-shaheen-threat-research-report-pdf-viewer.html?sfc=70144000001N29gAAC

Emotet payloads are often sandbox- / analysis-aware. Such examples have been observed abandoning execution or generating invalid indicators of compromise after detecting a sandboxed environment. Emotet payloads will typically establish persistence via the registry (Run key), service creation, or scheduled task creation.

The core banking-based module was removed from the executable Emotet payloads in 2017. The current version is more open and modular. There are separate modules now for data theft and exfiltration, SPAM and email distribution, spreading (SMB-based worm functionality), and more. Modules are handled and distributed in the form of DLL files. Emotet also uses some open-source components. The current communication protocol is built on Google Protobuf. Emotet also uses LZMA (compression) and OpenSSL (encryption).

Threat actors made some changes to the C2 protocol of Emotet in 2018. The overall protocol structure (Protobuf) was tweaked, mail client strings were removed, and compression and encryption routines were updated. The updated encryption included a ZLIB-based request structure coupled with AES and RSA encryption.

Emotet received new OS version data as well as a new miniupnp implementation (UPNP library). Cylance observed various uses of this module, but it is typically used to evade firewall rules by allowing port forwarding and binding to local ports. Additionally, there were updates to better obfuscate or mask code flow to confuse analysis (over-padding with junk data and superfluous jumps).

The key to Emotet's success is polymorphism paired with dynamic binaries and infrastructure. Malicious document templates are typically rotated every ten minutes during active campaigns. All Emotet payloads are packed or encrypted with custom tools (for evasion and anti-analysis). Encryption keys are rotated regularly. For example, the RSA keys used for communication between malware and C2 were frequently updated and rotated monthly, if not more often.

Current variants also include updated password lists for the SMB spreading (brute-force) module as well as legacy Emotet spreader tools including:

- **Outlook Scraper —** A name and address scraper targeting Microsoft Outlook accounts
- **WebBrowserPassView —** A recovery tool for browser-based passwords
- **MailPassView —** A recovery tool for email-client-based passwords
- **Netpass.exe —** A Nirsoft tool to pull passwords from user session and external devices

In October 2018, Cylance witnessed a functionality and feature update that allows Emotet to harvest full email message data from infected hosts. The trojan attempts to parse and exfiltrate full email body data (via Microsoft Outlook) for all emails over the past 180 days. The malware skims through the available messages in the IPM root folder. This new harvesting module copies the email data into a temporary file, allowing up to 300 seconds for the process to complete.

There are many obvious uses for this email data. One use, revealed later in 2018, was improving the efficacy of Emotet. The stolen email body data helped threat actors improve the social engineering success rate of Emotet's campaigns. Possessing the real email data from infected environments allows attackers to better construct and target their phishing attacks. Properly spoofed emails also provide a way to bypass traditional spam filters and email controls.

"The key to Emotet's success is polymorphism paired with dynamic binaries and infrastructure. Malicious document templates are typically rotated every ten minutes during active campaigns."

Another highlight of the spam module was the implementation of Domainkeys Identified Mail (DKIM). Cylance witnessed Emotet operators leverage DKIM to get around spam and email controls. With DKIM, the header of received email messages contain a public key certificate that authorizes and validates the sender of the email. Through using a clever domain-hijacking trick, the operators were able to bypass controls (DMARC[8]) and redirect the requests to specially crafted domains.

Cylance observed Emotet spreading several threats in 2018, including Trickbot, AZORult, IcedID, Qakbot, Dridex, and various ransomware families (Ryuk, UmbreCrypt, and more). Standard document files were not the only method of delivery for the first stage of Emotet infections. Some malicious emails contained a link to the malicious document, while other campaigns used alternate file types. Cylance has seen PDFs, XML Documents, and .js files all used in malicious Emotet spam.

Occasionally, specific exploits within the target platform were leveraged by Emotet. Other times, files were used to open malicious links (frequently the case with PDF files). Some emails contained obfuscated .js files that generate HTTP GET requests to the front-line C2 server. These requests may be for further instructions, to download scripts, for PowerShell commands, for executable payloads, or other resources.

The overall cost of Emotet grew in 2018. An active Emotet infection will cost an organization nearly $1 million to clean up[9].

Spotlight: Emotet and IcedID

In 2018, Cylance observed a sizeable uptick in the delivery of IcedID as a late-stage payload for Emotet campaigns. IcedID, also known as Bokbot, was originally discovered in 2017 and has continued to evolve and flourish among banking-focused trojan families. IcedID is a formidable threat on its own. However, in most of the campaigns Cylance observed, IcedID paired with more modular and scalable threats such as Emotet and Trickbot. While the initial focus of IcedID was the financial sector, Cylance has seen IcedID campaigns targeting other industries as well. IcedID expanded most heavily into the information technology, food, and agriculture industries.

IcedID was originally discovered in mid-to-late 2017, with IcedID v2 following in mid-2018. IcedID v2 introduced streamlined code, updated encryption, and obfuscation routines. IcedID v2 binaries are smaller, and the persistence mechanism was changed to a logon-based scheduled task. The v2 campaigns showed an increased focus on cryptocurrency exchanges and associated platforms.

IcedID has its own spreading capabilities (LDAP with brute-force), and special multi-step encryption routines to ensure each infection is unique and on the intended target. Perhaps the most interesting feature of IcedID is the included web redirection and injection capabilities. These capabilities involve creating a local proxy for routing traffic. This proxy allows the malware to monitor and exfiltrate any data of interest.

Browser sessions are also redirected by the proxy to fake phishing sites for credential harvesting and general data theft. IcedID can fool users by displaying the indicators of a secure session (SSL cert data, lock icon, etc.) as being present and intact. This gives browsing victims a false sense of security.

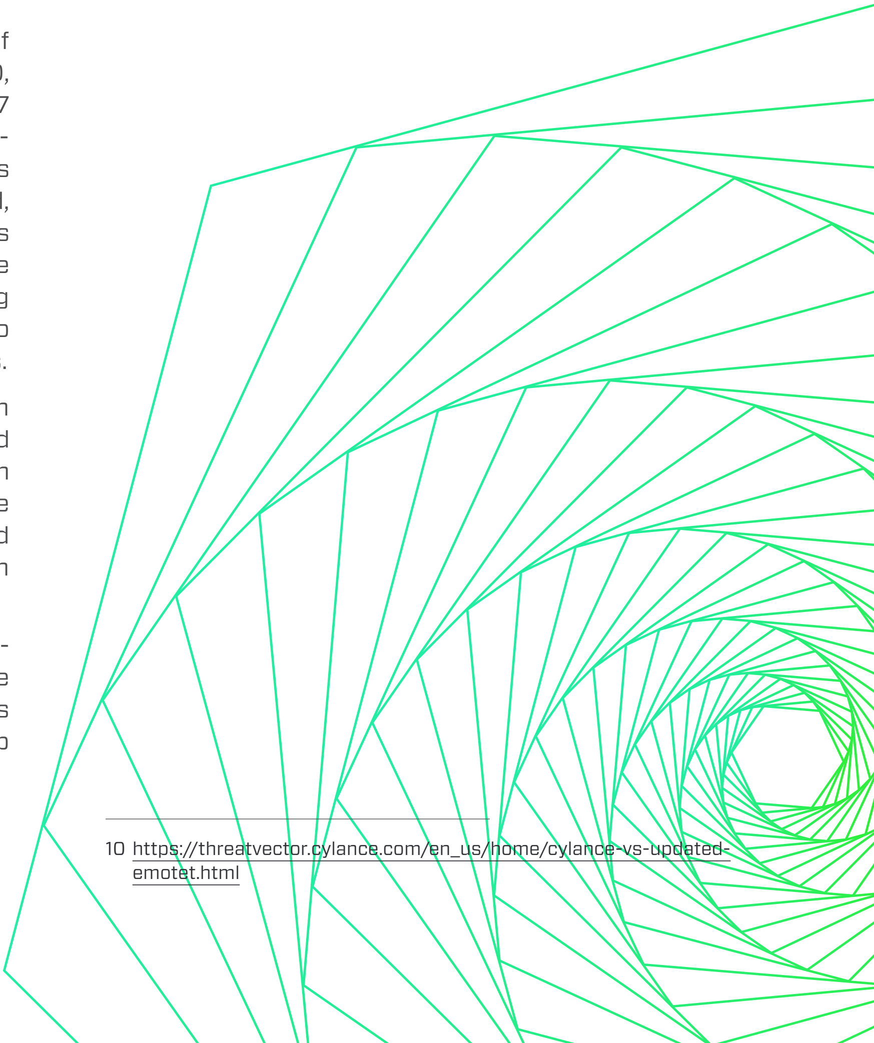
IcedID was heavily distributed by Emotet throughout 2018, but the relationship is not exclusive. Cylance observed IcedID paired with Trickbot, Hancitor, Dreambot, and others as well.

Quantified Increase in IcedID infections:

- Q1 to Q2 2018 – 479% increase
- Q3 to Q4 2018 – 316% increase

Predictive Advantage vs. Emotet

Emotet serves as a prime example of why prevention-based countermeasures and controls are required. Victims cannot wait a day or even an hour for a DAT/Signature update for their AV product. The AI models powering CylancePROTECT® demonstrated an ability to stop Emotet over two years prior to its discovery in the wild.[10]



[8] https://dmarc.org/

[9] https://www.us-cert.gov/ncas/alerts/TA18-201A

[10] https://threatvector.cylance.com/en_us/home/cylance-vs-updated-emotet.html

Attacks on Office365- A View from Cylance's Incident Response and Containment Team

The Cylance Incident Response and Containment team responded to several attacks on Office 365 over the past year.

Microsoft Office 365 (O365) Overview

In 2018, Cylance saw an increase in phishing attacks, most of them focused on Microsoft Office 365 (O365) credential harvesting.

The attacks were often financially motivated. They involved man-in-the-middle attacks (injections into organizations' wire-transfer processes), changing employee direct-deposit payment information, and stealing intellectual property.

Office 365 Attack Summary

Attackers send several phishing emails in an attempt to harvest user credentials. If successful, threat actors use the stolen credentials to gain access to an organization's O365 environment.

When attackers gain access to the O365 environment they typically create inbox forwarding rules that redirect email containing key phrases or words. For example, phrases such as "direct deposit", "malware", "wire transfer", and "payment" may trigger the email forwarding rule. Words that are indicative of intellectual property may also be used to flag emails for redirection.

The following sections detail some of the most common attack strategies observed by Cylance in 2018.

Direct Deposit and Payment Modifications

Direct-deposit-based attacks typically begin with the attacker sending phishing emails to obtain legitimate user credentials for the organization's O365 environment.

Once inside the environment, attackers create an inbox rule to delete any messages received that contain "direct deposit", "payment election", or similar financial terminology. Attackers will also use the stolen credentials to abuse improperly configured single sign-on (SSO) systems and authenticate to internal human resource systems, for example, WorkDay.

Once the attacker gains access to WorkDay (or similar HR system), they will modify the employee's payment elections and change the bank account information to redirect payments.

When the account information is successfully changed, the HR system notifies the user. However, because the attacker created an inbox rule to delete such emails, the user will never see this notification. The next time money is direct deposited it will go into the account configured by the attacker.

Wire Transfer Man-in-the-Middle

Man-in-the-middle attacks also use phishing emails to gain legitimate user credentials to an organization's O365 environment. With O365 man-in-the-middle attacks, Cylance typically sees two different scenarios. One approach involves attackers forwarding emails to an external email account via inbox rules, notifying the threat actors when a transaction occurs. The second method uses stolen user credentials to impersonate a legitimate user and proactively initiate wire transfers.

Both methods are often successful and may escape the attention of organizations until a financial loss is incurred.

Intellectual Property Theft

Intellectual property (IP) theft crimes are often financially motivated. Stolen IP is sold to third parties or occasionally used by attackers for a competitive edge. IP theft cases share many similarities with man-in-the-middle attacks. In both cases, attackers will phish for user credentials and abuse SSO to gain access to multiple systems.

The attackers typically setup an inbox rule with keywords related to the IP they seek to steal. When an email matching the flagged words is sent or received, it is forwarded to an external email address for the attackers to review. Cylance has also investigated cases where the emails will be copied into an internal mail folder for the attacker to retrieve upon their next log in. Attackers also use harvested user credentials to authenticate to OneDrive and SharePoint, where they continue searching for IP to steal.

Cylance has observed instances where the attacker will install OneDrive on another system and sync the compromised user's OneDrive files to the external location. When this type of attack is identified, responders must undertake the tedious task of sifting through voluminous and complex O365 audit logs. Doing so manually takes significant time, risks the possibility that key activities are missed, and delays the scoping, containment, and remediation process.

Cylance employs proprietary tools when responding to cloud security breaches of this nature. Cylance uses automated processes of data enrichment and normalization on logs to expedite recovery operations. Based on extensive cloud incident response and containment experience, Cylance has developed tools to:

- Quickly ingest raw O365 Audit Logs
- Restructure the O365 Audit Logs into an easy-to-digest structured data set
- Apply geographic location tagging to client IPs within the log data
- Look for known-bad indicators of compromise via the CylanceINFINITY™ Threat Intelligence database
- Apply clustering models to the structured data to identify user authentication abnormalities
- Provide context to the structured data to allow for faster processing by the Cylance Incident Response team
- Apply human intelligence by having Cylance's experienced specialists perform analysis on the processed and refined data

Microsoft Office 365 Attack Prevention and Mitigation Recommendations

Organizations can take some immediate steps to reduce the chances of a successful attack and improve their prevention, detection, and response capabilities, including:

- Enable multi-factor authentication (MFA) for all users
- Enable MFA for all administrator accounts
- Enable O365 Audit Logging
- Enable mailbox audit logging for all mailboxes
- Enable Client Rules Forward Block
- Review role changes weekly
- Devise an incident response process
- Review mailbox forwarding rules
- Review malware detection reports
- Review the risky sign-ins report within Azure Active Directory
- Review consent grants
- Configure spam filtering

Finance and eCommerce in the Crosshairs

From low-level financial fraud (e.g. carding, personal account theft, etc.) to sophisticated, nation-state-backed campaigns, the finance industry remains under siege by cyber criminals.

While numbers vary across studies and environments, Cylance data aligns with the following statistics:

- $12M to $15M – The average annualized cost of cybersecurity per entity across all sectors/verticals
- $19M to $20M – The average cost to the finance/financial services sector per cybersecurity breach
- $2.5M to $3.5M – The average cost per entity to rectify a major malware-based event or incident
- 25 days – The average time to remediate a catastrophic malware attack, including ransomware and related extortion attempts

In 2018, Cylance observed the continued adoption of COTS tools, LOTL tactics, and open source tools by organized and nation-state-backed threat groups. Implementing a variety of threat tools can serve as a distraction technique while also helping attackers successfully execute a malware campaign.

During the 2018 finance-focused campaigns, Cylance observed that:

- Malware continued to reign as the preferred method of attack, followed by web-based threats (drive-by, watering-hole, etc.), denial-of-service, and malicious insider attacks
- Phishing/spear phishing remained the primary vector for most cyber attacks

The most active malware families of 2018 for the financial sector ranged from trojans to ransomware, to the elaborate and targeted tools used in the HIDDEN COBRA campaign originating from within North Korea (DPRK). For example, recent campaigns attributed to DPRK centered around the mining and theft of cryptocurrency[11]. Malware families such as Emotet, Trickbot, Nanocore, and Adwind are also active players in the threat landscape.

Notable Malware Families

Emotet and IcedID

As previously described in this report, Emotet and IcedID were major players in attacks on the financial industry in 2018 (see The Year of Emotet).

Trickbot

Trickbot first appeared in 2016 as a banking trojan. Over the last year, Trickbot has rivaled Emotet in terms of self-propagation. Like Emotet, Trickbot steals and exposes sensitive information from infected targets. The hallmark capabilities of TrickBot include manipulation of network traffic, browser hijacking, credential harvesting, infecting connected devices, and downloading additional malicious code. Internal Cylance data suggests professional services, non-profits, and education will be the top targets for future Trickbot campaigns.

Cobalt Group

This threat group has increased its activity over the last year. The name refers to Cobalt Strike, a powerful offensive computing platform originally designed for red-team exercises and pen-testing. It is a popular tool often credited with having unmatched evasion and persistence capabilities, two features highly attractive to cyber criminals. Recent attacks like SpicyOmelette[12] illustrate a typical Cobalt Group attack pattern:

- Send spear phishing emails containing a malicious PDF file
- Direct victims to an AWS-hosted site containing malicious code
- Use core Microsoft utilities to sign and run the malicious code
- Assume control of system activity

Often the attackers will enable remote access to monitor various inputs and activities. The SpicyOmelette attack targeted payment system gateways, ATM machines, and other banking systems.

[11] https://www.reuters.com/article/uk-southkorea-northkorea-cryptocurrency/south-korean-intelligence-says-n-korean-hackers-possibly-behind-coincheck-heist-sources-idUSKBN1FP2XX

[12] https://www.zdnet.com/article/cobalt-threat-group-serves-up-spicyomelette-in-bank-attacks/

HIDDEN COBRA and FASTCash

Attacks originating from within DPRK[13] targeted banks in Asia and Africa, conducting tens of millions of dollars' worth of fraudulent transactions from 2017 to 2018. These attacks used remote connections to compromise application servers within the banking payment systems. According to a US-CERT alert[14] in October 2018:

> "HIDDEN COBRA actors target the retail payment system infrastructure within banks to enable fraudulent ATM cash withdrawals across national borders. HIDDEN COBRA actors have configured and deployed legitimate scripts on compromised switch application servers in order to intercept and reply to financial request messages with fraudulent but legitimate-looking affirmative response messages."

In addition, the FASTCash campaigns were one example of a string of cryptocurrency-focused attacks attributed to DPRK.

Direct Targeting of Transaction/ Payment Infrastructure

Over the years, there have been several attacks aimed at financial infrastructure. Threat actors' attempts to compromise RBS and SWIFT systems continue to grow in sophistication and frequency. The falling prices of cyber threat services and widespread availability of malicious code lowers the barrier to entry for up-and-coming cyber criminals.

In the last year, Cylance observed an increase in attacks against financial targets in Pakistan, India, South America, and others. In May 2018, Banco de Chile was targeted by the Lazarus Group. The attack employed both ransomware and wiper-based malware and resulted in costs estimated at nearly $10 million. In August 2018, the APT38 group targeted Cosmos Bank in India and caused roughly $13.5 million in damage. Within the span of a few hours, APT38 was able loot millions through a combination of fraudulent ATM withdrawals and unauthorized SWIFT transactions.

While examples of attacks on financial institutions are plentiful, the utter simplicity of these attacks often go unmentioned. A majority of these attacks begin with a simple spear phishing email. One bank employee opening the wrong email and clicking on the wrong attachment is all it takes to launch a malicious script. Once active in the infrastructure, malware can move laterally throughout an environment.

Exploitation of vulnerabilities on external-facing services and applications are another popular malware delivery method, as are web-based attack vectors. The world can expect to see the same methods being used in future attacks as long as they continue to produce reliable results. That being said, SWIFT has been actively promoting their Customer Security Programme (CSP). Anyone using SWIFT services would benefit from a review of their materials and guidelines[15].

The Dark Web

The Dark Web continues to be a primary source for fraud-focused tools and services. Visitors to the dark web can find an array of offerings from simple carding operations to elaborate affiliate services. Recently, some criminals have lost trust in the dark web due to market takedowns and successful hosting scammers. Yet, the demand for an ecosystem that facilitates the exchange of illicit goods persists and this continues to fuel the dark web.

Cylance witnessed a drop in the number of dark web open sellers and systems in 2018. Many vendors have created barriers between themselves and potential clients. A vendor may advertise their service or contact information on the dark web to attract inquiries, then demand negotiations proceed through other channels. For example, a vendor may require discussions continue via direct email using a secure messaging service like Protonmail. Telegram, Wickr, and WhatsApp have also been observed as serving as alternative communication platforms.

"The Dark Web continues to be a primary source for fraud-focused tools and services. Visitors to the dark web can find an array of offerings from simple carding operations to elaborate affiliate services."

[13] https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity

[14] https://www.us-cert.gov/ncas/alerts/TA18-275A

[15] https://www.swift.com/myswift/customer-security-programme-csp

What Consumers Want

When Cylance first considered offering its artificial intelligence technology to consumers, the company wanted to create a product and user experience people would love. Cylance knew its best bet was to go straight to the source. Cylance surveyed and talked to users from all walks of life to understand their attitudes and feelings towards the cybersecurity threats they faced. Here is what was discovered:

The biggest demand for a new, innovative, consumer antivirus, came from enterprise customers. This seems surprising at first, but when one considers the fact that enterprise companies spent $114B[16] on cybersecurity in 2018, it starts to make sense. Enterprise customers study cyber threat trends, assess risks facing their company, and eagerly seek new products and tools to improve their cybersecurity posture.

With today's workforce, enterprise security teams need to account for workers who are not confined within the company-controlled corporate network. In fact, 67% of workers use personal devices while at work[17]. Another 37% of U.S. workers telecommute[18]. The widespread adoption of cloud-based software allows employees to access corporate assets from countless devices. This means the boundaries of a company's network are no longer defined by the corporate firewall. It extends into their employees' homes via their personal devices. Companies want their employees to be as safe at home as they are at work.

In contrast to enterprise users, consumers expressed a general sense of frustration when it comes to cybersecurity. Although 97% of those surveyed said they use antivirus on their personal devices, 51% had switched vendors[19] in the past year. Why? The primary reason for switching was due to their antivirus product failing to protect their computer. Another 43%[20] anticipated they would likely switch in the future.

When asked to rank their most pressing security concerns, identity theft and financial fraud were consistently ranked first and second[21]. The debate over net neutrality and the Facebook-Cambridge Analytica data scandal brought privacy concerns once again to the forefront of consumers' minds. Consumer frustration stems from a feeling of helplessness. It arises from a sense of being unable to protect themselves no matter what they do (or don't do).

Why is there such a disparity between corporations' and consumers' attitudes towards cybersecurity? Enterprise security professionals know what they want, know what they must do, and can often take steps to improve their cybersecurity posture. Consumers feel like they do not have the time to keep up with cybersecurity or privacy trends, nor the knowledge to adequately protect themselves.

In Cylance's experience, consumers want the security product they select to do three simple things:

- Protect what they have – Computers, mobile devices, tablets, and home electronics
- Protect what they do – Online browsing, personal communications, shopping, and financial transactions
- Protect who they are – Personal identity, login credentials, and privacy

Cylance does not see any of those priorities and desires changing in 2019 as privacy and data concerns around the technology consumers use in their daily lives continue to mount.

[16] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[17] https://www.cbsnews.com/news/byod-alert-confidential-data-on-personal-devices/

[18] https://news.gallup.com/poll/184649/telecommuting-work-climbs.aspx

[19] Cylance, September 2017, internal Carbonview Survey: unpublished

[20] Cylance, September 2017, internal Carbonview Survey: unpublished

[21] Cylance, September 2017, internal Carbonview Survey: unpublished

Notable Credential-Based Hacks of 2018 — Why Authentication Matters

Successful cyber attacks made headlines throughout 2018. The unfortunate targets of these attacks included a major hospitality chain, Reddit, two large retailers, and hundreds of universities located around the globe.

Universities

Over 300 universities in the U.S. were targeted by Iranian attackers in 2018[22]. Of these targets, 144 were compromised. The attackers relied on spear phishing emails containing malicious links to scam network login credentials from university personnel. Once the threat actors had working credentials, they could easily access the victim's network infrastructure. Affected institutions suffered a combined loss of 31 terabytes of data and intellectual property estimated to be worth roughly $3 billion. The same threat group also attacked 176 universities in non-U.S. countries and 47 private companies.

Reddit

In another incident, the popular online platform Reddit suffered a credential-based attack that led to the compromise of user information and private communications[23]. Reddit requires their employees to use two-factor authentication. By intercepting SMS verification messages, the attackers were able to gain read-only access to Reddit backup systems. The backup systems allowed the attackers to view account credentials, email addresses, and all private and public content stored on compromised systems.

Marriott

The Marriott Starwood Hotel chain disclosed a four-year breach in their reservation system that exposed up to 500 million customer records in 2018[24]. The breach allegedly occurred when a cybersecurity vendor downloaded a malware sample, presumably for research. The malware sample managed to gain access to the Outlook Web Access (OWA) system at Marriott. The breach ultimately resulted in customer names, phone numbers, passport data, email addresses, and other PII being exposed[25].

Lord & Taylor

The popular luxury retailers Lord & Taylor and Saks suffered a breach affecting more than five million credit and debit card numbers[26]. The culprit was malicious software installed on cash registers that siphoned customer information. How the malicious software was installed on the point-of-sale systems remains unknown. Those involved with the remediation process suspect that successful phishing emails may have led to backdoors being installed on compromised systems.

How Can the Security Industry Respond?

For perspective on credential-based attacks, The Register[27] reports that attackers trying to crack user accounts may generate 90% of online retail traffic. Given the frequency of credential-based attacks, it is unsurprising that cyber criminals landed so many large attacks in 2018.

Visionary cybersecurity companies are continuously exploring new and innovative ways to thwart cyber attacks. One remedy to the notable breaches of 2018 may be AI-driven behavioral analysis. Tactics like credential hijacking and malicious service account activity can be quickly detected by AI trained to identify anomalous behavior. When potentially dangerous system behavior is detected, early mitigation steps can be initiated before real damage occurs.

[22] https://www.wired.com/story/2018-worst-hacks-so-far/

[23] https://www.theverge.com/2018/8/1/17639930/reddit-hack-security-breach-stole-user-data-2007-earlier

[24] https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#1ab153b3546f

[25] https://www.ndtv.com/world-news/china-may-have-been-behind-the-massive-marriott-data-breach-1958945

[26] https://www.nytimes.com/2018/04/01/technology/saks-lord-taylor-credit-cards.html

[27] https://www.theregister.co.uk/2018/07/20/credentials_login_slurp/

Conclusion

The year 2018 offered a variety of cybersecurity lessons without being dominated by a single standout threat or threat group. Economic pressures favored the rise of coinminers early in the year, but those favorable winds have since reversed. The future of cyptocurrency's value and its impact on the threat landscape throughout 2019 remain to be seen.

Overall malware attacks within the Cylance ecosystem rose by 10%. Cylance's 2018 observations concur with those made by the wider security industry; ransomware attacks are down and coinminer attacks are on the rise.

The cunning cyber criminals behind Emotet kept the cybersecurity world on their toes with a relentless barrage of innovations. They demonstrated that security measures commonly considered reliable can still be tricked, bypassed, or broken by motivated threat actors. By hard-coding common passwords in their brute force attacks, they showed the world even the simplest tactics occasionally succeeded in 2018.

Enterprise users demonstrated an encouraging awareness and interest in emerging, AI-driven cybersecurity solutions, tools, and practices. Consumers reminded us that there is room to improve in informing the public on cybersecurity issues and directing them toward more effective solutions. Cylance will continue to address the needs of both types of users by providing AI-native solutions to automate security for consumers and deliver cutting-edge prevention-based approaches for enterprises.

Cylance Predicts

While Cylance security solutions can claim a lab-verified prediction rate of 99.1%, Cylance's engineers, researchers, and executives cannot make the same claim. Though their accuracy may not match Cylance's products, Cylancers are not dissuaded from sharing their best guesses on upcoming security trends.

In January, they made the following predictions for what's ahead in 2019:

- We will witness a major infrastructure outage (power, water, gas, transportation, etc.) caused by a security issue in the industrial control space. This may be the result of a prolific malware attack or a direct attack. In either case, there will be significant financial or human costs.
- In the E.U., we will see a rise in GDPR enforcement based upon controllers and processors failing to provide adequate security.
- In the U.S., individual states, not the federal government, will largely drive privacy regulation.
- We will see an increased focus on implanting hardware with threats as a result of the Bloomberg SuperMicro article[28].
- There will be a surge in security intelligence, particularly as it relates to data that scales beyond human comprehension. In 2019, more data sources will become integrated, resulting in larger data volumes. Dependencies on APIs that facilitate these data integrations will grow as well, forcing security practitioners to innovate new ways to approach their environments.
- Extortion will become the shortest path to monetizing malspam campaigns based around Emotet and repurposed Dridex/Dyre variants. The malware's ability to insta-exfiltrate emails and user credentials will allow attackers to quickly extort users with information discovered in stolen emails. This approach may be found preferable to the risks involved with encrypting data and demanding (trackable) cryptocurrency payments.
- Attackers may begin to leverage alert-fatigue against enterprise targets. Threat actors may strike boldly then use the resulting noise as a diversion to distract from their actual objective. They may also seek to exhaust threat responders with a flood of alerts, knowing that millions[29] of cybersecurity positions remain unfilled.

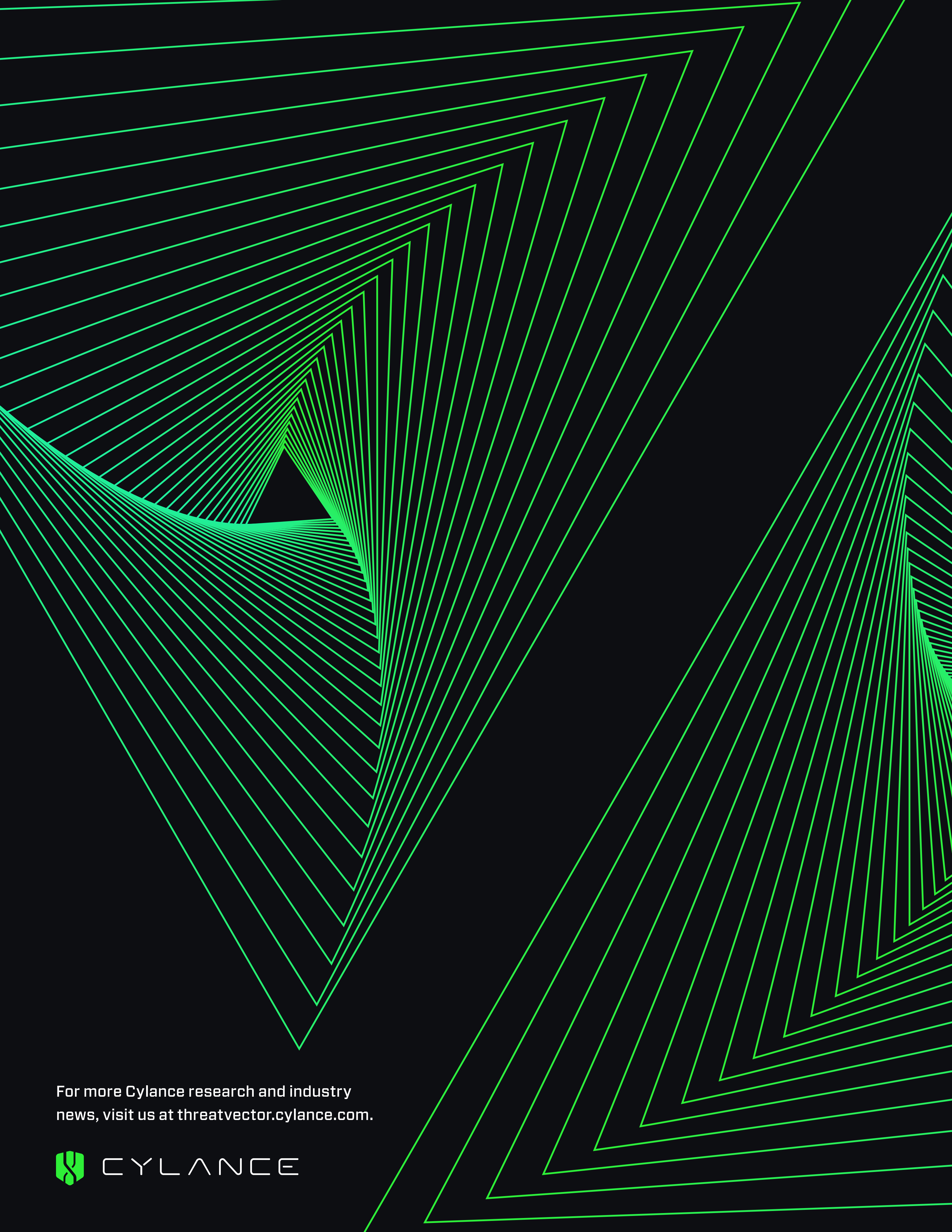
[28] https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom

[29] https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#4977d505a6b3

Appendix

Threat E:I:D Ratings

Family	Execution (1-4)	Identity (1-3)	Denial of Service (1-3)
MyWebSearch	1	0	0
InstallCore	1	0	0
PolyRansom	2	0	2
Neshta	2	3	1
Upatre	1	2	1
Ramnit	2	3	1
Emotet	1	3	1
GandCrab	1	0	2
Qukart	2	3	2
Ludbaruma	2	2	2
Cimpli	1	0	0
CoinMiner	1	1	1
FlashBack	1	2	0
Keyranger	2	1	2
MacKontrol	1	3	3



For more Cylance research and industry news, visit us at threatvector.cylance.com.

CYLANCE