

2018 Annual Threat Report

Produced by eSentire Threat Intelligence

Table of Contents

03	Preface
04	Executive Summary
06	Emerging Threats
09	Industry Trends
11	Phishing
13	Malware
15	Network Exploits
22	Socio-Political Context in 2018
23	Takeaways and Recommendations
24	Methodology
25	References

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 known and unknown cyber threats in real-time, 24x7x365.

This report provides a snapshot of events investigated by the eSentire SOC in 2018. It provides both visual and data analysis, written analytical analysis, practical recommendations and key assumptions for readers seeking to understand and better respond to the cybersecurity threat landscape.

EXECUTIVE SUMMARY

eSentire's *2018 Annual Threat Report* highlights a growing botnet attack infrastructure, an exponential increase in coinmining and the rising threat of Maldocs.

In 2018, the use of botnets increased 500 percent over 2017, with Mirai and its variants continuing to be the most observed threat. This surge in botnet activity led to a 250 percent increase in overall intrusion attempts when compared to 2017. As IoT devices continue to increase in numbers, they continue to be a significant contributor to a rapidly growing threat surface which increases with each newly published exploit.

Throughout 2018, coinmining emerged in two forms: malware on compromised assets and in-browser mining that persists only through the browsing session. Once infected, the coinmining malware silently mines cryptocurrency while consuming a significant amount of CPU cycles, resulting in compromised devices with sluggish performance and reduced battery life. Numerous financially-motivated incentives have led threat actors to prefer coinmining over alternative methods such as ransomware. These incentives drove a fifteenfold year-over-year increase in the amount of coinmining observed by eSentire.

Multiple Maldocs downloaders continued to propagate during 2018. Marap emerged as a new threat, while Emotet's increased its pervasiveness by adding enhancements. This allowed it to evade detection, spread internally on a network, and deliver modular packages. Maldocs downloaders typically enter organizations embedded within Office and PDF documents delivered through email, however, 2018 also saw the addition of seasonally-themed (Winter holiday, Independence Day) lures disguised as greeting cards.

The Top 10 affected industries in 2018 remained the same as in 2017. For many industries, however, their placement within the Top 10 shifted. Most shifts were small (one or two rankings), but the education industry climbed to first place from 10th place. This change for the education industry is likely a result of the combination of a highly exposed threat surface, with an increased volume in botnet activity. DocuSign continues to dominate phishing lures in the corporate environment, followed by Office365 and OneDrive.

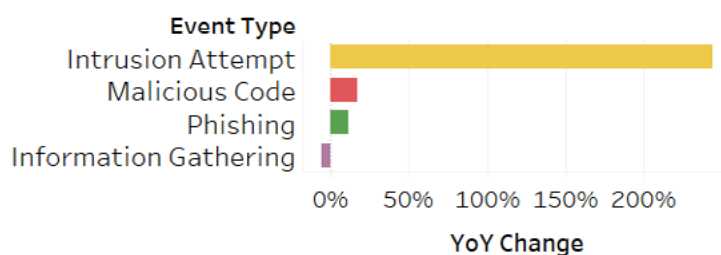
With the exponential growth of cybersecurity threats being a common theme in 2018, 2019 will present significant challenges for organizations looking to stay ahead of threats. For even the most prepared organizations, the increase in threats will present considerable operational and financial challenges as automation has made it easier, and more economical than ever, for threat actors to execute attacks. In order to stay ahead, it will be crucial for both organizations and security vendors to turn to emerging technologies such as artificial intelligence (AI) to help take on a proactive approach to protecting their most valuable assets.

EMERGING THREATS

Growing Attack Infrastructure

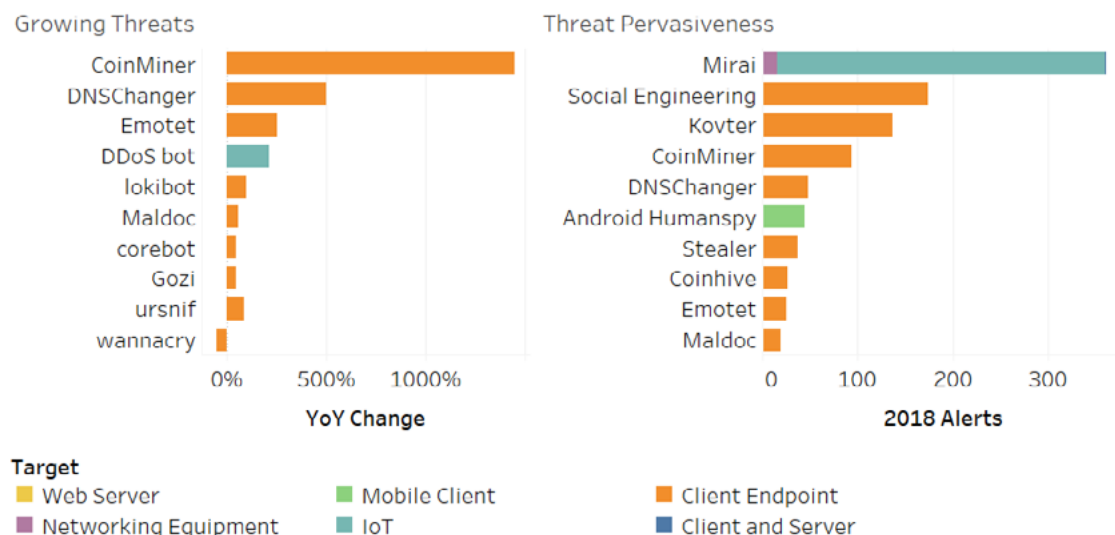
A surge in botnet activity led to a 250 percent increase in intrusion attempts in 2018 (Figure 1).

As reported in eSentire's Q2 2018 Quarterly Threat Report, a significant degree of this traffic appears to come from compromised servers.⁹ This observation is consistent with recent trends in multi-stage attacks.¹⁰ Threat actors often compromise low-hanging, low-value devices for which there is no direct opportunity for monetary gain. However, once compromised, they become part of larger-scale attacks more likely to yield a financial benefit. Threat actors have also been known to offer access to compromised servers for sale on the black market.¹¹ Thus, the demand and utility of compromised servers are clear. The opportunity to recruit servers is made possible by a growing threat surface across the globe, as new technologies are adopted at a rate exceeding the average organization's interest and awareness in cybersecurity.



■ Figure 1: Year over Year change in threats from 2017 to 2018.

In 2018, the use of botnets increased by 500 percent over 2017, with Mirai continuing to be the most observed threat (Figure 2, right). In 2018, there was a fifteen fold increase in CoinMiners, a fivefold increase in DNSChangers, and a threefold increase in Emotet (Figure 2, left). The rise of DNSChangers is consistent with an increasing trend in the utilization of compromised servers, as they can be programmed as rogue a DNS server (to which a DNS change request would direct victims). Similarly, a compromised server provides free processing power that threat actors can use to mine coin for extra income.



■ Figure 2: Exploit campaigns observed April 1 – July 1, 2018.

Emotet's increased pervasiveness in 2018 over 2017 may be caused by numerous enhancements allowing it to evade detection, spread internally on a network, and deliver modular packages.¹²

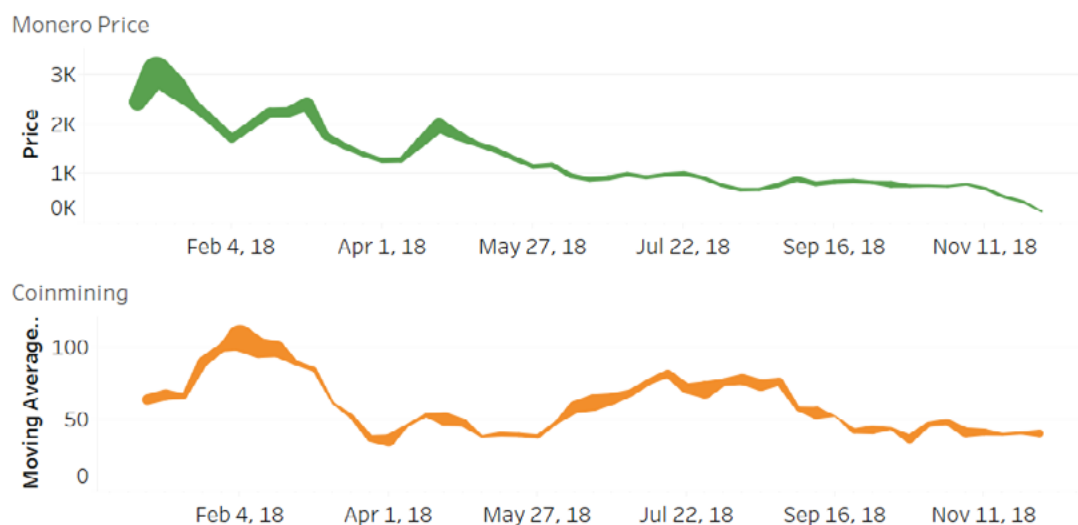
Aside from botnet activity, the most prevalent threats for 2018 were social engineering, Kovter, Coinminers and DNSChangers. Social engineering has continued to grow, as observed use of exploit kits have declined significantly—a prediction made in eSentire's Q1 2017 Quarterly Threat Report.¹³ The employee base remains one of the most challenging security controls as eSentire observed social engineering attempts in 2018 that ranged from low-effort mass spam campaigns to highly targeted and contextualized emails and phone calls (vishing).

Coinminers

Throughout 2018, coinmining emerged in two forms: malware on compromised assets (CoinMiner) and in-browser mining that persists only through the browsing session (such as Coinhive). Numerous financially-motivated incentives lead threat actors to prefer coinmining over alternative methods such as ransomware. First, cryptomining requires little time investment. Once the miner is deployed successfully, threat actors can immediately leverage the compromised system's processing power. On the other hand, ransomware and banking trojans result in a delayed return on investment since they both require the victim to act in a preferred way (such as paying a ransom or visiting a financial institution's website). Additionally, they require victims to have funds available in order to extort or steal them in the first place.

Monero¹⁴ is a popular cryptocurrency choice for illicit activity due to its enhanced privacy and distributed mining capabilities. Monero gained mainstream attention in 2017 with its use in the WannaCry incident and Shadow Brokers leaks. In 2018, F5 reported actors leveraging vulnerabilities in Apache Struts to install XMRig on web servers.¹⁵ A supply-chain attack discovered by eSentire early in February 2018 was installing coinmining malware through an exploit in remote access software. This software is leveraged by MSPs to access and administer their customer's networks, and allowed the actor to deploy malware to remote endpoints.¹⁶

Presumably, the price of various cryptocurrencies should impact threat actor motivation. The price of various currencies spiked in late 2017, leading to predictions that such operations would grow in popularity in 2018. Despite the volatility of currencies such as Monero, coinmining activity observed by eSentire remained consistent throughout 2018 (Figure 3).

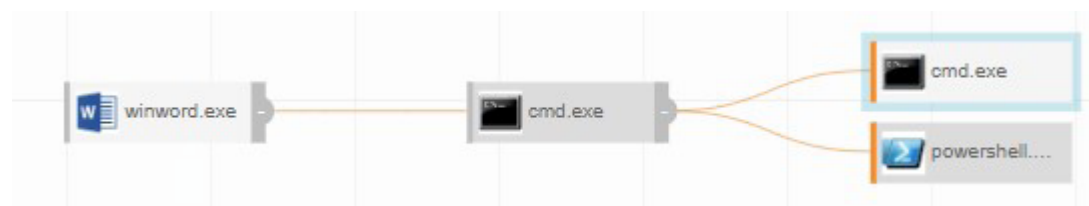


■ Figure 3: The price of Monero (top) and coinmining activity observed by eSentire (bottom).

Organizations can mitigate common coinmining threats in several ways. For browser-based mining, consider blocking traffic to sites such as *hxxps://coin-hive[dot]com*. Several Adblocker extensions and AV vendors have started blocking these JavaScript-based miners. For other coinmining threats, mitigation strategies vary. Opportunistic actors look to leverage the latest vulnerability in web technologies to deploy miners at scale. Robust patch management at the perimeter ensures you remain a hardened target (see *Recommendations: Exploits*). For more sophisticated threats, reducing the attack surface associated with applications such as PowerShell will go a long way (see *Recommendations: Malicious Documents*). Endpoint visibility provides additional flexibility, in that defenders can observe when trusted processes perform unexpected actions, such as connecting to a mining pool.

Maldocs (Marap, Ursnif and Emotet)

Marap emerged as a popular new downloader in 2018.¹⁷ Similar to Emotet, Marap enters organizations embedded within Office and PDF documents delivered through email. Ursnif continues to evolve, however detections followed close behind. Behavioral detection from the endpoint perspective remained largely sufficient for detecting Maldocs, since execution followed a predictable path. For example, monitoring Office applications which spawn child processes is simple, yet effective (Figure 4).



■ **Figure 4:** Example of winword.exe spawning PowerShell through CMD.

In instances where execution did not follow a typical path, it was generally trivial to trace the activity back to the root cause. This visibility has its advantages over static detections which can be bypassed through code obfuscation or by rotating C2 infrastructure—something that can result in a continuous arms race between a signature writer and malware author. Preventive/detective controls which address adversaries' tactics, techniques and procedures (TTPs), i.e., the techniques they use to deliver, install and persist malware across their targets, prove much harder for them to change. For example, Emotet was observed changing the obfuscation of command-line parameters executed by PowerShell. This may have been in response to improvements in PowerShell monitoring by defenders and AV vendors. However, this change has little impact on behavioral detections since the chain of events remains the same (Word spawns Command Prompt, which spawns PowerShell, which downloads a payload from a remote source).

There are numerous strategies for addressing Maldocs. Preventing macro execution is a common and excellent recommendation (although macroless execution techniques do exist). Limiting PowerShell should be seen as a priority, as it remains a prolific execution technique for various malware. As stated above, simply preventing Office documents from spawning child processes, or preventing PowerShell from downloading untrusted code from the internet, could cause challenges for adversaries.

See *Recommendations: Malicious Documents*.

INDUSTRY TRENDS

The Top 10 affected industries in 2018 were the same as in 2017 (Figure 5). However, for many industries, their placement within the Top 10 shifted. Most shifts were small (one or two rankings) but the education industry climbed to first place from 10th place. This is likely a result of the combination of a highly exposed threat surface with an increased volume in botnet activity. It should also be noted that the education vertical within eSentire's customer base is primarily administrative offices, and not networks that contain endpoint devices used by students.

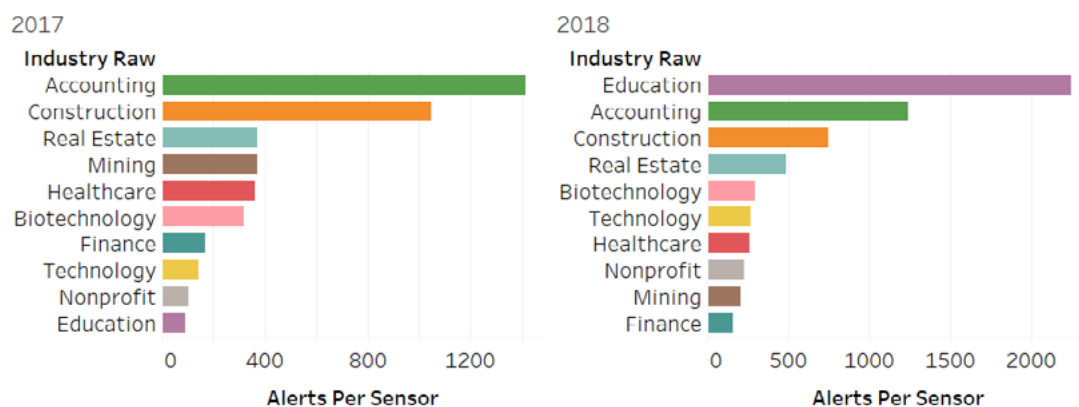


Figure 5: Overall Industry Ranking.

In 2018, the financial sector continued to mature its cybersecurity posture due to increased awareness. While many institutions initially only adopted an advanced cybersecurity posture in response to regulatory requirements, the increased exposure to cybersecurity concepts and events over the years has led to fewer alerts per sensor.

Phishing Across Industries

DocuSign continues to dominate phishing lures in the corporate environment, followed by Office365 and OneDrive (Figure 6). The overall composition of phishing in various industries has not changed much from 2017, however, an increase in lures targeting social media was observed in 2018.

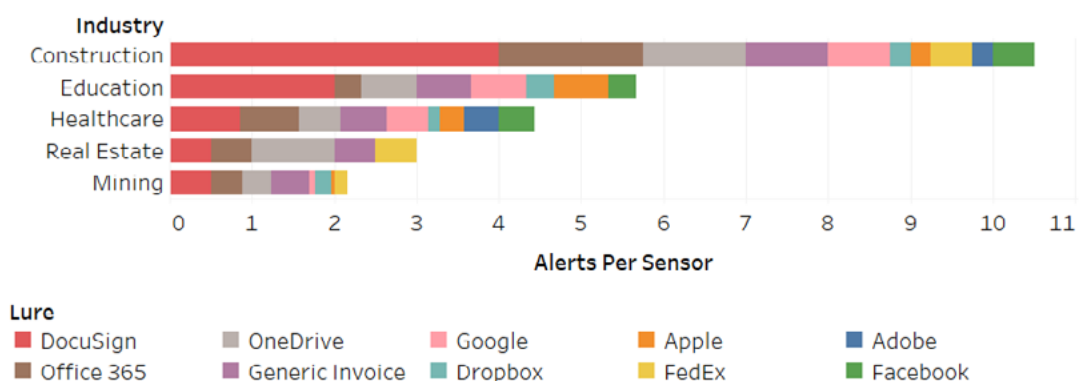


Figure 6: Phishing Lures in the top five industries.

Phishing events were most pervasive in the construction, education and healthcare industries. It is unlikely these verticals are more targeted than financial or legal industries. Rather, the volume of phishing events speaks to a lack of both technical controls and employee awareness around phishing, and a susceptibility to opportunistic attacks.

Malware Across Industries

Malware typically enters organizations through two sources: email that includes links to a malicious website or a malicious attachment, and through web-browsing.

The mining industry experienced the largest volume and diversity of malware, including numerous banking trojans, torrent-based (P2P) malware, and browser-based exploits (Figure 7). These infections enter the organization through the actions of employees—either through email or browser-based downloads (including torrents).

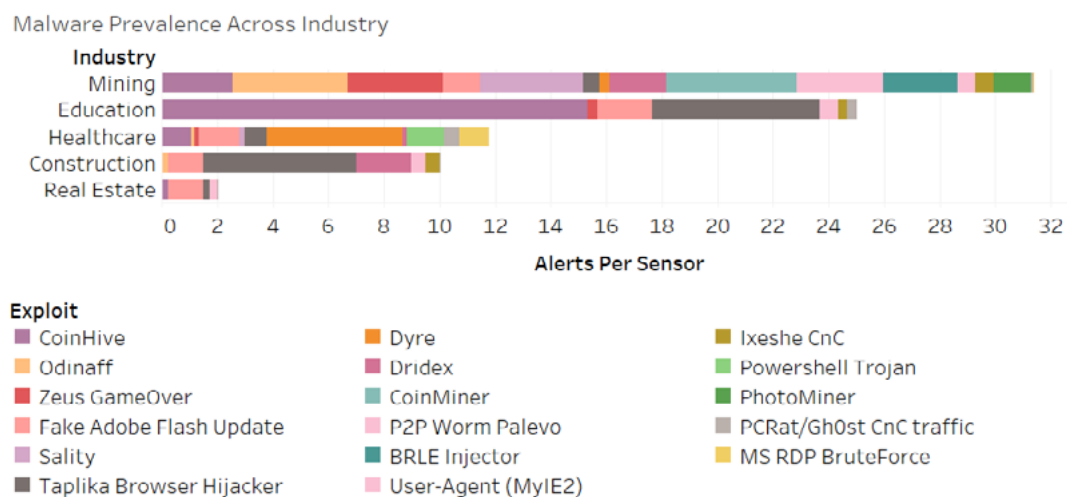


Figure 7: Malware varieties detected via network traffic.

The education industry's malware footprint was dominated by browser-based code injection, which persists only as long as the browser is open to a malicious page. Healthcare saw a large degree of Dyre, which is most often delivered through a malicious link in an email.¹⁹ This is also the case for Dridex,²⁰ which appeared in both the construction and mining industries. Lastly, both healthcare and construction proved to be more susceptible to browser-based social engineering exploits, such as the fake Adobe Flash update, which coaxes users into installing cryptocurrency miners on their Windows system.²¹

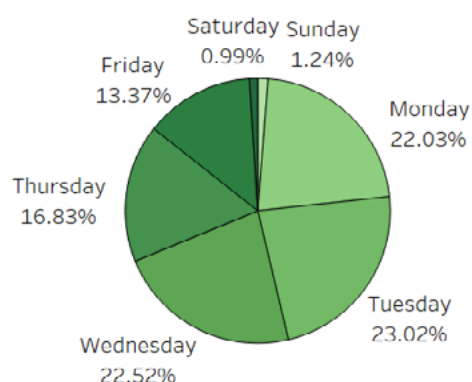
Many of these malware types are preventable when best practices for internet browsing and email are in place. For a large labor or guest force, additional mitigations may be necessary at the application and process level, including endpoint monitoring, strict firewall rules, and security staff to assess and address the organization's security posture.

Malware across industries demonstrates the need for better controls around email and browsing.

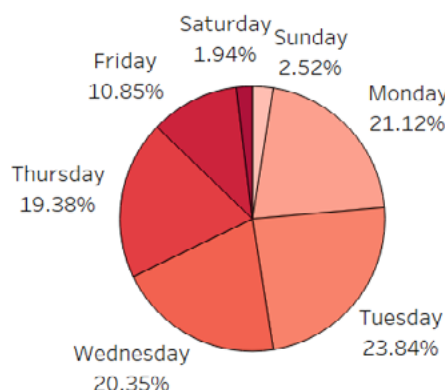
PHISHING

eSentire's Threat Intelligence Team has previously concluded that employee susceptibility to phishing is tied to workplace productivity. Similar to previous reports, employee participation in phishing tapers through Thursday and Friday (Figure 8). Because phishing events are associated with common workplace lures, this plausibly reflects less overall or email-based productivity near the end of the week.

What Days Are Phishing Link Clicked?



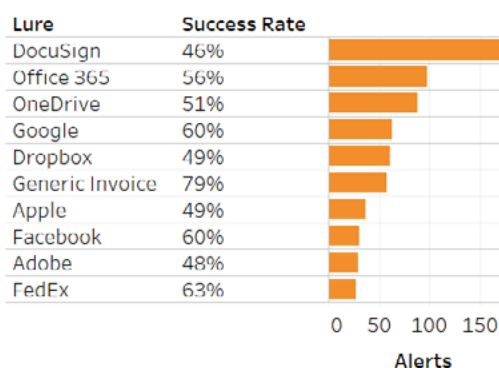
What Days Are Credentials Submitted?



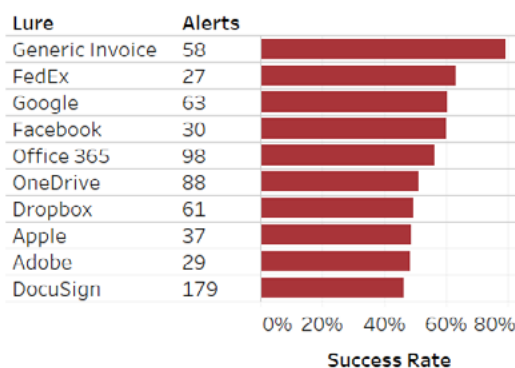
■ Figure 8: Distribution of phishing events over the week.

DocuSign, Office365 and OneDrive have remained consistently popular lures throughout 2018 (Figure 9). Most lures imitated applications (Adobe, DocuSign and Office 365), social media (Facebook), cloud storage (Dropbox, OneDrive and Google), and shipping companies (FedEx). The greatest success rate results from the generic invoice lure. Rather than phishing for credentials, this email attack attaches a malicious document (such as Emotet, Hancitor, Ursnif or the new Marap) disguised as an invoice.

Most Observed Lure



Most Successful Lures

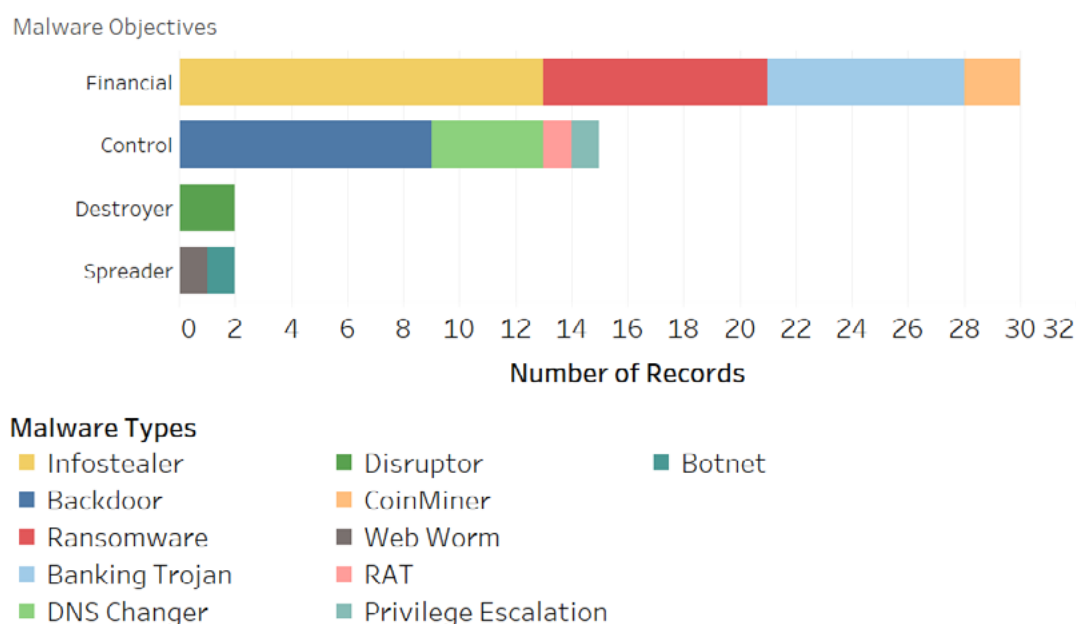


■ Figure 9: Most common lure observed in 2018 (left) compared to the most successful lures, in terms of credentials submitted (right).

Phishing lures imitate applications, social media, private cloud storage and shipping companies.

MALWARE

The majority of observable cybercrime is known to be financially motivated,²² but that does not always make financially-motivated cybercrime the most impactful. For example, WannaCry had a widespread impact, costing approximately \$4 billion USD in losses and damages around the globe.²³ However, WannaCry and similar outbreaks, including NotPetya, appear to be cases of intentional destruction disguised as ransomware.²⁴ Disruptors are destructive malware that encrypt files, similar to ransomware. However, disruptors have no direct path to decryption, whereas ransomware attacks are financially motivated and include a payment that promises to decrypt the victim's systems. Only two infections intended for disruption were observed in sandbox samples detonated in 2018 (Figure 10).

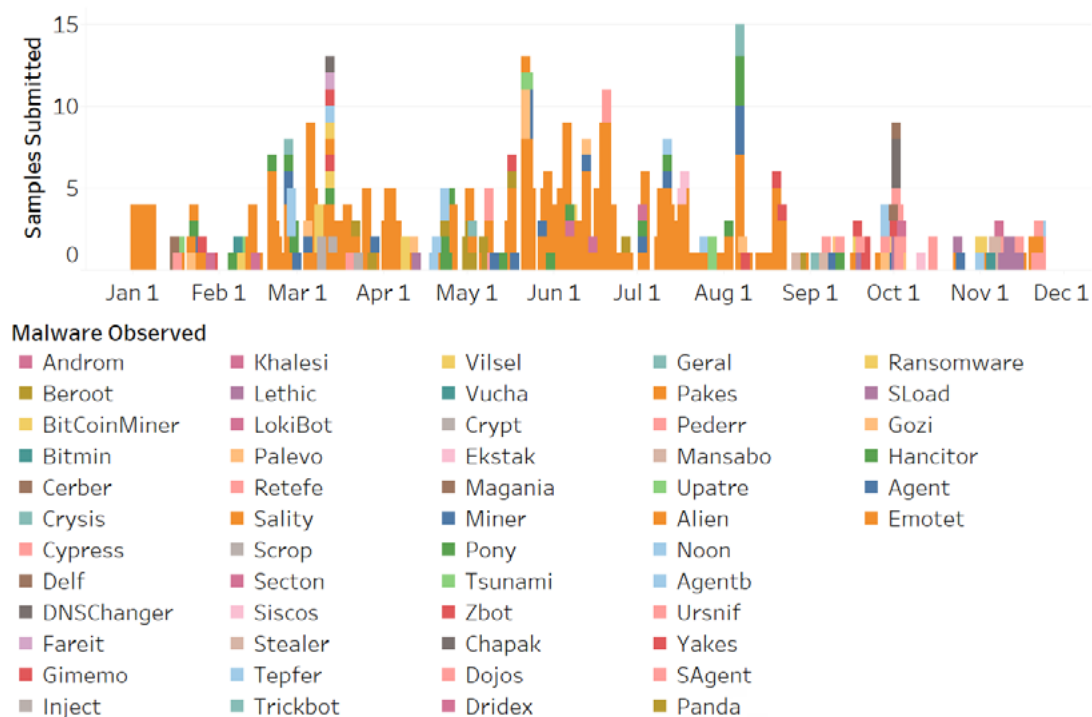


■ **Figure 10:** Malware types observed and their inferred objectives (excluding MalDocs).

The majority of malware samples observed were classified as malicious documents or MalDocs. Most MalDocs observed were disguised as invoices or missed payment notifications which entice employees to download a payload that can carry out further objectives. Web-based downloaders were another delivery method. Typically, the delivered payload is a banking trojan, a type of infostealer that is designed to harvest credentials for banking information as users interact with their financial institutions via the browser. Other infostealers can steal a broad range of credentials from web applications, including banking credentials and credit card information. Some infostealers are not financially motivated and may be considered a control malware, depending on what system credentials they retrieve. Control malware like backdoors, DNS changers, and RATs can give attackers access to a compromised system which can then be used to carry out further objectives.

Analysis of malware samples observed show financial motives dominate, but other motivations can be more impactful globally.

The full breadth and taxonomy of malware observed in 2018 demonstrates a vibrant ecology of malware (Figure 11).



Malware Taxonomy

Delivery	MalDoc	Dovs Emotet Gozi Hancitor Noon Pederr SAgent SLoad Ursnif Vucha
	Downloader	Chapak Cypress Geral Upatre Vilsel Yakes
Control	Backdoor	Alien Androm Lethic Tsunami
	DNS Changer	DNSChanger Pakes
	Privilege Escalation	Beroot
	RAT	Pony
Destroyer	Disruptor	Crypt
Financial	Ransomware	Crusis Foreign GandCrypt Gimemo Locky Scrop Takburn Zerber
	Infostealer	Delf Fareit Khalesi Magania Mansabo Siscos Tepfer
	Banking Trojan	Panda Retefe Trickbot Zbot
	CoinMiner	BitCoinMiner Bitmin
Spreader	Botnet	Salinity
	Web Worm	Palevo
Vagueware	Vagueware	Agent Agentb Chou Dojos Ekstak Inject Miner Secton Stealer

■ **Figure 11:** Malware samples observed in 2018. Classified via sandbox detonation and anti-virus definitions.

During observed holidays, malware lures shift from impersonating invoices to impersonating seasonal greeting cards.

Emotet was the most observed malware across clients. The majority of Emotet lures came in the form of invoices and unclassified Microsoft Word documents—many of which are likely to be fake invoices (Figure 12). A notable dip in Emotet activity was observed in October 2018, an observation echoed by several researchers,²⁵ before Emotet re-emerged in November with new email exfiltration capabilities.²⁶ A sprint of shipping-related lures was observed March 1, and lures were also seen attempting relevance by being seasonally themed. In January, a handful of Christmas card lures were still being observed—as well as other generic greeting cards (Figure 13, green and dark green). On Independence Day in the United States (July 4), eSentire Threat Intelligence observed Independence Day lures, as well as more generic greeting cards (Figure 13, green and blue).

Emotet Delivery Method

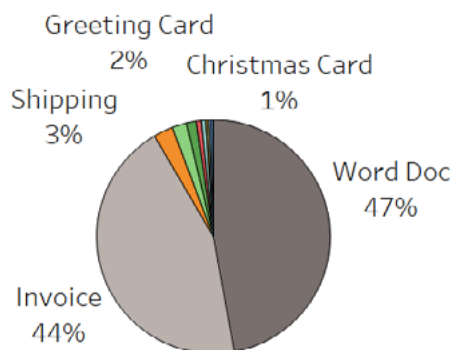


Figure 12: Breakdown of Emotet lures observed.

Maldoc Timecourse

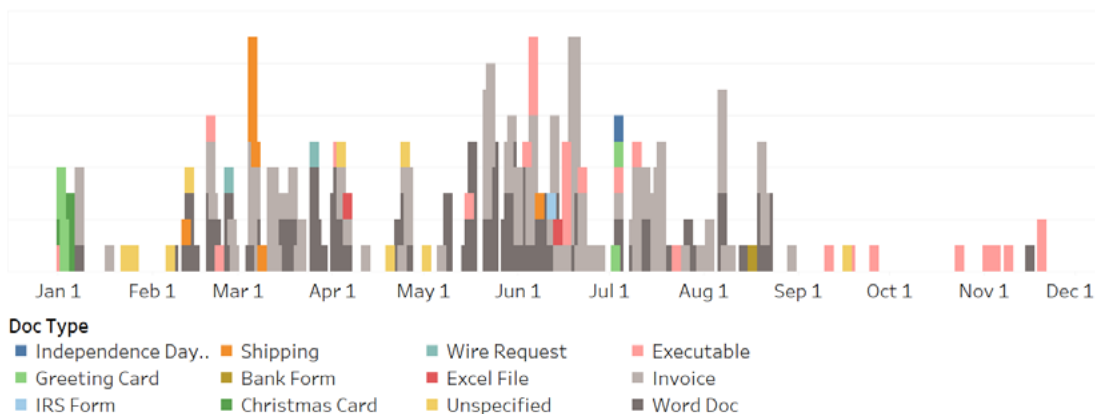
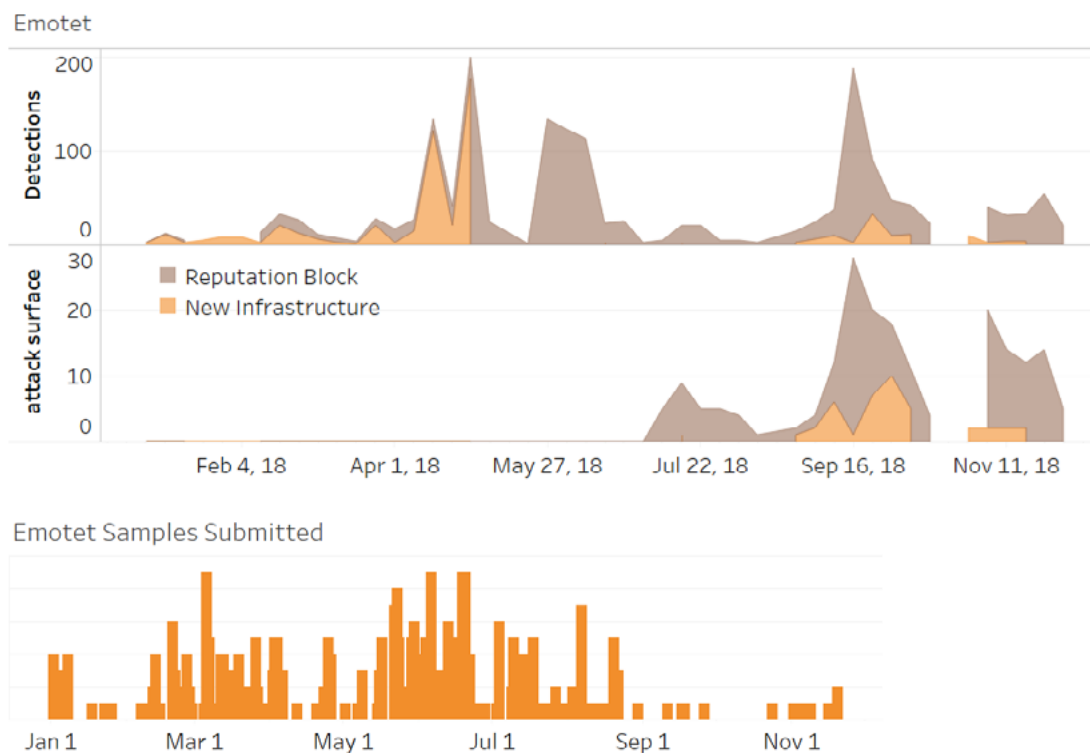


Figure 13: Emotet lures observed over 2018.

Sandbox Analysis and Network Detection

Sandbox analysis and network detection are individual tools that analysts use when investigating events—neither is particularly superior; rather, a security analyst uses both as needed. Downloaders likely delivered much of the other observed malware with the majority of payloads being banking trojans like Panda and Trickbot (Figure 14). While sandbox samples tend to come from emails, before detonation, network coverage of Emotet detects compromised systems beaconing to known Emotet infrastructure. A large degree of reputation blocks based on Emotet infrastructure occurred in April, September and November; times when few sandbox samples were submitted.



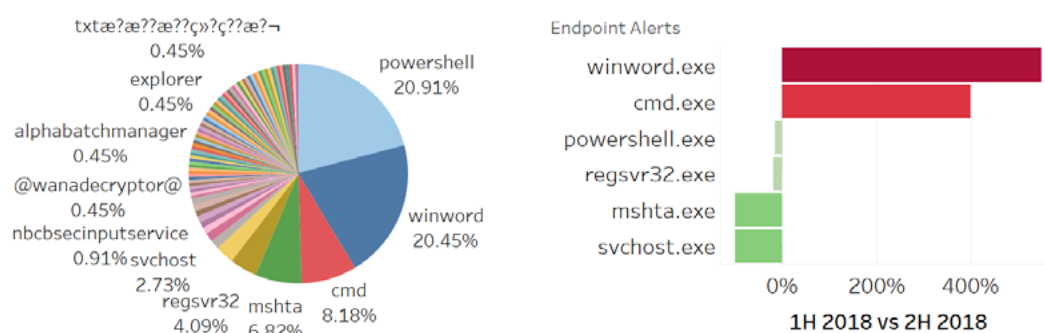
■ Figure 14: Emotet Network detections (top) and sample submissions (bottom).

Malware Tactics

Compared to network-based detection, endpoint telemetry allows for a more in-depth perspective on how attacks are carried out. When comparing detection points for confirmed threats in 2018, the use of trusted Windows processes remains a popular method for gaining a foothold on endpoints. The popularity of PowerShell and Microsoft Word (winword.exe) speak to the trends in Maldocs mentioned throughout this report.

eSentire observed various techniques for obscuring PowerShell commands throughout 2018 (Figure 15). This included writing data to other locations before calling it, such as environment variables, registry keys, Dropbox and Pastebin, among others. Public research into command-line obfuscation methods has led to adaptation by threat actors.²⁸ Downgrade attacks or masquerading of the PowerShell process were also observed. This continuous effort to bypass detections indicates that threat actors may overly rely on PowerShell for code execution and defense evasion. The lack of observed alternative methods for reliable code execution poses a risk for adversaries who are overly reliant on PowerShell. As Windows 7 approaches end-of-life and more organizations take advantage of security features available in Windows 10, adversaries will have to adapt their tactics. For Windows 10 users, layering Attack Surface Reduction rules can be effective.²⁹

Additional mitigation techniques are outlined in *Recommendations: Malicious Documents*.



■ **Figure 15:** Processes used in attacks (left). H1 over H2 change in use of trusted Windows processes (right).

NETWORK EXPLOITS

Vulnerabilities in externally-facing assets present an alternative method to social engineering for infiltrating networks. When exposed devices are left unpatched or zero-day exploits become available to threat actors, organizations can become at-risk to network-based exploits. Incidents involving successful exploitation of perimeter assets were rare in 2018, speaking to strong patch management at the perimeter. It's generally considered best practice for organizations to prioritize patching perimeter assets over those residing safely inside the network. In one case however, a victim accidentally exposed several critical systems that had not been patched for the SMB exploit known as EternalBlue. Once exposed, the systems were immediately compromised. With this one exception in 2018, the vast majority of network exploit attempts observed on the eSentire threat detection surface were unsuccessful. The majority of attacks against routers, switches, and IoT devices were likely perpetrated by botnets similar to the Mirai botnet - some direct variants of Mirai, while web server exploits appeared to come from compromised servers.⁹

IoT attacks incentivized by a lack of security awareness and presence around IoT devices.

IoT devices continue to contribute to a rapidly growing threat surface³⁰ as each connected device increases the chance of exploitation. In the case of IoT devices, there is little in the way of mitigating security. Few consumers are aware of the importance of changing default credentials on such devices, leading California to ban default passwords for connected devices,³¹ with Germany also beginning to enforce similar legislation on consumer-grade routers.³² Infections on routers and IoT devices are difficult to detect since the device is typically designed for direct human interaction, lacking enterprise capabilities for diagnostic services or event logging.

Attacks on web servers, home routers, and IoT devices likely dominated by botnets and automated exploit campaigns.

As shown in the second quarter of 2018, activity pertaining to many of these exploits corresponded to the release of a new exploit on exploitDB.⁹ Note that exploitDB is not necessarily the first source to publish, but is a consistent and reliable source for exploits. Further, the publishing of exploits often coincides with the implementation to detect them, meaning attacks could have preceded network detection and release dates.

Microsoft IIS 6.0 on Windows servers was the most targeted configuration on the eSentire threat detection surface (Figure 16). Attacks were initially coupled with WebLogic exploits. Web servers and routers were also a primary target in 2018, following numerous releases of exploit code. Drupal was a popular target following the release of the Drupalgeddon2 exploit.³³ Exploits for Apache Struts and PHP appeared as background radiation in the sense that there were persistent attacks anticipating accidental exposure of vulnerable systems or the misconfiguration of webpages.

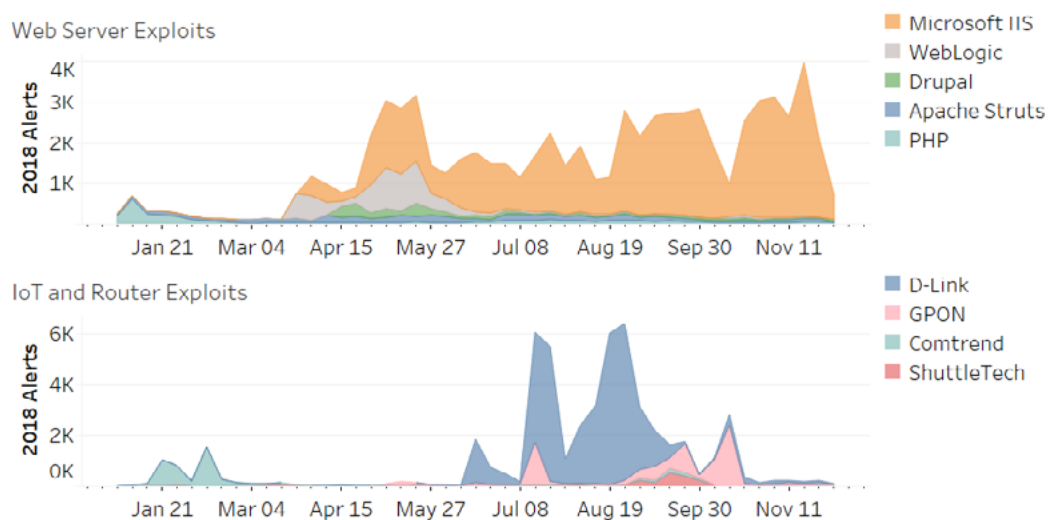


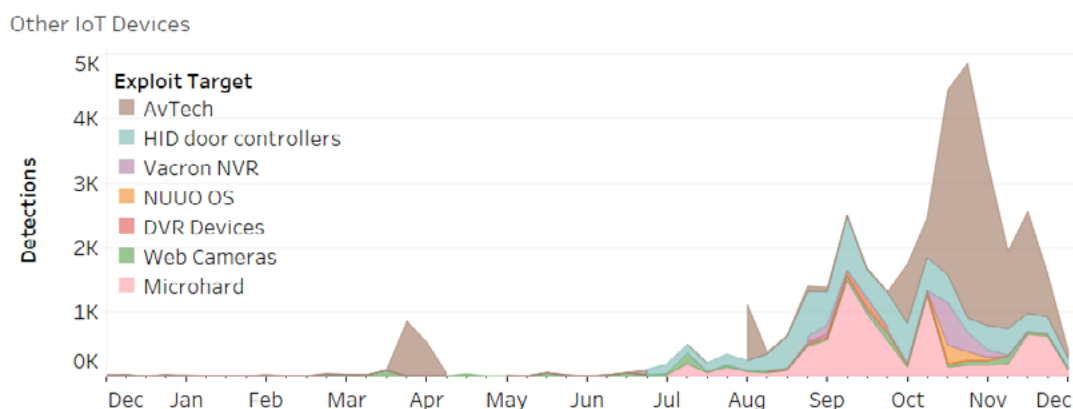
Figure 16: Attacks targeting web servers and routers in 2018.

Attacks targeting D-link home routers were detected early in the summer (Figure 16). A larger campaign in mid-July targeting both D-Link and GPON was detected by both eSentire and 360 Netlab as reported to Threatpost.³⁴ Later, GPON attacks re-appeared next to DNS poisoning attacks against ADSL-type routers, such as Comtrend and ShuttleTech routers. DNS poisoning occurs when an attacker tries to either reconfigure target devices to trust a DNS server that the attacker controls (such as through command injection) or alter the DNS records of a trusted DNS server. Attacks targeting Comtrend appeared early in the year, then returned later alongside ShuttleTech, the primary target of DNS poisoning attacks observed on eSentire's detection surface in Fall 2018.

Attacks on IoT Devices

eSentire Threat Intelligence observed a growing trend in IoT exploits targeting cameras, door controllers, surveillance equipment and media devices (Figure 17). Many of these exploits appear to be related to variants of the Mirai botnet. The majority of this activity occurred following the summer release of exploit code before observed attacks:

- **May and August** - Two DVR exploits added to growing list.^{35,36}
- **July 9** - HID door controllers exploit published.³⁷
- **July 17** - Microhard Systems Cellular Ethernet and Serial Gateway — default password and numerous exploits published.^{38,39}
- **July 23** - NUUO remote code execution exploit published.⁴⁰



■ **Figure 17:** Attacks on IoT devices.

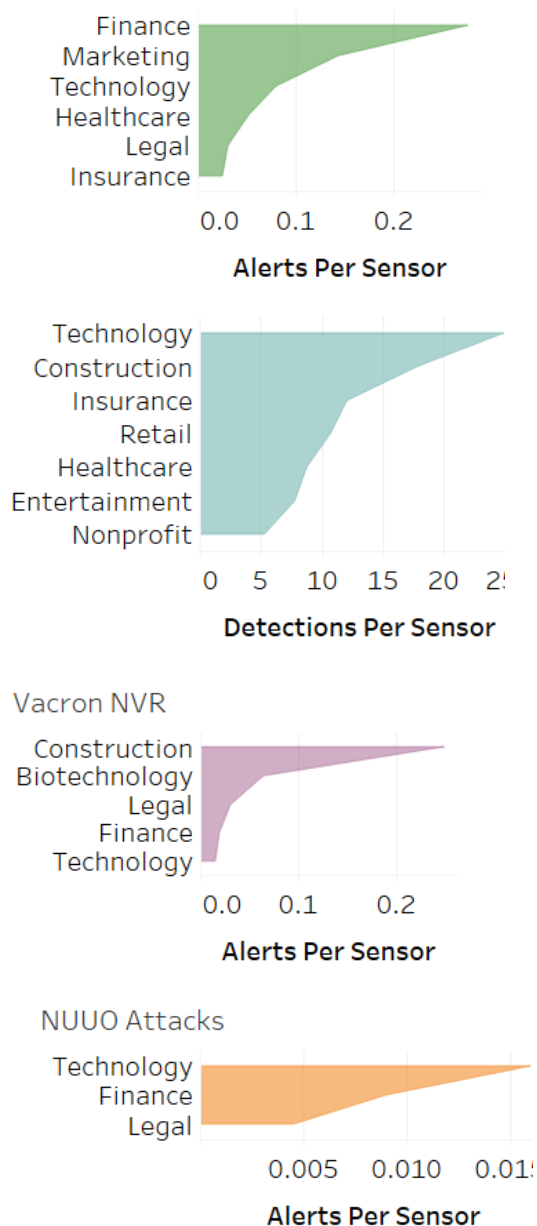
A large degree of attacks targeting IoT devices appear to be targeting physical security devices in protected industries.

Vacron NVR, NUUO and IP Camera Attacks

Vacrons and NUUO Video management devices aggregate local IP cameras for storing, monitoring and reviewing security footage. Attacks against these three systems were most observed within the technology, finance, construction and legal industries (Figure 18). There is no certainty whether these industries were the intended target, or that the emphasis on these industries was related to exposure. With the exception of construction, these industries demonstrate above-average cybersecurity awareness. Therefore, it is likely that they also practice physical security and have these systems on-premise. Construction organizations are also likely to have physical security measures in place for protecting the property they are contracted for, as well as any on-site equipment owned by the construction company.

HID Door Controllers

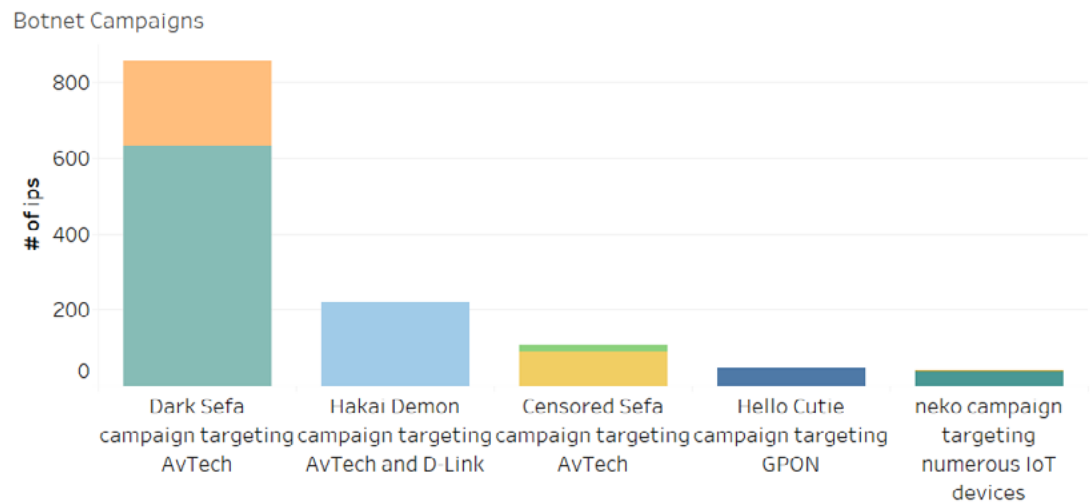
Door controllers operate security doors that help companies maintain physical security by restricting public access to their property. The associated exploit for HID brand door controller can allow attackers to download the controller's database, which can contain sensitive employee account information. To date, none of these attacks are known to have been successful.



■ Figure 18: Security devices targeted on protected industries.

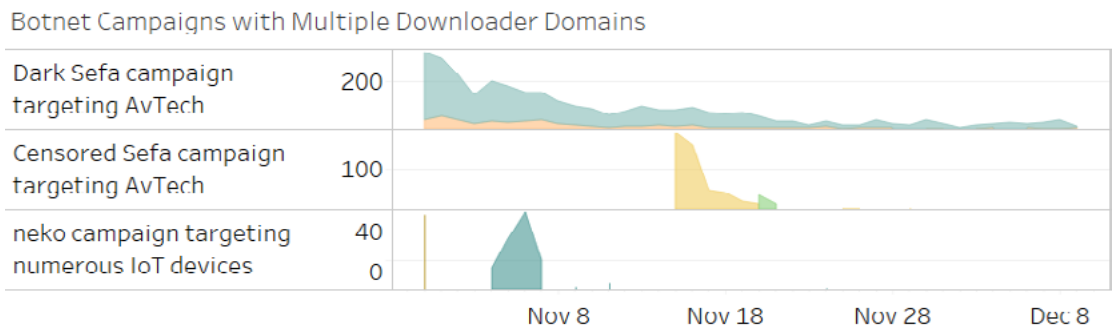
Exploitation Campaigns

The majority of campaign activity appeared to be generated by the Dark Sefa campaign (Figure 19). The campaign targeted AvTech IP cameras, using two different downloader domains. Attacks have tapered since November. An apparent botnet targeting AvTech and D-Link used a ‘Hakai’ user-agent, implying some connection to the Hakai botnet. The Censored Sefa campaign, which targeted AvTech devices, included a payload with an offensive filename.



■ Figure 19: Botnet campaigns observed in 2018.

Some IPs were seen carrying two different hailing domains—allowing the two domains to be linked together as part of a broader campaign (Figure 20). This was the case for the Sefa campaigns where both included “Sefa” in the user agent—they may have been linked, but there is currently no evidence supporting this.



■ Figure 20: Botnets observed using multiple downloader domains.

Another campaign targeting multiple IoT devices was observed utilizing two different hailing domains from October to November. Exploits hailing the domain contained the user agent ‘neko’.

Bruteforce attacks target default credentials on web servers, routers, and switches. Apache, Sun and Microsoft are the most relevant targets and 3COM and Cisco are the most targeted.

Bruteforce Attacks

eSentire Threat Intelligence maintains a honeypot, called ThreatLab, that captures millions of bruteforce login attempts per year. Cross-referencing attempted username and password combinations with a list of default credentials for known technologies yields a sample of targeted vendor technology. Widely used generic credentials (such as root/root) have been removed to increase the accuracy of the relationship between attempted credentials, and devices and software known to utilize those credentials. The remaining data set is then filtered to a Top 10 list based on particular measures described below.

Most Relevant Attack Targets

For the United States, the most relevant attack target was Cisco (Figure 21). Default credentials for many Cisco devices are shared, but prime candidates include switches and routers. The most exposed devices were Apache devices in Germany—though the majority of them are likely Struts instances. Most exposed Tomcat instances were reported as being located in China and the United States where exposure was measured using Shodan.⁴¹

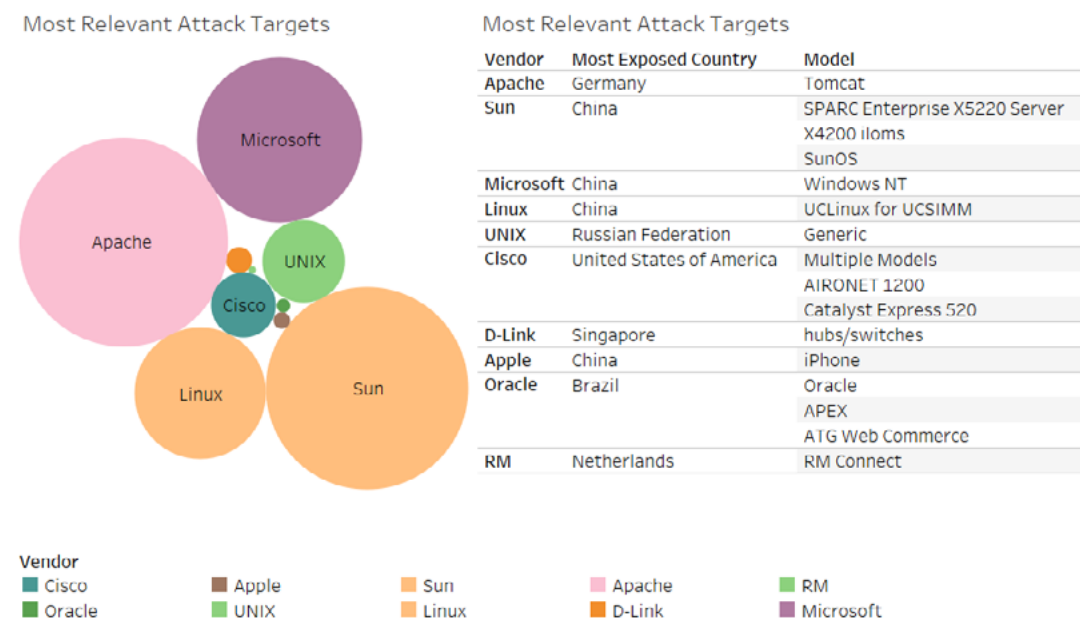
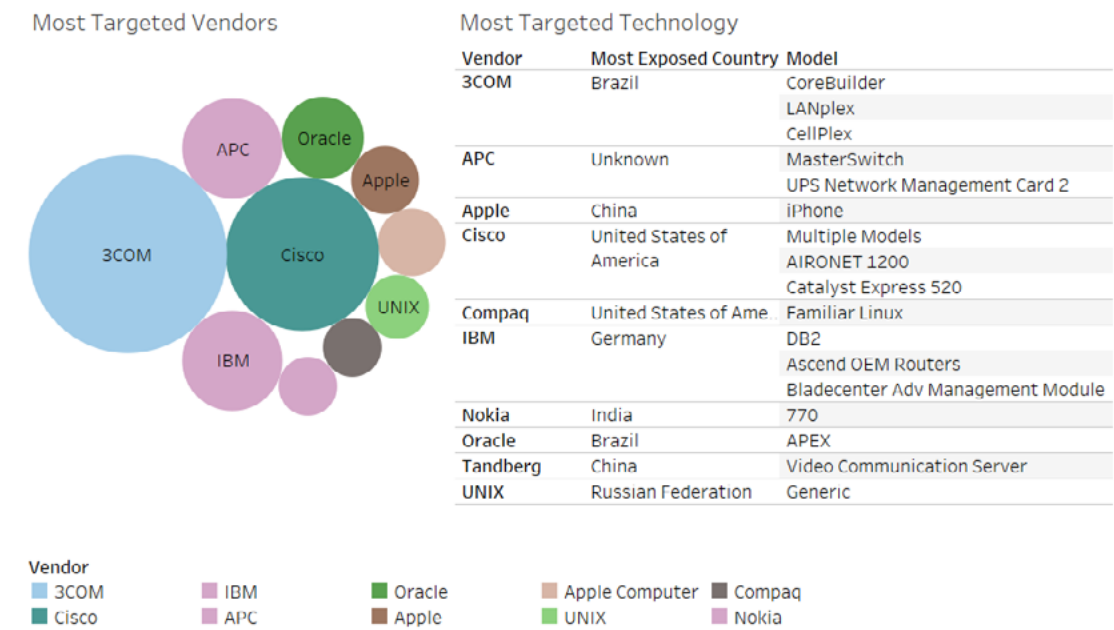


Figure 21: Target technologies exhibiting the most exposure via Shodan [RR].

Home and office devices in China also demonstrated high exposure rates. In particular, systems running desktop Microsoft, Linux and Apple operating systems, implying they are personal or workstation computers.

Most Targeted Vendors

Switches, hubs and routers were the primary target of brute-force attacks using default credentials (Figure 22). Exposed 3COM devices were largely found in Brazil, while Cisco devices were dominant in the United States. IBM routers in Germany may also be at risk.



■ **Figure 22:** Target technologies exhibiting the most exposure via Shodan [RR].

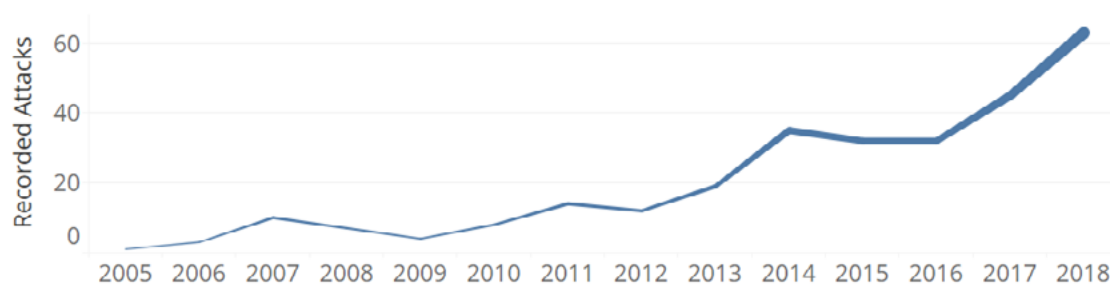
The most targeted vendor is measured by the number of login attempts observed using default credentials unique to that vendor. The full list of attempted credentials is filtered down to the Top 10 most attempted credentials as observed in ThreatLab, giving an idea of attacker preference, regardless of exposure.

SOCIO-POLITICAL CONTEXT IN 2018

Deterrence for financially motivated criminals, hacktivists and hobby hackers is still limited as it remains difficult to attribute and charge individuals for these crimes. There were notable arrests stemming from international law enforcement efforts in 2018, including the arrests of FIN7 members⁴² and the creators of the CTB-Locker ransomware.⁴³ An increase of publicized arrests is important as it highlights that cybercriminals are not immune from law enforcement and dissuades potential criminals.

While eSentire does not track nation-state activity, collateral damage from nation-state actions is not without effect on clients. With nation-state activity ramping up, the risk of an impending malware outbreak increases (Figure 23). Political and social events play a significant role in shaping the threat landscape, both in terms of adversary campaigns and international responses to attacks. The fallout from such activity has consequences beyond the scope of other nation-states and can directly affect the general public. The notorious WannaCry outbreak, for example, had a significant impact on civilians across the globe. WannaCry was an outbreak caused by one nation-state using a sophisticated exploit written by an adversarial nation-state. Now famous, the WannaCry exploit, EternalBlue, has become part of the background internet noise of opportunistic attacks. No such outbreaks were observed in 2018, but mounting nation-state activity may put organizations across the globe at risk, regardless of the industry.

Recorded Nation State Attacks 2005-2018



■ **Figure 23:** Escalation of nation-state attacks. Data for this visual compiled with data from CFR.

TAKEAWAYS AND RECOMMENDATIONS

eSentire Threat Intelligence has several recommendations that organizations can implement to prevent their networks from being compromised by common types of attacks.



Email-based Attacks

Email is one of the most common attack vectors observed by eSentire. Reducing this attack surface will protect your organization from both phishing and email-borne malware.

- User-awareness training for employees
 - » Continuous simulated phishing exercises to assess effectiveness
- Implement a simplified process for reporting and responding to suspicious emails
- Implement spam filtering, URL rewrite and attachment sandboxing
- Only allow email attachments containing trusted file types
- Restrict execution from temporary directories, such as AppData
- Implement tagging for external emails¹
- Enable spoofing protection²
- Block or purchase domain names that are similar to your organization in order to prevent abuse



Malicious Documents

The majority of endpoint infections detected in 2018 leveraged PowerShell and other trusted Microsoft Windows processes for executing code downloaded from the Internet. PowerShell is observed being launched from Microsoft Office documents through CMD.EXE.

- Block Macros in Microsoft Office documents that originate from the internet^{3,4}
- Block Microsoft Office execution from temporary directories such as Outlook and internet browsers
- Set notepad.exe as a default program for scripting file types (.js, .jse, .ps, .vba, etc.)
- Reduce the attack surface associated with PowerShell:
 1. For Windows 10, consider implementing attack surface reduction rule⁵
 2. Block PowerShell via Windows firewall⁶
 3. Prevent version downgrade of PowerShell
 4. Anti-malware Scan Interface (AMSI)
 5. PowerShell script-block logging



Exploits (Webservers, Switches, Routers and IoT Devices)

The number of Internet-connected devices is growing each year significantly, and this growth brings an increased number of exploitable endpoints that threat actors can leverage as part of an attack.

- Work with your IT or security department to implement a regular patching schedule⁷
- Implement monitoring and detection of asset exposure to external networks⁸
- Consider two-factor authentication for externally-facing remote access points

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.

REFERENCES

- [1] <https://www.securit360.com/blog/configure-warning-messages-office-365-emails-external-senders/>
- [2] <https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-spf-in-office-365-to-help-prevent-spoofing>
- [3] <https://cloudblogs.microsoft.com/microsoftsecure/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/>
- [4] <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/using-software-restriction-policies-and-applocker-policies>
- [5] <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard>
- [6] <https://isc.sans.edu/forums/diary/Blocking+Powershell+Connection+via+Windows+Firewall/21829/>
- [7] https://www.acsc.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Applying_Patches.pdf
- [8] <https://www.cisecurity.org/controls/limitation-and-control-of-network-ports-protocols-and-services/>
- [9] <https://dev-admin.esentire.com/resources/knowledge/q2-2018-quarterly-threat-report>
- [10] <https://securelist.com/energetic-bear-crouching-yeti/85345/>
- [11] <https://www.computerworld.com/article/3086849/security/hackers-sold-access-to-170000-compromised-servers-many-in-the-us.html>
- [12] <https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor>
- [13] <https://www.esentire.com/resources/knowledge/2017-q1-threat-summary-report/>
- [14] <https://blog.malwarebytes.com/security-world/2017/12/how-cryptocurrency-mining-works-bitcoin-vs-monero/>
- [15] <https://www.f5.com/labs/articles/threat-intelligence/apache-struts-2-vulnerability--cve-2018-11776--exploited-in-cron>
- [16] <https://www.esentire.com/news-and-events/security-advisories/kaseya-update-cryptocurrency-mining-campaign/>
- [17] <https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-prepare-more-part-1-marap>
- [18] <https://www.managedsolution.com/construction-companies-partner-with-microsoft-and-office-365-to-work-smarter/>
- [19] <https://krebsonsecurity.com/tag/dyre/>
- [20] <https://www.proofpoint.com/us/threat-insight/post/high-volume-dridex-campaigns-return>

REFERENCES

- [21] <https://threatpost.com/stealthy-fake-adobe-flash-updates-tout-malicious-crypto-miners/138199/>
- [22] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
- [23] <https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later>
- [24] <https://threatpost.com/motivation-mystery-behind-wannacry-expetr/126970/>
- [25] <https://www.bleepingcomputer.com/news/security/emotet-trojan-begins-stealing-victims-email-using-new-module/>
- [26] <https://blog.kryptoslogic.com/malware/2018/10/31/emotet-email-theft.html>
- [27] <https://www.us-cert.gov/ncas/alerts/TA18-201A>
- [28] <https://github.com/danielbohannon/Invoke-Obfuscation>
- [29] <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard>
- [30] <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
- [31] <https://www.engadget.com/2018/10/05/california-default-password-ban-information-privacy-connected-devices-bill/>
- [32] https://www.theregister.co.uk/2018/11/20/germany_versus_openwrt_ccc/
- [33] <https://www.exploit-db.com/exploits/44448>
- [34] <https://threatpost.com/d-link-dasan-routers-under-attack-in-yet-another-assault/134255/>
- [35] <https://www.exploit-db.com/exploits/45312/>
- [36] <https://www.exploit-db.com/exploits/44577/>
- [37] <https://www.exploit-db.com/exploits/44992/>
- [38] <https://www.exploit-db.com/exploits/45040/>
- [39] <https://www.exploit-db.com/exploits/45041/>
- [40] <https://www.exploit-db.com/exploits/45038/>
- [41] <https://shodan.io>
- [42] <https://www.reuters.com/article/us-fin7-cyber-us/three-hackers-arrested-in-europe-in-connection-with-tens-of-millions-of-dollars-in-losses-idUSKBN1KM5OJ>
- [43] https://www.washingtonpost.com/local/public-safety/romanian-hackers-arrested-in-international-ransomware-investigation/2017/12/20/44a380b6-e5bc-11e7-833f-155031558ff4_story.html?utm_term=.78a975b65881



eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks 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 \$6 trillion in corporate assets, 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 on Twitter.