Cisco 2017 Midyear Cybersecurity Report

Table of Contents

Executive Summary

For nearly a decade, Cisco has published comprehensive cybersecurity reports that are designed to keep security teams and the businesses they support apprised of cyber threats and vulnerabilities—and informed about steps they can take to improve security and cyber-resiliency. In these reports, we strive to alert defenders to the increasing sophistication of threats and the techniques that adversaries use to compromise users, steal information, and create disruption.

With this latest report, however, we find we must raise our warning flag even higher. Our security experts are becoming increasingly concerned about the accelerating pace of change—and yes, sophistication—in the global cyber threat landscape. That is not to say defenders are not improving their ability to detect threats and prevent attacks, or to help users and organizations avoid or recover more quickly from them. But we see two dynamics undermining their hard-won successes, hindering further progress, and helping to usher in a new era of cyber risks and threats:

The escalating impact of security breaches

Revenue generation is still the top objective of most threat actors. However, some adversaries now have the ability—and often now, it seems, the inclination—to lock systems and destroy data as part of their attack process. As explained in the "Introduction" to the *Cisco 2017 Midyear Cybersecurity Report* on page 7, our researchers see this more sinister activity as a precursor to a new and devastating type of attack that is likely to emerge in the near future: Destruction of service (DeOS).

Within the past year, we have also observed adversaries employing Internet of Things (IoT) devices in DDoS attacks. Botnet activity in the IoT space suggests some operators may be focused on laying the foundation for a wide-reaching, high-impact attack that could potentially disrupt the Internet itself.

The pace and scale of technology

Our threat researchers have been monitoring for years how mobility, cloud computing, and other technology advancements and trends are stretching and eroding the security perimeter that enterprises must defend. What they can see even more clearly today, however, is how malicious actors are taking advantage of that ever-expanding attack surface. The breadth and depth of recent ransomware attacks alone demonstrate how adept adversaries are at exploiting security gaps and vulnerabilities across devices and networks for maximum impact.

Lack of visibility into dynamic IT environments, the risks presented by "shadow IT," the constant barrage of security alerts, and the complexity of the IT security environment are just some reasons resource-strapped security teams struggle to stay on top of today's evasive and increasingly potent cyber threats.

What we cover in this report

The *Cisco 2017 Midyear Cybersecurity Report* explores the above dynamics through the discussion of:

Adversary tactics

We examine select methods that threat actors are using to compromise users and infiltrate systems. It is important for defenders to understand changes in adversaries' tactics so that they can, in turn, adapt their security practices and educate users. Topics covered in this report include new developments in malware, trends in web attack methods and spam, the risks of potentially unwanted applications (PUAs) like spyware, business email compromise (BEC), the changing economics of malicious hacking, and medical device compromise. Our threat researchers also offer analysis of how—and how quickly—some adversaries are evolving their tools and techniques, and deliver an update on Cisco's efforts to reduce our Time to Detection (TTD) of threats.

Vulnerabilities

In this report, we also provide an overview of vulnerabilities and other exposures that can leave organizations and users susceptible to compromise or attack. Weak security practices, such as not moving swiftly to patch known vulnerabilities, not limiting privileged access to cloud systems, and leaving infrastructure and endpoints unmanaged, are discussed. Also in focus: Why the expanding IoT and the convergence of IT and operational technology (OT) create even more risk for organizations and their users, as well as for consumers, and what defenders should do now to address these risks before they are impossible to manage.

Opportunities for defenders

The *Cisco 2017 Midyear Cybersecurity Report* presents additional findings from Cisco's latest Security Capabilities Benchmark Study. We offer in-depth analysis of the key security concerns of eight industry verticals: Service providers, public sector, retail, manufacturing, utilities, healthcare, transportation, and finance. Industry experts from Cisco offer recommendations on how these businesses can improve their security posture, including using services to bridge knowledge and talent gaps, reducing complexity in their IT environment, and embracing automation.

The concluding section of the report includes a call to action for security leaders to seize the opportunity to engage senior executives and boards of directors in discussions about cybersecurity risks and budgets—and offers suggestions for how to start that conversation.

Acknowledgments

We would like to thank our team of threat researchers and other subject-matter experts from within Cisco, as well as our technology partners, who contributed to the *Cisco 2017 Midyear Cybersecurity Report*. Their research and perspectives are essential to helping Cisco provide the security community, businesses, and users with relevant insight into the complexity and vastness of the modern, global cyber threat landscape, and present best practices and knowledge for improving their defenses.

Our technology partners also play a vital role in helping our company to develop simple, open, and automated security that allows organizations to integrate the solutions they need to secure their environments.

For a full list of the contributors to the *Cisco 2017 Midyear Cybersecurity Report*, which includes our technology partners, see page 85.

Major Findings

- Business email compromise (BEC) has become a highly lucrative threat vector for attackers. According to the Internet Crime Complaint Center (IC3), US$5.3 billion was stolen due to BEC fraud between October 2013 and December 2016. In comparison, ransomware exploits took in US$1 billion in 2016.
- Spyware that masquerades as potentially unwanted applications (PUAs) is a form of malware—and a risk that many organizations underestimate or dismiss completely. However, spyware can steal user and company information, weaken the security posture of devices, and increase malware infections. Spyware infections are also rampant. Cisco threat researchers studied three select spyware families and found that they were present in 20 percent of the 300 companies in the sample.
- The Internet of Things (IoT) holds great promise for business collaboration and innovation. But as it grows, so too does security risk. Lack of visibility is one problem: Defenders are simply not aware of what IoT devices are connected to their network. They need to move quickly to address this and other hurdles to IoT security. Threat actors are already exploiting security weaknesses in IoT devices. The devices serve as strongholds for adversaries, and allow them to move laterally across networks quietly and with relative ease.
- Cisco has been tracking our median time to detection (TTD) since November 2015. Since that time, the overall trend has been downward—from just over 39 hours at the start of our research to about 3.5 hours for the period from November 2016 to May 2017.
- Cisco has been observing an overall increase in spam volume since mid-2016, which seems to coincide with a significant decline in exploit kit activity during the same period. Adversaries who had relied heavily on exploit kits to deliver ransomware are turning to spam emails, including those containing macro-laden malicious documents that can defeat many sandboxing technologies because they require user interaction to infect systems and deliver payloads.
- Supply chain attacks offer adversaries a way to spread malware to many organizations through a single compromised site. In an attack studied by RSA, a Cisco partner, a software vendor's download webpage was compromised, allowing the infection to spread to any organization that downloaded the software from this vendor.
- The dramatic increase in cyber attack frequency, complexity, and size over the past year suggests that the economics of hacking have turned a corner, according to Radware, a Cisco partner. Radware notes that the modern hacking community is benefiting from quick and easy access to a range of useful and low-cost resources.
- When it comes to enterprise security, cloud is the ignored dimension: Open authorization (OAuth) risk and poor management of single privileged user accounts create security gaps that adversaries can easily exploit. Malicious hackers have already moved to the cloud and are working relentlessly to breach corporate cloud environments, according to Cisco threat researchers.
- In the exploit kit landscape, activity has declined dramatically and innovation has stagnated since Angler and other leading players have disappeared or changed their business model. This situation is likely temporary, given previous patterns in this market. But other factors, such as the greater difficulty of exploiting vulnerabilities in files built with Adobe Flash technology, may be slowing the resurgence.
- DevOps services that have been deployed improperly or left open intentionally for convenient access by legitimate users pose a significant risk to organizations, according to research by Rapid7, a Cisco partner. In fact, many of these instances have already been ransomed.
- A ThreatConnect analysis of colocated domains used by adversaries connected to the Fancy Bear cyberespionage group showed the value of studying bad actors' IP infrastructure tactics. By studying this infrastructure, defenders gain a larger list of domains, IP addresses, and email addresses to proactively block.
- In late 2016, Cisco threat researchers discovered and reported three remote code-execution vulnerabilities in Memcached servers. A scan of the Internet a few months later revealed that 79 percent of the nearly 110,000 exposed Memcached servers previously identified were still vulnerable to the three vulnerabilities because they had not been patched.

Introduction

Introduction

The threat landscape is always changing. But the rapid evolution of threats and the magnitude of the attacks that Cisco's threat researchers and technology partners have been observing of late are troubling. There is a sense throughout the security community that actors in the shadow economy may be carefully laying the groundwork for campaigns that not only will have far-reaching impact, but also will be extremely difficult to recover from.

The new strategy: Destruction of service (DeOS)

Adversaries now seek to eliminate the "safety net" that organizations rely on to restore their systems and data following malware infestations, a ransomware campaign, or any other cyberincident that severely disrupts their operations. How DeOS attacks will play out and what they will look like depends on the threat actors' core motivations and the limits of their creativity and capabilities.

What we can be sure of is that the emerging Internet of Things (IoT), and its myriad devices and systems with security weaknesses ripe for exploitation, will play a central role in enabling these campaigns of escalating impact. The IoT is a bold new frontier for attackers and defenders in their arms race.

Meanwhile, on the old and familiar playing field, adversaries face constrained time and space to operate. They must pivot constantly from one strategy to another to evade detection. They must innovate quickly to escalate the effectiveness of their threats, as they have done by using Bitcoin and Tor to make ransomware more effective. They also find they must turn—or return—to tactics such as malicious email and social engineering when the efficacy of go-to tools for moneymaking, like exploit kits, is diluted by defenders or a lack of innovation in the marketplace.

The key: Reducing the fragmented security toolbox

Defenders can point to victories, but they must always assume that attackers will continue to dodge their threat defenses. To slow down attackers and constrain their operational time and space, defenders already have most of the solutions they need. The problem is how they use them. Security professionals in every industry report that they deploy many tools from many vendors—a complicated approach to security, when it should be seamless and holistic.

A fragmented and multiproduct security approach hinders an organization's ability to manage threats. It also exponentially increases the number of security triggers that resource-strapped security teams must review. When security teams can consolidate the number of vendors used—and adopt an open, integrated, and simplified approach to security—they can reduce their exposure to threats. They can also better prepare their organizations to meet the security challenges of the rapidly emerging IoT world and the data protection requirements of the General Data Protection Regulation (GDPR) that becomes enforceable in May 2018.

Attacker Behavior

ATTACKER BEHAVIOR

This section provides an overview of trends in the evolution and innovation of threats that adversaries employ for web- and email-based attacks. Cisco threat researchers and technology partners present their research, observations, and insights to help business leaders and their security teams understand the tactics that adversaries might use to target their organizations in the coming months—and as the IoT takes shape. We also provide recommendations for making security improvements that can help to reduce business and user exposure to these risks.

Exploit kits: Down, but not likely out

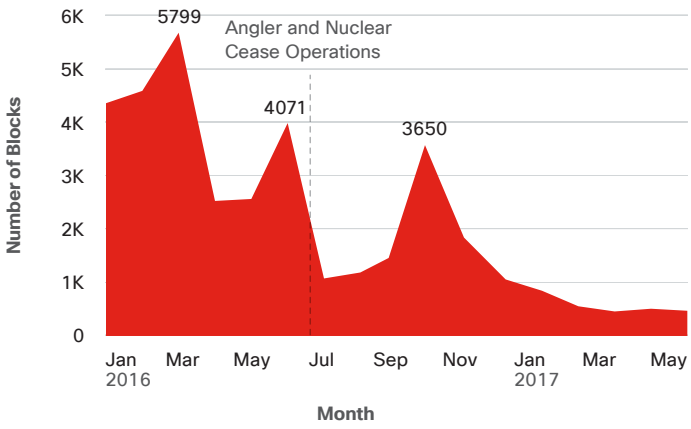
In 2016, three leading exploit kits—Angler, Nuclear, and Neutrino—abruptly vanished from the threat landscape.[1] Angler and Nuclear have not returned. Neutrino's disappearance was only temporary: The exploit kit is still active but resurfaces only for short periods. Its authors rent it to select operators in exclusive arrangements. This approach helps to contain Neutrino's activity so it doesn't become too prevalent—and easier to detect.

In the *Cisco 2017 Annual Cybersecurity Report*, we explained how these dramatic changes in the exploit kit landscape presented opportunities for smaller players and new entrants to make their mark. But as of mid-2017, no one appears to be seizing them. Only a handful of exploit kits are active. RIG, which has been a leading exploit kit for some time, is the most visible in the landscape; it is known to target vulnerabilities in Adobe Flash, Microsoft Silverlight, and Microsoft Internet Explorer technologies.

Overall, exploit kit activity has been declining dramatically since January 2016, as Figure 1 shows.

This trend echoes what we observed after the author and distributor of the pervasive Blackhole exploit kit was arrested in Russia.[2] When Blackhole subsequently ceased operations, it had a tremendous impact on the exploit kit market, and it took time for new leaders to emerge. The big winner of that race was Angler, which took the sophistication of exploit kits and drive-by downloads to a new level.[3]

Figure 1 Exploit kit activity



Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

1 *Cisco 2016 Midyear Cybersecurity Report*: cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.
2 "Meet Paunch: The Accused Author of the Blackhole Exploit Kit," by Brian Krebs, KrebsonSecurity blog, December 6, 2013: krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/.
3 "Connecting the Dots Reveals Crimeware Shake-Up," by Nick Biasini, Talos blog, July 7, 2016: blog.talosintelligence.com/2016/07/lurk-crimeware-connections.html.

Angler targeted many vectors. Its authors were innovative, and they moved faster than everyone else in the marketplace to include new vulnerabilities in their exploit kit. In many ways, they raised the bar for other players in the space—and drove data and technique-stealing between other kits determined to stay competitive. Now that Angler is gone, innovation among exploit kits appears to have hit a slump.

Angler's exit is only one likely cause for this stagnation. Another is that Flash technology has become harder to exploit. Flash vulnerabilities helped to grow and sustain the exploit kit market for years. But heightened awareness about those vulnerabilities and faster patching by defenders make the software harder to exploit. Adversaries now often find they must target multiple vulnerabilities to exploit a system.

Automatic security updates in modern operating systems and web browsers are also helping to shield users from exploit kit compromise. Another trend: Cybercriminals, likely in response to the shifts in the exploit kit marketplace, have been turning to (or back to) email to deliver ransomware and other malware quickly and cost-effectively. They are also getting creative with their methods to evade detection. For example, Cisco threat researchers have observed growth in spam containing macro-laden malicious documents, including Word documents, Excel files, and PDFs, that can defeat many sandboxing technologies by requiring user interaction to infect systems and deliver payloads.[4]

A quiet evolution underway?

There is little doubt that we will see a resurgence in the exploit kit market, given that crimeware is an industry worth billions. As soon as a new attack vector emerges that is easy to exploit and can affect users at scale, the popularity of exploit kits will rise again—and so will competition and innovation.

Defenders must therefore remain vigilant. Many exploit kits are still in operation and remain effective at compromising users and delivering malware to end systems. These threats can strike at any time in any environment. All it takes is one vulnerability on one system for an exploitation to occur. Organizations that are diligent about patching vulnerabilities swiftly—especially vulnerabilities in web browsers and associated browser plug-ins—and practice defense in depth can mitigate this risk. Making sure users employ secure browsers and disable and remove unnecessary web plug-ins can also greatly reduce exposure to the exploit kit threat.

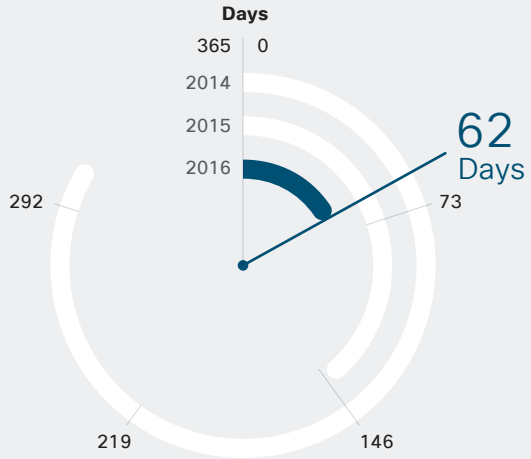
4 "Threat Spotlight: Mighty Morphin Malware Purveyors: Locky Returns via Necurs," by Nick Biasini, Talos blog, April 21, 2017: blogs.cisco.com/security/talos/locky-returns-necurs.

How defender behavior can shift attackers' focus

More timely patching of known vulnerabilities in Flash software by defenders is one factor that's been helping to slow growth and innovation in the exploit kit market. As discussed in previous cybersecurity reports from Cisco, Flash software has long been an attractive web attack vector for adversaries who want to exploit and compromise systems. However, it is becoming increasingly difficult to exploit due, in part, to better patching practices.

Research from network security and vulnerability management firm Qualys, a Cisco partner, shows that defenders have significantly reduced the time needed to patch 80 percent of known Flash vulnerabilities in their organization from 308 days in 2014, to 144 days in 2015, to 62 days in 2016, on average (see Figure 2). The research is based on data sourced from the more than 3 billion vulnerability scans that Qualys conducts annually across its global base.

Figure 2 Number of days required to patch 80% of Flash vulnerabilities



Source: Qualys

As defenders move faster to patch new vulnerabilities in Flash software, some exploit kit authors might shift their focus to exploiting older vulnerabilities that may have been overlooked. Security teams should therefore take time to assess whether all known Flash vulnerabilities have been addressed, and to prioritize patching critical vulnerabilities that place the organization at risk.

Also, some adversaries who have relied on exploit kits that target Flash software to deliver their ransomware and other malware are likely to increase their use of other techniques, at least in the short term, so that they can continue to meet their revenue targets.

For example, Cisco threat researchers have observed growth in spam emails with seemingly benign attachments that contain malicious macros (see "Malware evolution: A 6-month perspective," page 23). That trend appears to coincide with the recent decline in exploit kit activity (for more on this topic, see "Exploit kits: Down, but not likely out," page 9).

Web attack methods provide evidence of a mature Internet

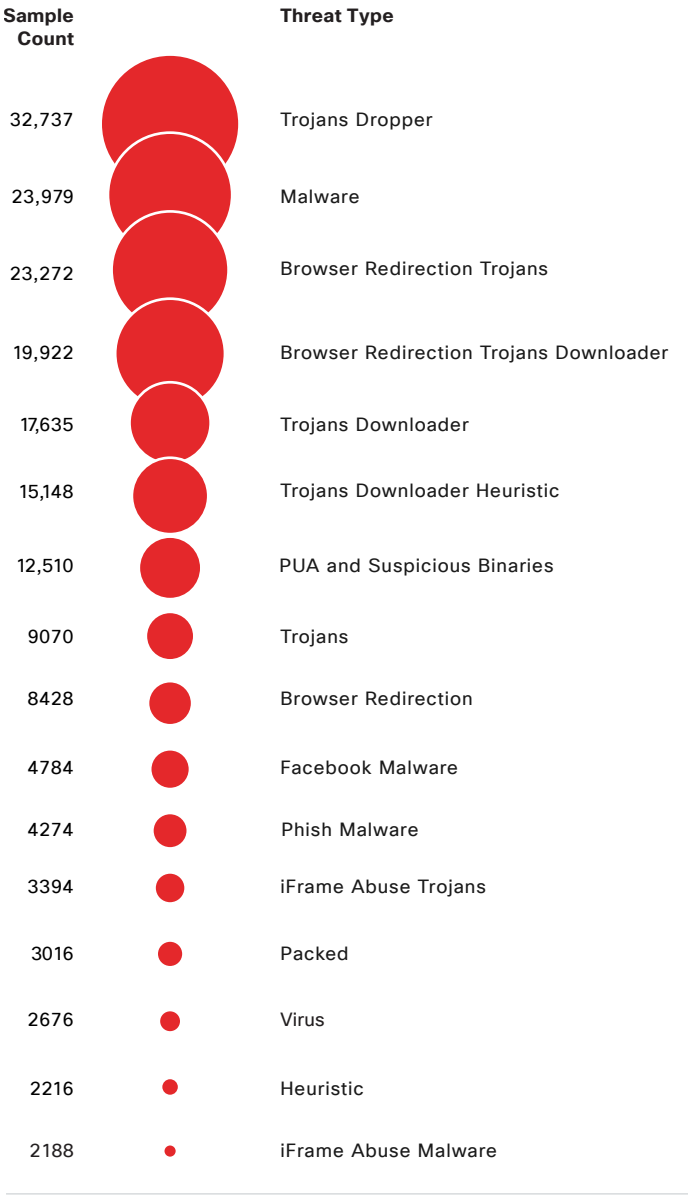
Proxies have been around since the nascent years of the web, and their functionality has matured right along with the Internet. Today, defenders employ proxies in content scanning to help detect potential threats looking for vulnerable Internet infrastructure or network weaknesses that allow adversaries to gain access to users' computers, infiltrate organizations, and carry out their campaigns. These threats include:

- Potentially unwanted applications (PUAs), such as malicious browser extensions
- Trojans (droppers and downloaders)
- Links to web spam and ad fraud
- Browser-specific vulnerabilities, such as JavaScript and graphics-rendering engines
- Browser redirects, clickjacking, and other methods used to direct users to malicious web content

Figure 3 shows the most common malware types that adversaries used from November 2016 through May 2017. To create the chart, Cisco threat researchers used our company's managed web security logs. The list in Figure 3 features a range of some of the most reliable and cost-effective methods for compromising large populations of users and infecting computers and systems. They include:

- "First-stage payloads" like Trojans and utilities that facilitate the initial infection of a user's computer. (A macro virus in a malicious Word document is an example of this type of tool.)
- PUAs, which include malicious browser extensions.
- Suspicious Windows binaries, which deliver threats such as adware and spyware.[5]
- Facebook scams, which include fake offers, media content, and survey scams.
- Malware, such as ransomware and keystroke-stealing agents, that deliver payloads to compromised hosts.

Figure 3 Most commonly observed malware (top malicious blocks), November 2016–May 2017

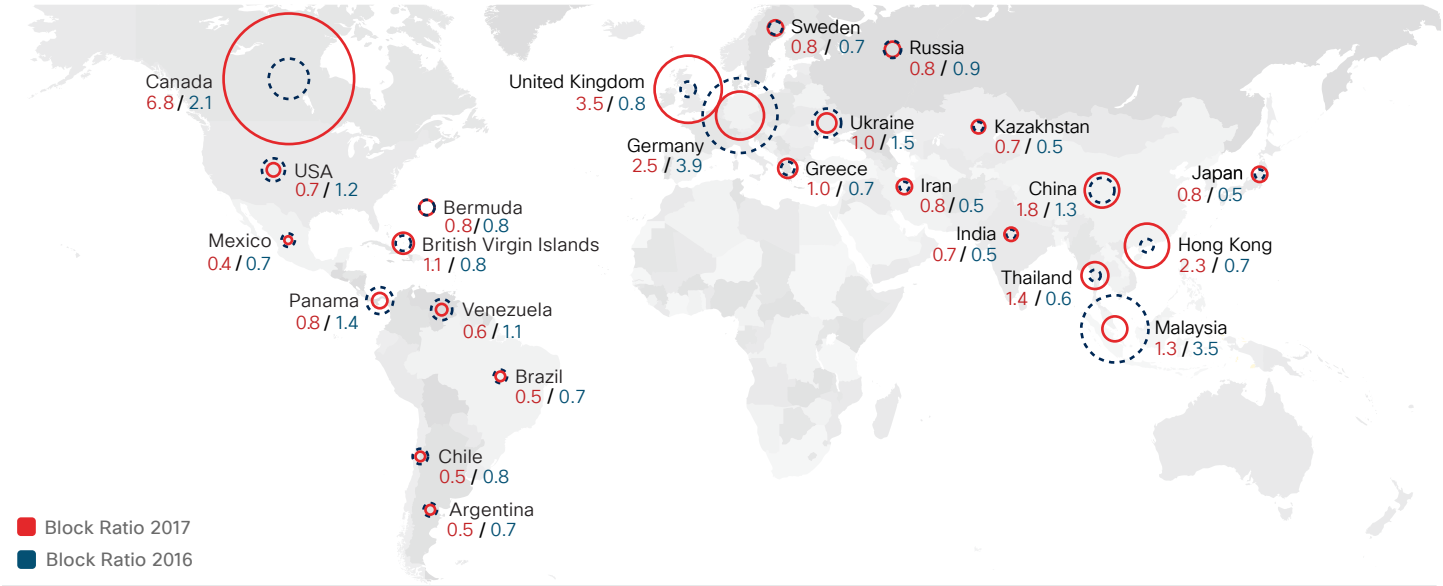


Source: Cisco Security Research

5 Note: In the *Cisco 2017 Annual Cybersecurity Report* (available at b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153), Cisco threat researchers warned that malicious adware, which includes ad injectors, browser-settings hijackers, utilities, and downloaders, is a growing problem. In this report, on page 14, we examine the risks that PUAs like spyware present to users and organizations.

All the above appear regularly on our lists of most commonly observed malware. The consistency in the lineup suggests that the Internet has matured to the point where adversaries know, with certain confidence, which web attack methods will be most effective at compromising users at scale and with relative ease. Using secure browsers and disabling or removing unnecessary browser plug-ins remain two of the most important ways for users to reduce their exposure to common web-based threats.

Figure 4 Web blocks global, November 2016–May 2017



Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Web block activity around the globe

Cisco tracks malware-based block activity originating by country or region. Adversaries frequently shift their base of operation, searching for weak infrastructures from which they can launch their campaigns. By examining overall Internet traffic volume and block activity, Cisco threat researchers can offer insight on where malware is originating.

We select the countries for our study based on their volume of Internet traffic. A "block ratio" value of 1.0 indicates that the number of blocks we see is proportional to network size. Countries and regions that have block activity that we consider higher than normal likely have many web servers and hosts with unpatched vulnerabilities on their networks. The chart above shows web block activity around the globe.

Spyware really is as bad as it sounds

Much of today's advertising software online known as potentially unwanted applications (PUAs) is spyware. Spyware vendors promote their software as legitimate tools that provide useful services and abide by end-user license agreements. But no matter how they try to spin it, spyware is nothing more than malware.

Spyware masquerading as PUAs is software that collects and transmits information about the user's computer activities covertly. It is usually installed on a computer without the user's knowledge. For the purposes of this discussion, we put spyware in three broad categories: Adware, system monitors, and Trojans.

In the corporate environment, spyware presents a range of potential security risks. For example, it can:

- Steal user and company information, including personally identifiable information (PII) and other sensitive or confidential information.
- Weaken the security posture of devices by modifying their device configurations and settings, installing additional software, and allowing third-party access. Spyware can also potentially enable remote code execution on devices, allowing attackers to fully control the device.
- Increase malware infections. Once users are infected with PUAs like spyware or adware, they are vulnerable to even more malware infections.

To better understand spyware infections, Cisco researchers studied the network traffic of about 300 companies from November 2016 to March 2017 to determine what types of spyware families are present in organizations and to what extent.

Through our research, we found that three spyware families affected more than 20 percent of the companies in our sample during the period observed: Hola, RelevantKnowledge, and DNSChanger/DNS Unlocker. On a monthly basis, the infections were identified in more than 25 percent of all the organizations in our sample (see Figure 5).

There are hundreds of spyware families. But we focused on these three specific families because, while they are not new, they were the most commonly observed "brands" in the corporate environments we observed. Following are more details about these three spyware families.

Figure 5 Percentage of companies affected by selected spyware families, November 2016–March 2017

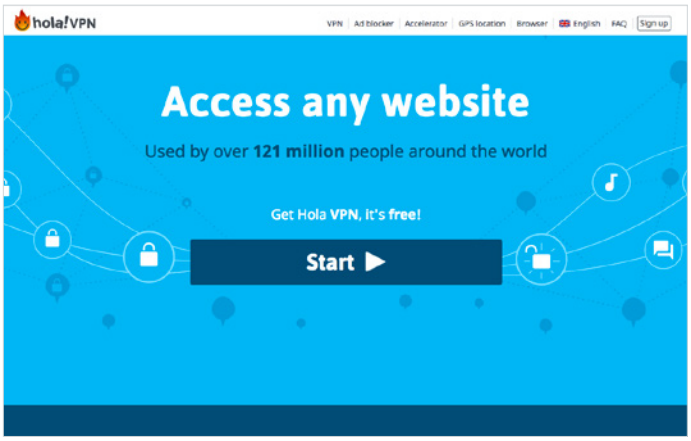
Source: Cisco Security Research

Hola VPN

Hola (spyware and adware) is a freemium web and mobile application that provides a form of VPN to its users through a peer-to-peer network. It also uses peer-to-peer caching, making users "store" content downloaded by other users. Hola is distributed as a client-side browser-based application. The software is available either as a browser extension or a standalone application.

The screenshot of Hola's website in Figure 6 shows how the spyware's operators are marketing the spyware as a free, helpful service that lets users "access any website." They also claim that Hola is "used by over 121 million people around the world."

Figure 6 Screenshot of Hola VPN's homepage



Why it is considered spyware: Hola's functionality includes, among other things, selling users' bandwidth through a service called Luminati, installing its own code-signing certificate on users' systems, downloading any file with an option to bypass antivirus checking, and running code remotely.

RelevantKnowledge

RelevantKnowledge (spyware and system monitor) collects mass quantities of information about Internet browsing behavior, demographics, systems, and configurations. RelevantKnowledge may be installed directly or through software bundles, sometimes without direct user consent.

Figure 7 Screenshot of RelevantKnowledge's homepage

Like Hola, its homepage (Figure 7) features messaging designed to make users feel good about signing up for the service. For example, the spyware operators claim that they will make a tree donation to "Trees for Knowledge" in honor of every member.

Why it is considered spyware: As mentioned earlier, RelevantKnowledge can install software without a user's consent. Also, it collects information to create user profiles that are sold, anonymously, either individually or as part of aggregate data, to third parties for "research" purposes.

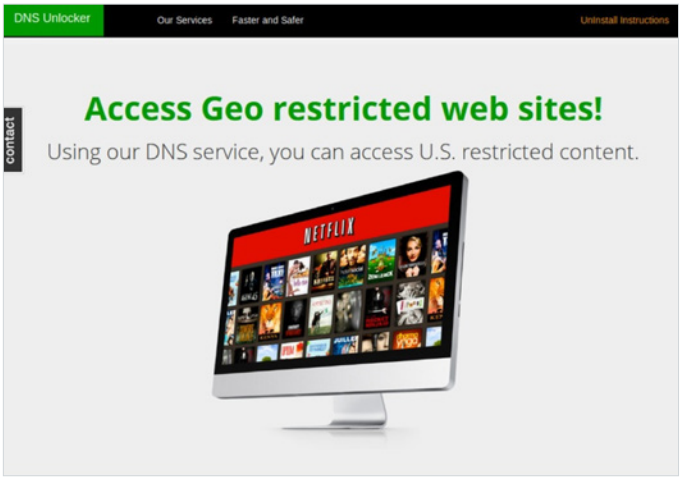
DNS Changer and DNS Unlocker

DNS Changer and DNS Unlocker are two versions of the same malicious software. The former is a Trojan that changes or "hijacks" the DNS settings on the infected host.[6] DNS Unlocker is an adware service that provides an uninstall option.

The spyware replaces the nameservers with its own nameservers to direct HTTP and other requests from the host to a set of attacker-controlled servers that can intercept, inspect, and modify host traffic. It infects endpoints, not browsers. By using PowerShell, an object-oriented programming language and interactive command-line shell for Microsoft Windows, it can run commands on the infected host. That opens the door to remote access by the attackers.

The operators of DNS Unlocker promote the spyware as a service that lets users access geo-restricted content, such as streaming video.

Figure 8 Screenshot of DNS Unlocker's homepage

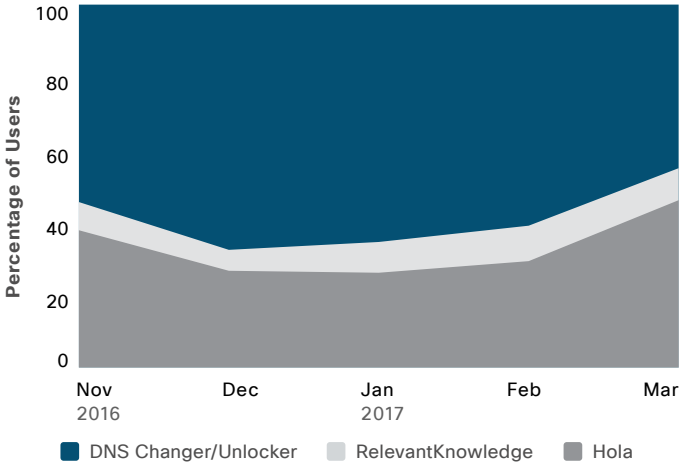


Why it is considered spyware: In addition to the functionality listed above and other capabilities, DNS Unlocker can steal PII, redirect user traffic, and modify user content on the fly by injecting content on specific services, like online advertising.

Study shows DNS Unlocker is the most prevalent

Of the three families that we focused on in our study, DNS Unlocker is the most prevalent. It is responsible for more than 40 percent of monthly spyware infections in the companies in our sample.

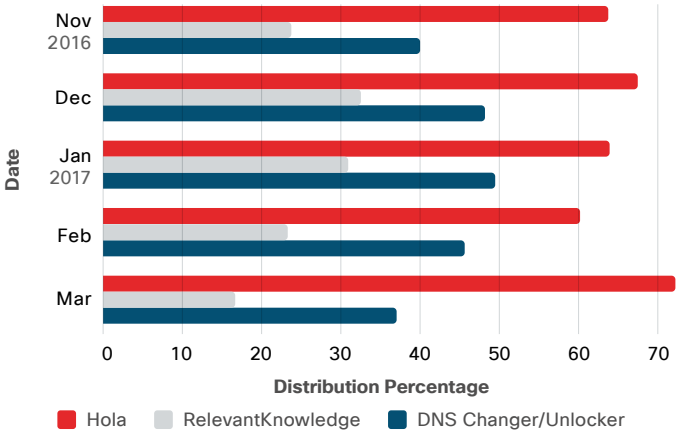
Figure 9 Comparison of affected users per spyware family



Source: Cisco Security Research

6 "DNSChanger Outbreak Linked to Adware Install Base," by Veronica Valeros, Ross Gibb, Eric Hulse, and Martin Rehak, Cisco Security blog, February 10, 2016: blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base.

Figure 10 Spyware distribution



Source: Cisco Security Research

Among the three families, we found that Hola is the most distributed—affecting more than 60 percent of the organizations in our sample monthly during the period observed (see Figure 10). This spyware family is also becoming more distributed over time, albeit slowly.

DNS Unlocker, meanwhile, affects more users overall, but across fewer organizations (Figure 10). In January, the number of infections related to this spyware family had increased significantly from the rate seen in November, but has been declining since, according to our researchers.

Spyware infections must be taken seriously

Spyware infections are rampant in many organizations, but are not typically considered a significant security risk. However, like adware infections—which we found in three-quarters of the companies we surveyed in another recent study[7]—spyware infections can place users and organizations at risk for malicious activity.

Although operators may market spyware as services designed to protect or otherwise help users, the true purpose of the malware is to track and gather information about users and their organizations—often without users' direct consent or knowledge. Spyware companies are known to sell or provide access to the data they collect, allowing third parties to harvest information with relative anonymity. That information can be used to identify critical assets, map internal infrastructures in organizations, and orchestrate targeted attacks.

Spyware infections on browsers and endpoints must be remediated quickly. Security teams must maintain active awareness of spyware capabilities and determine what type of information is at risk. They should also take the time to develop a playbook for remediating spyware, adware, and riskware[8] infections and for educating end users about the risk of PUAs. Before accepting end-user license agreements for any PUA, users should, at minimum, take a moment to scan sections on how their information will be collected, stored, and shared.

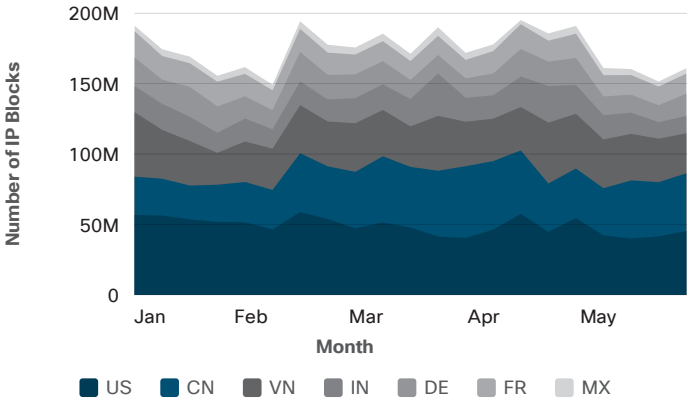
Not viewing spyware masquerading as PUAs as a form of malware can lead to more infections and security risks. The spyware problem is poised to grow, as operators incorporate more malicious capabilities into their software and continue to take advantage of the lack of remediation inside organizations.

7 To see our previous reporting on this topic, download the *Cisco 2017 Annual Cybersecurity Report*, available at: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.
8 Riskware is legitimate software that could be modified by malicious actors and used for nefarious purposes.

Decline in exploit kit activity likely influencing global spam trends

Cisco threat researchers observed an increase in IP connection blocks coming from the Chinese IP space from January to May 2017. Overall spam volumes in the first half of the year have declined and are steadying from the spam volume highs that peaked toward the end of 2016.

Figure 11 IP blocks by country



Source: Cisco Security Research

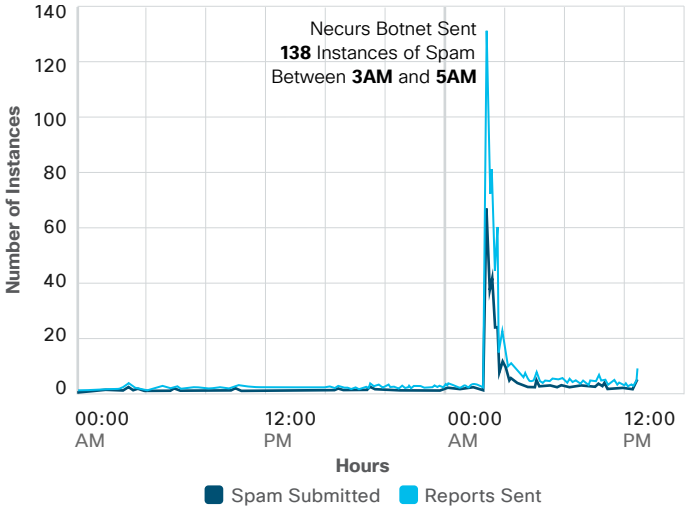
The overall increase in spam volume our threat researchers have observed since August 2016[9] appears to coincide with the significant decline in exploit kit activity that began around the same time. Adversaries have been turning to other tried-and-true methods, like email, to distribute ransomware and malware and generate revenue (see "Exploit kits: Down, but not likely out," page 9).

Cisco threat researchers anticipate that the volume of spam with malicious attachments will continue to rise while the exploit kit landscape remains in flux. Email has the potential to go straight to the endpoint. Adversaries also can count on "help" from unsuspecting users to move their campaigns beyond the inbox. Through crafty social engineering (phishing or more targeted spear phishing), they can easily dupe users and eventually compromise entire organizations.

Some adversaries are also relying on spam emails containing macro-laden malicious documents to deliver ransomware. These threats can defeat many sandboxing technologies because they require some type of positive user interaction, such as clicking "OK" on a dialog box, to infect systems and deliver payloads (see "Malware evolution: A 6-month perspective," page 23).

Spam-sending botnets—especially the massive botnet Necurs—are also thriving and contributing to the overall increase in global spam volume. Earlier this year, Necurs was sending penny stock "pump-and-dump" spam, to great effect, and focusing less on distributing spam containing sophisticated threats like ransomware.[10] Figure 12, an internal graph generated by Cisco's SpamCop service, shows an example of this type of activity by Necurs. That the botnet's owners are relying heavily on these low-quality spam campaigns suggest that these less resource-intensive efforts are successfully generating revenue.

Figure 12 Necurs "pump-and-dump" spam activity (over 24 hours)



Source: SpamCop

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

More recently, the Necurs botnet was sending Jaff, a new variant of ransomware, through multiple, large-scale malicious spam email campaigns. The emails included a PDF attachment with an embedded Microsoft Word document functioning as the initial downloader for the Jaff ransomware.[11]

9 To see our previous reporting on this topic, download the *Cisco 2017 Annual Cybersecurity Report*, available at: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

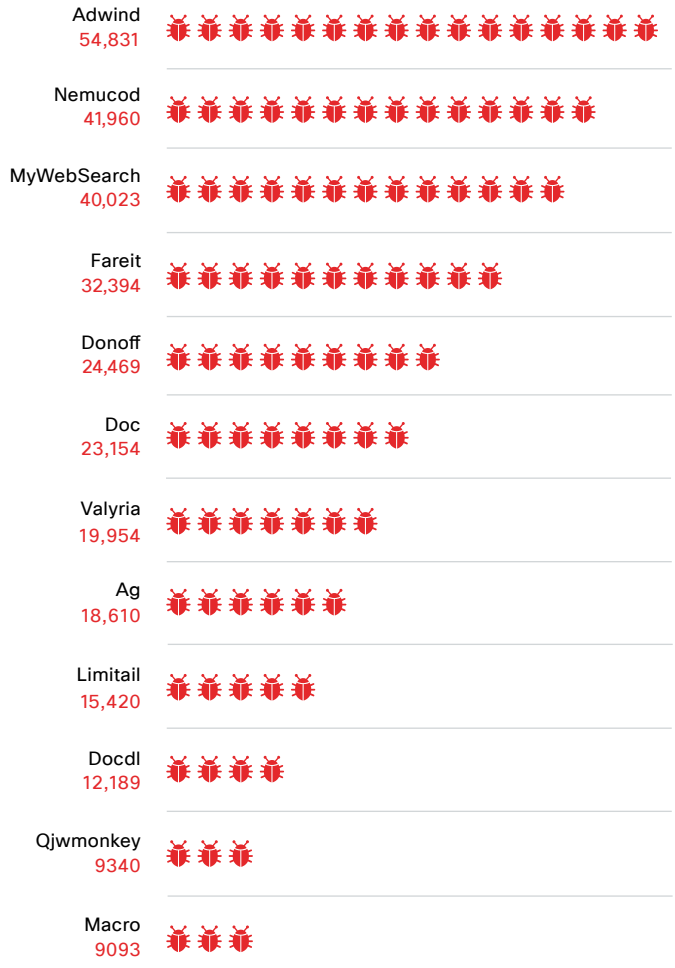
10 "Necurs Diversifies Its Portfolio," by Sean Baird, Edmund Brumaghin, and Earl Carter, with contributions from Jaeson Schultz, Talos blog, March 20, 2017: blog.talosintelligence.com/2017/03/necurs-diversifies.html.

11 "Jaff Ransomware: Player 2 Has Entered the Game," by Nick Biasini, Edmund Brumaghin, and Warren Mercer, with contributions from Colin Grady, Talos blog, May 12, 2017: blog.talosintelligence.com/2017/05/jaff-ransomware.html.

Malicious email: A closer look at malware authors' file type strategies

As more cybercriminals turn—or return—to email as a primary vector for spreading ransomware and other malware, Cisco threat researchers are tracking the file types that top malware families employ. That knowledge helps us to reduce our time to detection (TTD) of known threats as well as to track the different ways malware operators are evolving their threats, which includes changing file extension types (see page 26 for more on TTD; see also "Time-to-evolve trends: Nemucod, Ramnit, Kryptik, and Fareit," on page 28).

Figure 13 Most commonly detected malware families by count



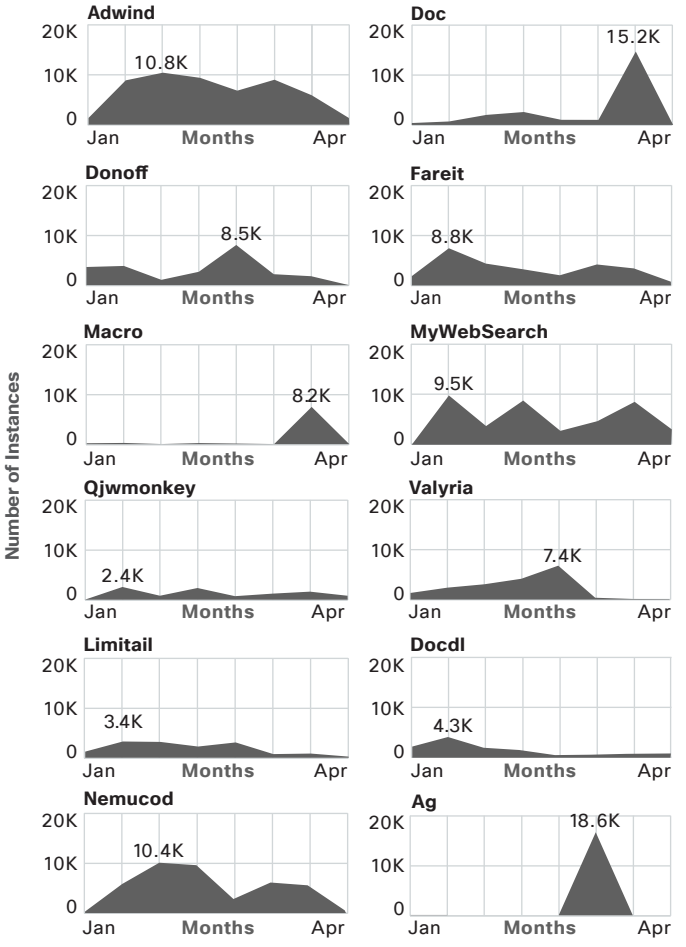
Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

We analyzed malware detections from January through April 2017 to identify the top 20 malware families observed (by count) in malicious email payloads during that period (see Figure 13).

Figure 14 shows the number of detections, by family, that included a malicious payload file extension, such as .zip or .exe. Note the significant spike in macro-related malware in April, which is the traditional tax season in several countries, including the United States and Canada (for more about spam with macro-laden malicious documents, see "Malware evolution: A 6-month perspective," on page 23).

Figure 14 Patterns of top malware families, 2017

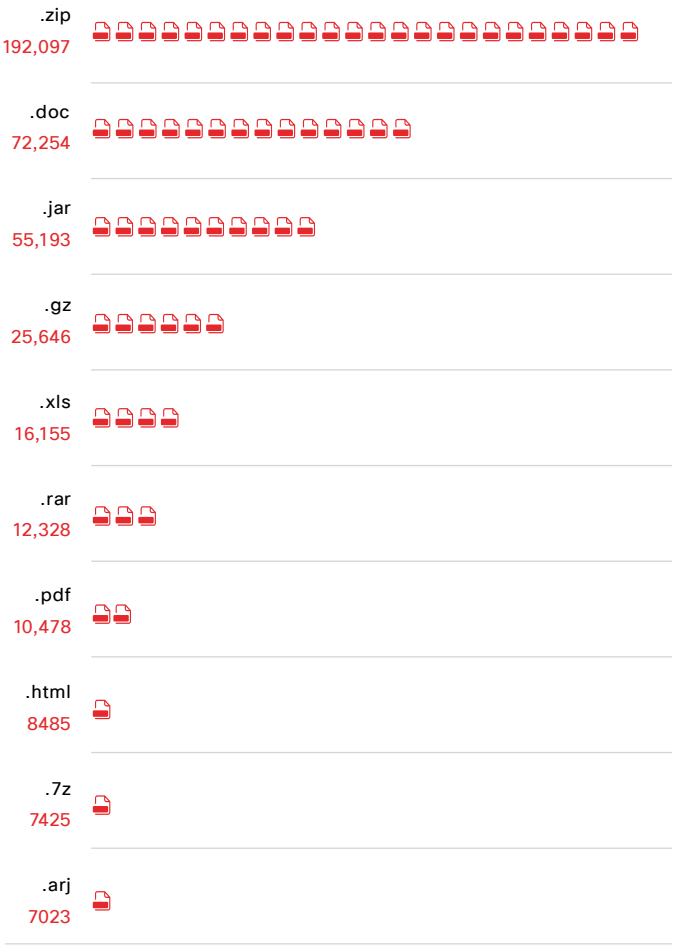


Source: Cisco Security Research

We also looked at counts by payload attachment to compile a list of the most commonly seen malicious file extensions in email documents (see Figure 15). Malicious .zip files were the most dominant, followed by Microsoft Word .doc extensions.

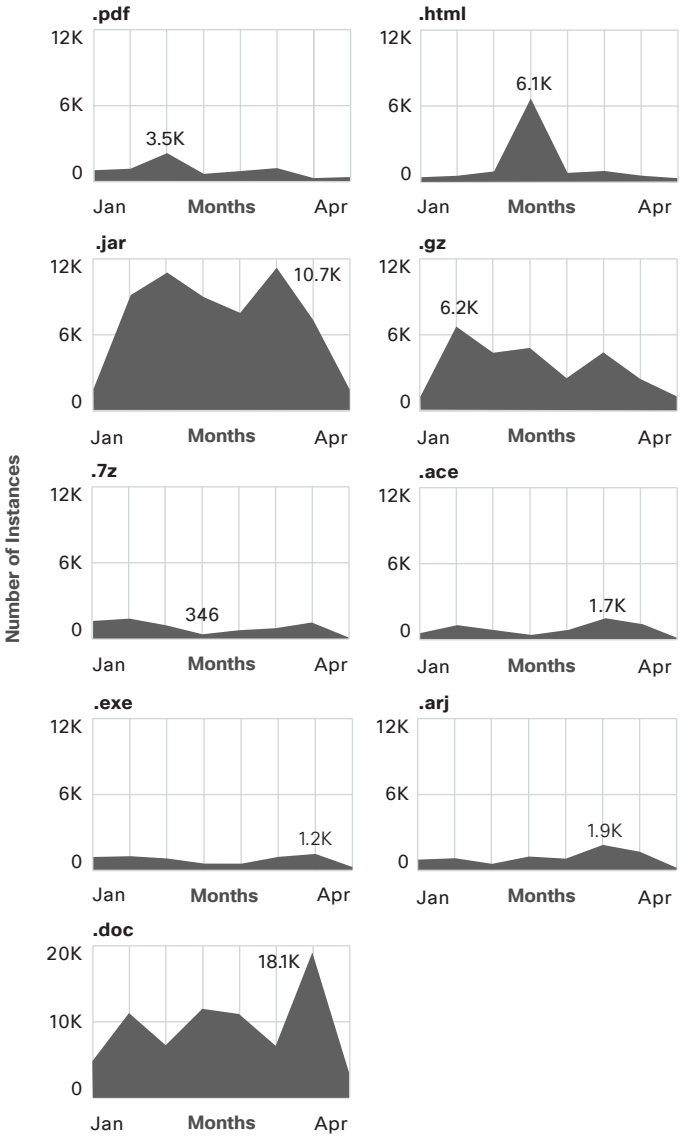
We then examined how the popularity of these various extensions changed over time (see Figure 16).

Figure 15 Most commonly detected malicious file extensions by count



Source: Cisco Security Research

Figure 16 Patterns of top malicious file extensions, 2017



Source: Cisco Security Research

File type "favorites" observed with top malware families

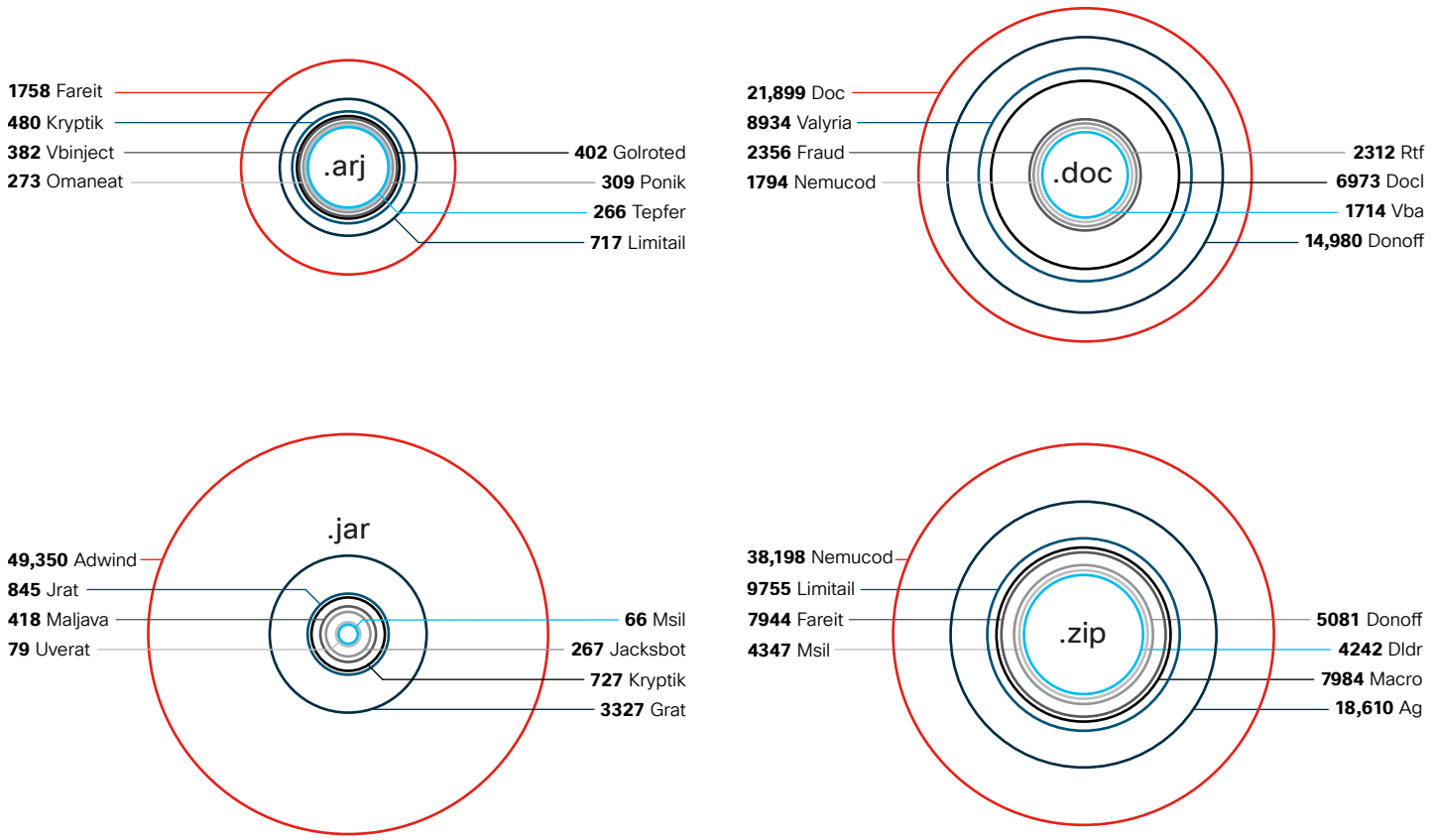
Looking at the top five malware families in our research sample, we can see that each malware family has different file type strategies, as well as some extensions that they use regularly. For example:

- Adwind, a remote access Trojan (RAT), frequently uses .jar files (Java archive extensions).
- Nemucod, a Trojan downloader known to distribute ransomware, uses .zip as its go-to file extension.
- MyWebSearch, which is malicious adware, is very selective: It only employs .exe file extensions, sometimes using only one type per month.
- Fareit, another RAT, uses a wide variety of file types, but seems to favor .zip and .gz file extensions. (The latter is an archive file extension.)
- Donoff malware, malicious macro-dropping ransomware, mostly uses Microsoft Office document file types, especially .doc and. xls.

Figure 17 provides a different view of malicious email patterns: The relationships between select file extensions and various malware families. Our analysis shows that file types used widely in business environments, like .zip and .doc, are employed regularly by several top malware families, including Nemucod and Fareit.

However, we also see many malware families using more obscure and older file extension types, like .jar and .arj. (The latter is a type of compressed file.)

Figure 17 File extension (.arj, .doc, .jar, .zip) and malware family relationships



Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Worried about ransomware? Business email compromise may be a bigger threat

Ransomware has been drawing much of the attention in the security world lately. However, a threat that's not nearly as high-profile is raking in far more for its creators than ransomware: Business email compromise, or BEC. The risk intelligence provider Flashpoint, a Cisco partner, has studied the BEC problem and has determined that it's currently the most lucrative and profitable method to extract large amounts of money from a business. It's a deceptively easy attack vector that relies on social engineering to trigger the theft.

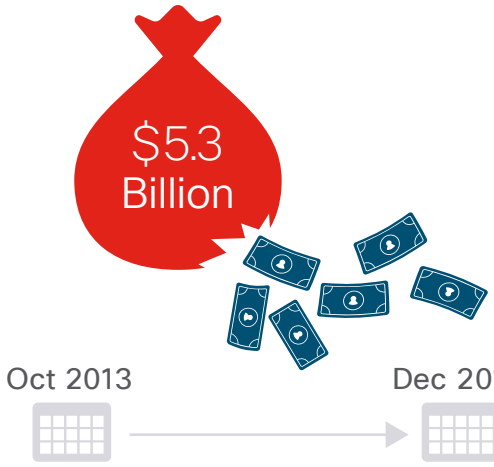
At its most basic, a BEC campaign involves an email (sometimes using spoofing to appear as though it's from a co-worker) delivered to financial employees who can send funds by wire transfer. The adversaries have usually done some research on the company hierarchy and its employees—for example, using social network profiles to piece together the likely chain of command. The email may appear to be from the CEO or another top executive, asking the recipient to send a wire payment to a supposed business associate or to pay a vendor. The message may express some urgency to compel the recipient to send the money, which typically ends up in foreign and domestic bank accounts owned by cybercriminals.

BEC scams are aimed at big targets—and big targets have fallen victim to them, even though such organizations may have mature threat defenses and safeguards against fraud. Both Facebook and Google have been victims of BECs and wire fraud.[12] Because BEC messages don't contain malware or suspect links, they can usually bypass all but the most sophisticated threat defense tools.

How bad is the BEC problem? The Internet Crime Complaint Center (IC3)—a partnership of the Federal Bureau of Investigation, the U.S. Department of Justice, and the National White Collar Crime Center—reports that US$5.3 billion was stolen due to BEC fraud between October 2013 and December 2016, an average of $1.7 billion per year[13] (see Figure 18). By way of comparison, ransomware exploits took in about US$1 billion in 2016.[14]

U.S. victims of BEC fraud totaled almost 22,300 from October 2013 to December 2016.

Figure 18 Amount of loss due to BEC



Source: Internet Crime Complaint Center

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

12 "Exclusive: Facebook and Google Were Victims of $100M Payment Scam," by Jeff John Roberts, Fortune.com, April 27, 2017: fortune.com/2017/04/27/facebook-google-rimasauskas/.
13 "Business E-mail Compromise, E-Mail Account Compromise: The 5 Billion Dollar Scam," Internet Crime Complaint Center (IC3) and the Federal Bureau of Investigation (FBI), May 4, 2017: ic3.gov/media/2017/170504.aspx.
14 "Ransomware Took In $1 Billion in 2016—Improved Defenses May Not Be Enough to Stem the Tide," by Maria Korolov, CSOonline.com, January 5, 2017: csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html.

Combating BEC fraud usually requires improvements in business processes, as opposed to threat defense tools. Flashpoint recommends user education: For example, training employees to identify out-of-the-ordinary requests for financial transfers, such as an out-of-country transfer at a business that operates domestically. Organizations can also require employees to verify wire transfers with another employee—perhaps by phone—to bypass a spoofed email.

As for threat tools, sender policy framework (SPF) defenses can help block emails with spoofed addresses. However, organizations may be hesitant to turn on this feature because SPF can also block legitimate emails (such as marketing messages or newsletters) unless it is properly managed by IT.

The bottom line is that organizations with an online presence—from giants like Facebook and Google to businesses with just a few dozen employees—are potential targets for BEC fraud. It's a low-cost, high-return approach for criminals, which means it will likely grow as a threat vector.

Malware evolution: A 6-month perspective

Cisco security researchers have been watching the evolution of malware during the first half of 2017 and have identified several trends that shed light on what malware authors are thinking about most when developing their strategies—namely, delivery, obfuscation, and evasion.

Trend 1: Adversaries are using malware distribution systems that require users to take some type of positive action to activate the threat

We have observed an increase in malicious email attachments that are able to bypass automated malware detection systems. When placed in a sandbox environment, these attachments do not show any evidence of being malicious, so they are forwarded to the user who may then encounter:

- A password-protected malicious document (with the password conveniently provided to the user in the body of the email)
- A malicious document that presents a dialog box asking for the user's permission (such as, "Click OK") to take some type of action
- Malicious OLE objects in a Word document
- Malicious Word documents embedded in PDFs[15]

Trend 2: Adversaries are using ransomware codebases to their advantage

Malicious actors are creating malware quickly, easily, and cost-effectively by using open-source codebases, like Hidden Tear and EDA2, which publicly release ransomware code for "educational" purposes. Adversaries tweak the code so it looks different from the original and then deploy the malware. Many of the "new" ransomware families Cisco threat researchers have observed in recent months are based on open-source code from educational codebases.

Trend 3: Ransomware-as-a-service (RaaS) platforms are growing fast

RaaS platforms, such as Satan, are ideal for lazy adversaries who want to enter the ransomware market and launch a successful campaign without having to perform any coding or programming or devote resources to developing innovative tactics. The operators of these platforms, which are growing in number, take a cut of attackers' profits. Some will even deploy the ransomware and provide additional services, such as tracking the progress of their customers' campaigns.

15 "Threat Spotlight: Mighty Morphin Malware Purveyors: Locky Returns via Necurs," by Nick Biasini, Talos blog, April 21, 2017: blogs.cisco.com/security/talos/locky-returns-necurs.

Trend 4: Fileless or "memory resident" malware is becoming more prevalent

We are seeing this type of malware infecting systems around the world. It relies on PowerShell or WMI to run the malware completely in memory without writing any artifacts to the file system or registry, unless the attacker wants to put persistent mechanisms in place.[16] That makes the malware harder to detect. It also makes forensics investigations and incident response more challenging.

Trend 5: Attackers are relying more on anonymized and decentralized infrastructure for obfuscation of command and control

Cisco threat researchers have observed an increase in the use of "bridging services" for facilitating access to malware and command-and-control services that are hosted within the Tor network. One example is Tor2web, a proxying service that allows systems on the Internet to access things that are hosted within Tor, without requiring the installation of a local Tor client application.[17]

Essentially, Tor2web makes it easier for adversaries to use Tor without having to change their malware code or include a Tor client within their malware payload. Since an attacker can configure a Tor2web proxy server on any domain they choose, it is more difficult to block them as they are deployed.

Threat intelligence from Talos: On the trail of attacks and vulnerabilities

Cisco's Talos website (blog.talosintelligence.com) strives to be a source for vulnerability research and trends in the threat landscape. Vulnerability research is particularly important because it highlights the struggle between attackers and defenders over time.

Attackers are usually considered to have an advantage because they have time on their side, while defenders are at a disadvantage because they do not. Defenders are constrained by the time needed to contain the damage caused by bad actors. Vulnerability research allows defenders to get in front of weaknesses before attackers can exploit them. By identifying zero-day vulnerabilities and working with software vendors to ensure that patches are developed and distributed, researchers can help close this gap.

The security industry has become more adept at handling ransomware. Exploit kit activity has declined, allowing Talos researchers to examine other threats. In short, the information security industry has become more cognizant of understanding how ransomware works and identifying new ransomware variants.

Another key trend discussed on the Talos blog is adversaries' shift to email-based threats as they move away from exploit kits. Since the once-dominant Angler exploit kit vanished in 2016, threat researchers have been watching to see if another player will become the clear leader—or if other significant trends in the landscape emerge (see "Exploit kits: Down, but not likely out," page 9). In tandem, researchers are watching a decline in threats that involve Flash or Java software; as browser developers block the related plug-ins, adversaries are less likely to use them as attack vectors.

16 For more on this topic, see "Covert Channels and Poor Decisions: The Tale of DNSMessenger," by Edmund Brumaghin and Colin Grady, Talos blog, March 2, 2017: blogs.cisco.com/security/talos/covert-channels-and-poor-decisions-the-tale-of-dnsmessenger.

17 For more on this topic, see "Go RAT, Go! AthenaGo Points 'TorWords' Portugal," by Edmund Brumaghin, with contributions from Angel Villegas, Talos blog, February 8, 2017: blog.talosintelligence.com/2017/02/athena-go.html.

The following are recent Talos blog posts that highlight research into specific threats and provide insights on how attackers are forced to innovate to stay ahead of defenders:

Player 3 Has Entered the Game: Say Hello to 'WannaCry': This post is an introduction to the highly publicized WannaCry ransomware variant, along with suggestions for protecting networks from the threat.

MBRFilter: Can't Touch This!: In this post, Talos researchers released MBRFilter, a disk filter to prevent malware from writing to sector 0 on all disk devices connected to a system. This is a tactic that ransomware variants such as Petya use: The malware tries to overwrite the master boot record (MBR) of an infected system and replace the bootloader with a malicious one.

Sundown EK: You Better Take Care: This post covers the Sundown exploit kit. Its related campaign operated from just a handful of IP addresses, but Talos researchers discovered more than 80,000 malicious subdomains associated with more than 500 domains using various registrant accounts. That approach means that the exploit can evade traditional blacklisting solutions.

Without Necurs, Locky Struggles: Talos researchers outlined the decline in activity for the Locky ransomware variant, a result of the Necurs botnet going offline temporarily. Researchers keep a close watch on the Necurs botnet: When it's up and running, it has the potential to distribute staggering amounts of spam delivering Locky as well as the Dridex banking malware.

Go RAT, Go! AthenaGo Points "TorWords" Portugal: In this post, Talos researchers identify AthenaGo, a malware campaign distributed through malicious Word documents and targeting victims in Portugal. The unique angle of the campaign, researchers explained, was that AthenaGo used a remote access Trojan (RAT), with the capability to download and run additional binaries on infected systems. The malware was written using the Go programming language, which is not a common tactic. Also, the command-and-control communications that the malware uses relies on Tor2web proxies, which malware writers employ to evade detection.

Covert Channels and Poor Decisions: The Tale of DNSMessenger: Talos researchers outlined their analysis of a malware sample using DNS TXT record queries and responses to create a bidirectional command-and-control channel—an uncommon and evasive tactic used by attackers to remain undetected while operating in targeted environments.

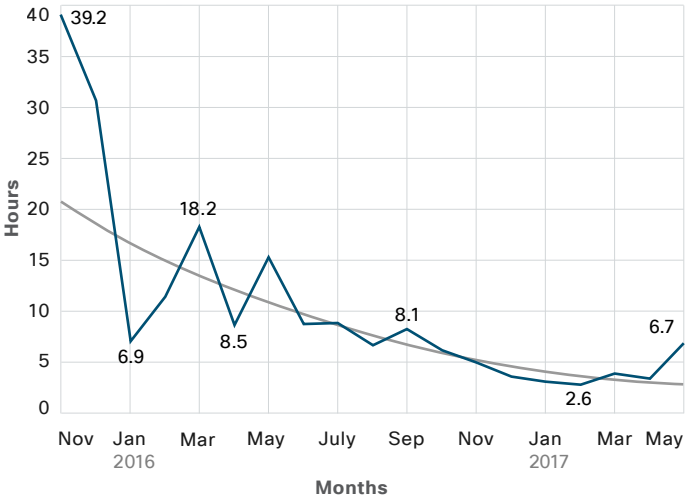
Necurs Diversifies Its Portfolio: In this post, researchers discuss new activity from the giant Necurs botnet, which was diversifying its spam delivery to include pump-and-dump penny stock messages.

Threat Spotlight: Mighty Morphin Malware Purveyors: As the Necurs botnet returned to action after ceasing operations temporarily, researchers identified a new burst of activity from Locky: A large-scale spam campaign.

Time to detection: The tug-of-war between attackers and defenders tightens

Cisco has been tracking our median time to detection (TTD) since November 2015. Since that time, the overall trend has been downward—from just over 39 hours at the start of our research to about 3.5 hours for the period from November 2016 to May 2017 (see Figure 19).

Figure 19 Median TTD by month



Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Increases in the median TTD indicate times when adversaries introduce new threats. Decreases show periods where defenders are identifying known threats quickly. Since the summer of 2016, the ongoing tug-of-war between attackers and defenders has been less dramatic, with the latter taking back ground quickly after each attempt by adversaries to gain—and maintain—the upper hand.

Cisco defines "time to detection," or TTD, as the window of time between a compromise and the detection of a threat. We determine this time window using opt-in security telemetry gathered from Cisco security products deployed around the globe. Using our global visibility and a continuous analytics model, we can measure from the moment malicious code runs on an endpoint to the time it is determined to be a threat for all malicious code that was unclassified at the time of encounter.

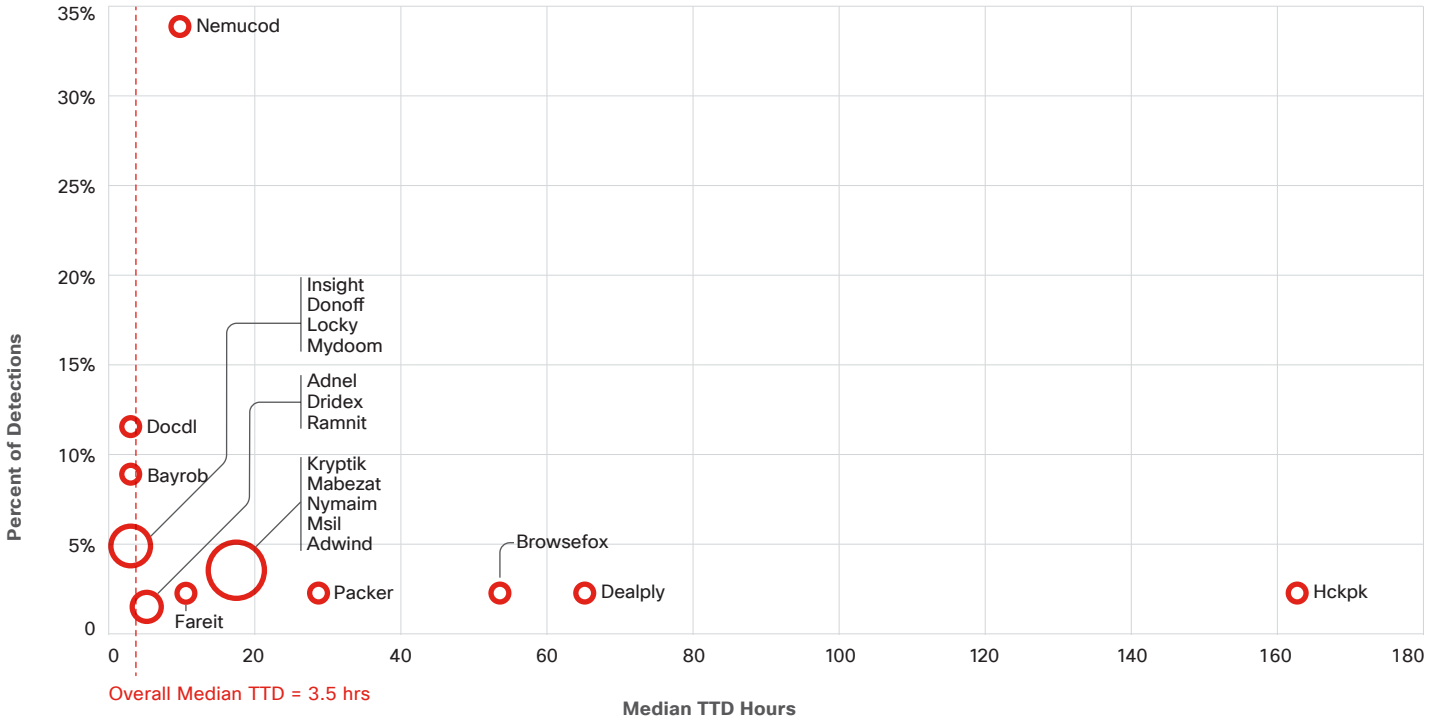
Developments in the threat landscape, especially within the past six months, show that cybercriminals are under even more pressure to evolve their threats to evade detection and devise new techniques.

Figure 20 shows the median TTD for the top 20 malware families by percentage of detections that our researchers observed from November 2016 to April 2017. Many of the families that Cisco products are detecting within our median TTD of 3.5 hours are industrialized threats that move fast and are widespread. Old and prevalent threats are also typically detected below the median TTD.

Many malware families can still take a long time for defenders to identify even though they are known to the security community. That's because the actors behind these threats use various obfuscation techniques to keep their malware active and profitable. In the next section, we examine how four specific malware families—Fareit (a remote access Trojan or "RAT"), Kryptik (a RAT), Nemucod (a downloader Trojan), and Ramnit (a banking Trojan)—use specific strategies to stay ahead of defenders.

Their methods are effective: As Figure 20 shows, all these families were outside our median TTD window of 3.5 hours—Kryptik significantly so. Even Nemucod, the most frequently detected among the top families shown, takes longer to identify because it evolves so rapidly.

Figure 20 TTD medians of top 20 malware families



Source: Cisco Security Research

Time-to-evolve trends: Nemucod, Ramnit, Kryptik, and Fareit

Cisco closely monitors how malware authors evolve their payload delivery types, the pace at which they generate new files (to defeat hash-only detection methods), and whether and how they employ domain-generation algorithms (DGAs) to keep their malware fresh and effective at compromising users and systems. Some malware families generate large numbers of DGA domains, which are all slightly different variations of a given domain name, as a way to conceal their traffic and evade detection (for more on DGA domains, see "The expanding life spans—and overlap—of DGA domains," page 33).

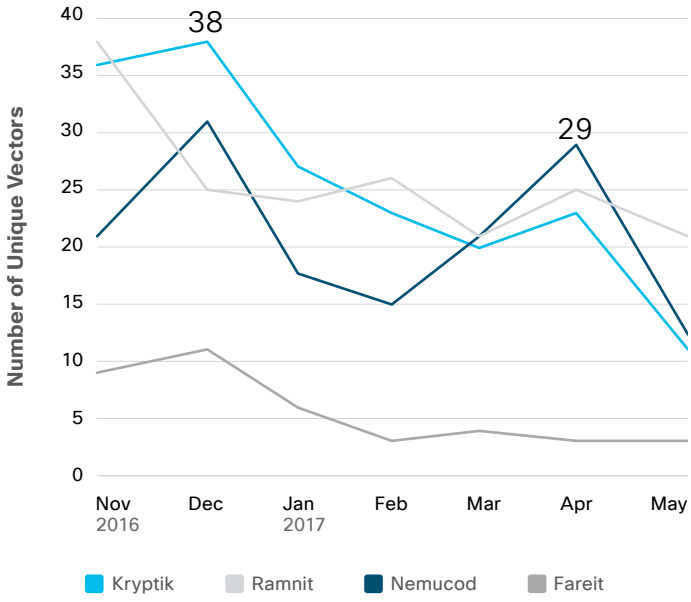
We analyze web attack data from different Cisco sources, including web proxy data, cloud and endpoint advanced malware products, and composite antimalware engines. The data that our analysis yields allows us to measure the "time to evolve" (TTE)—the time it takes adversaries to change the way specific malware is delivered and the length of time between each change in tactics.

Insight on each malware family's unique pattern of evolution—and how they employ new and old tools and tactics to try to stay ahead of defenders—helps us to refine our security practices and technology so we can continuously improve our time to detection (TTD) (for more on TTD, see "Time to detection: The tug-of-war between attackers and defenders tightens," page 26).

From November 2016 through May 2017, we centered our analysis on four well-known malware families—Nemucod, Ramnit, Kryptik, and Fareit. We looked for changes in file extensions delivering the malware and the file content (or MIME) type as defined by a user's system. For each family, we examined the patterns in both web and email delivery methods.

Figure 21 shows the number of unique vectors used by each of the four malware families for web attacks during the period observed.

Figure 21 Number of unique vectors seen per month in web events



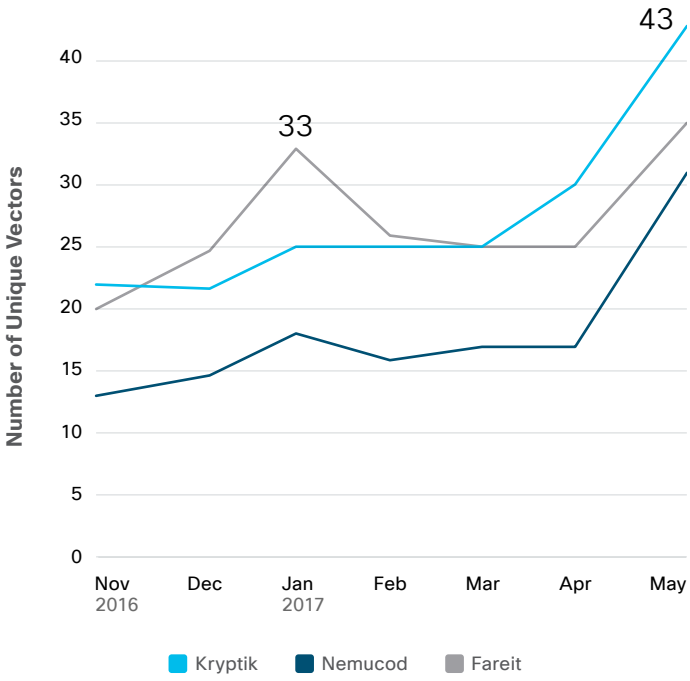
Source: Cisco Security Research

Figure 22 shows the number of unique vectors each family used for email attacks during the period observed. Note that the Ramnit malware family was excluded from analysis because our researchers identified only about a handful of associated events (blocks) with Ramnit-related files.

Our TTE analysis includes examining the age of hashes that a malware family is using (per month) at the time of the block. That helps us to determine how frequently and how fast the malware needs to evolve to evade hash-based detection.

Following is an overview of our research highlights for each of the four malware families in our study.

Figure 22 Number of unique vectors seen per month in email events



Source: Cisco Security Research

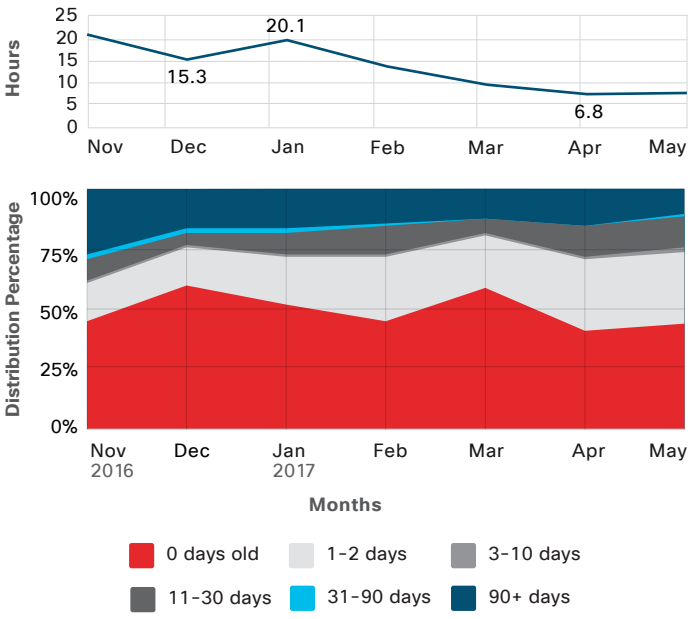
TTE analysis: Kryptik

Kryptik malware (also known as GozNym) is the result of the merger between an advanced banking Trojan, whose source code was leaked publicly, and a downloader.[18] About one-third (35 percent) of the web events for the Kryptik malware family that we observed in our recent TTE study involved JavaScript, while another 26 percent used a .php file extension. MIME types we identified included MS Word, octet-stream, or HTML. Most email events for the Kryptik RAT involved .zip, .js, or executable files.

We also discovered that the Kryptik malware family was employing hashes of varying ages during the period observed (see Figure 23).

The TTD trend for Kryptik shown in Figure 23 illustrates that the malware is difficult to detect, although Cisco products have been identifying the threat more quickly in recent months. By the end of April 2017, our median TTD for the Kryptik RAT was about twice our overall median TTD of 3.5 hours (for more details on how we calculate TTD, see page 26). However, this figure is still well below the TTD of 21.5 hours that we measured for Kryptik in November 2016.

Figure 23 TTD and hash ages for the Kryptik malware family per month



Source: Cisco Security Research

18 "Visualizing 2016's Top Threats," by Austin McBride and Brad Antoniewicz, Cisco Umbrella blog, February 8, 2017: umbrella.cisco.com/blog/blog/2017/02/08/visualizing-2016s-top-threats/.

TTE analysis: Nemucod

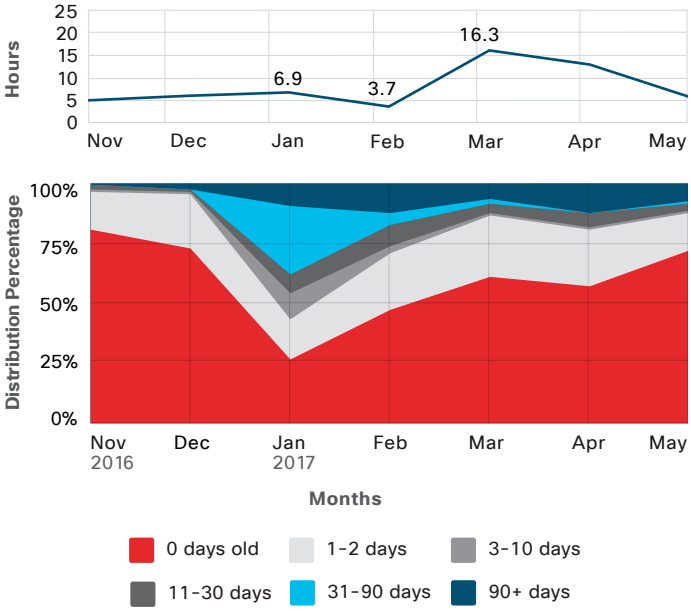
Nemucod continues to be among the most frequently seen malware families during 2017. The downloader malware is used to distribute ransomware and other threats, such as backdoor Trojans that facilitate credential theft or click fraud. Some variants also serve as mechanisms for delivering the Nemucod malware payload.

The way that Nemucod evolves likely has a lot to do with its continued success. Figure 24 shows that Nemucod consistently uses 15 or more combinations of file extensions and file content types. For example, 70 percent of Nemucod web events we observed involved JavaScript; the balance of events had .php (16 percent) or .zip file extensions (9 percent). Additionally, Nemucod events associated with email blocks primarily had .zip, .wsf (Windows script file), or .js files.

In Figure 24, we see that Nemucod relies primarily on hashes that are less than a day old to keep ahead of defenders.

In recent months, the malware has been increasing its use of older hashes. That may indicate that the security community is becoming more effective at detecting new instances of Nemucod, so the malware authors may be reverting to older hashes that have proven effective. Regardless, Figure 24 shows that the TTD for Nemucod increased in March and April, further exhibiting the push-and-pull between attackers and defenders. Whether it is related to how attackers are cycling through hashes, their delivery methods, or other obfuscation methods, Nemucod's authors apparently developed delivery mechanisms that were harder to detect.

Figure 24 TTD and hash ages for the Nemucod malware family per month



Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

TTE analysis: Ramnit

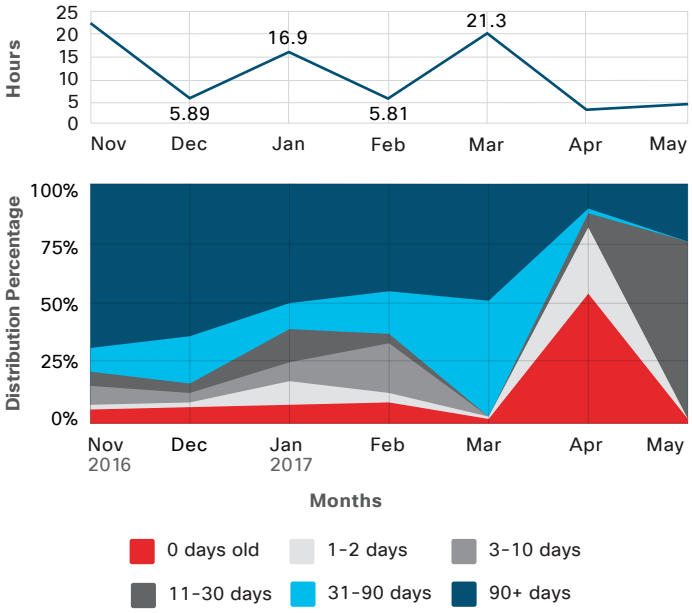
Ramnit originally surfaced in 2010 as a self-replicating worm. Its developers later added data-stealing capabilities and other enhancements using exposed source code from the notorious Zeus Trojan. Today, Ramnit is one of the most persistent among known banking Trojans.

In our latest TTE study, we found that almost every web event (99 percent) involving Ramnit malware had a text or HTML MIME type. File extensions were varied, but were primarily HTML (41 percent).

Our research also shows that Ramnit found success evading defenders for several months by using mostly hashes that were 90 days or older (Figure 25).

However, Figure 25 also shows that by April, Ramnit's operators were using primarily new hashes—with more than half being less than one day old. This is likely due to defenders becoming more successful at detecting instances of Ramnit that employed the older hashes. In fact, our median TTD for Ramnit declined from just over 21 hours in March to about five hours by the beginning of May.

Figure 25 TTD and hash ages for the Ramnit malware family per month



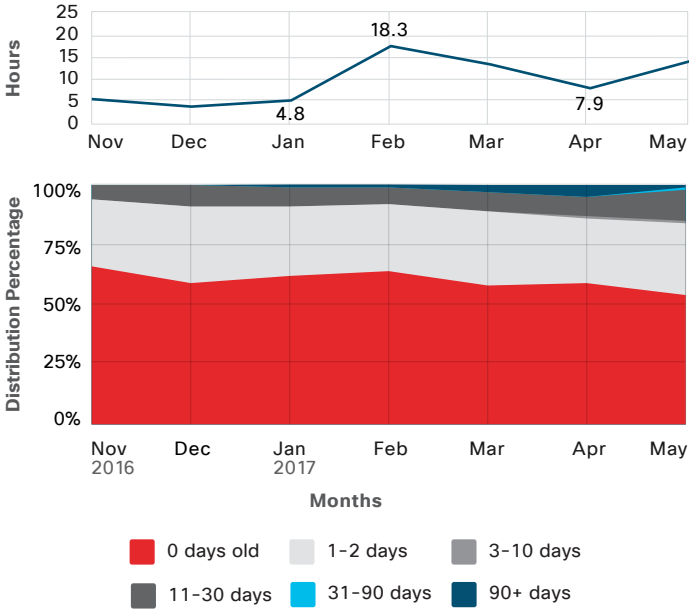
Source: Cisco Security Research

TTD analysis: Fareit

Fareit is another well-known and pervasive malware family. The Fareit RAT steals credentials and distributes multiple types of malware. Almost all (95 percent) of Fareit malware variants involved in web attacks used the .dll file extension, according to our research. Eighty-four percent had an msdos program or msdownload MIME type. Fareit file extensions in email were mostly associated with Word documents, or with ACE (compression archive), executable, or .zip files.

Fareit, like Kryptik malware, changes hashes frequently to avoid detection (Figure 26). The median TTD for Fareit spiked significantly in February and March. During that time, the malware had slightly increased its use of new hashes while also introducing some significantly older ones (90 days or older) into the mix.

Figure 26 TTD and hash ages for the Fareit malware family per month



Source: Cisco Security Research

Domain activity: Nemucod and Ramnit

Cisco threat researchers analyzed domain activity related to two of the malware families in our latest TTE study: Nemucod and Ramnit. The purpose of this exercise was to learn more about how these specific malware families use domains to deliver their malware.

During the period that we observed (November 2016 to March 2017), we found that Nemucod was employing a wide range of compromised websites—more than Ramnit.

Meanwhile, Ramnit appeared to be using hundreds of domain-generation algorithm (DGA) domains (for more about DGA domains and why malware developers use them, see "The expanding life spans—and overlap—of DGA domains," on page 33).

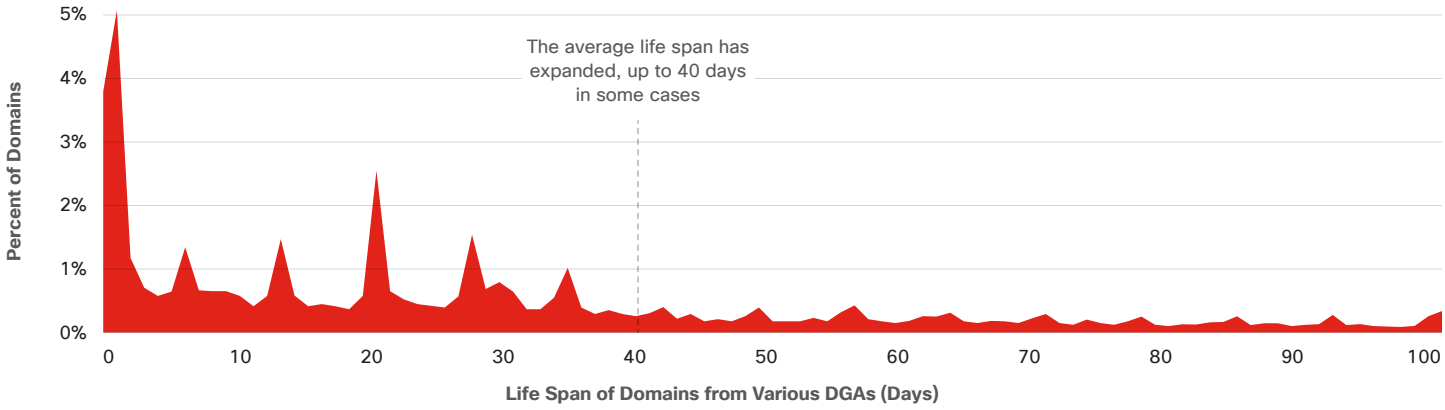
The expanding life spans—and overlap—of DGA domains

Many leading malware families rely on domain-generation algorithms (DGAs) to rapidly generate pseudo-random domain names to evade detection. DGA domains are typically short-lived but can sometimes last for months, which makes heuristic blocking more challenging for defenders.

Anomali, a Cisco partner and threat intelligence provider, tracks the life spans of suspected DGA domains associated with a wide range of different malware families. According to Anomali's threat researchers, most DGA domains observed about 5 years ago had a life span of 3 days or less. Since then, the average life span of DGA domains has expanded significantly—up to about 40 days, in some cases (see Figure 27). Some even endure beyond that mark.

Note: About 45 different malware families in sample.

Figure 27 DGA life spans



Source: Anomali

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

The likely reason for this trend is that adversaries are under pressure to evolve threats faster to avoid being blocked and to remain undiscovered longer in the organizations that they have already compromised (for more on this topic, see "Time-to-evolve trends: Nemucod, Ramnit, Kryptik, and Fareit," on page 28). Malware authors need to move fast enough to avoid blocklists, but not so fast that defenders gain the upper hand in blocking all new domains.

In most cases, the algorithms behind the malware that generate DGA domains vary just two elements when creating domains: The length of the domain name and the possible top-level domains it can use. (Note: Nearly all algorithms use different approaches to randomize how they pick the letters in the second-level domain.)

Those limitations, combined with the need to generate new DGA domains constantly, result in malware families often overlapping their efforts to generate and register DGA domains. They may end up colliding with each other in heavily saturated combinations like 8-10 character .com domains, for example. In such saturated spaces, a DGA domain could end up on a blocklist due to a competitor's use of a similar DGA domain that has been identified by defenders.

Analyzing infrastructure broadens knowledge of attacker tools

As discussed in the Security Capabilities Benchmark Study focus on verticals (see page 77), many security teams struggle to make sense of the thousands of security alerts they receive daily. Exploiting actors' registration and hosting tactics—specifically, the infrastructure in which bad actors operate—can allow security professionals to zero in on the sources of threats and block them.

In an analysis of infrastructure used by the Fancy Bear cyberespionage group, the research team at ThreatConnect, a Cisco partner and provider of the industry's only extensible, intelligence-driven security platform, identified potentially malicious domains, IP addresses, and aliases, helping defenders to take action before adversaries could break into networks.[19] Not only is this approach proactive, it is also potentially predictive, allowing vendors to gather advance intelligence about adversaries.

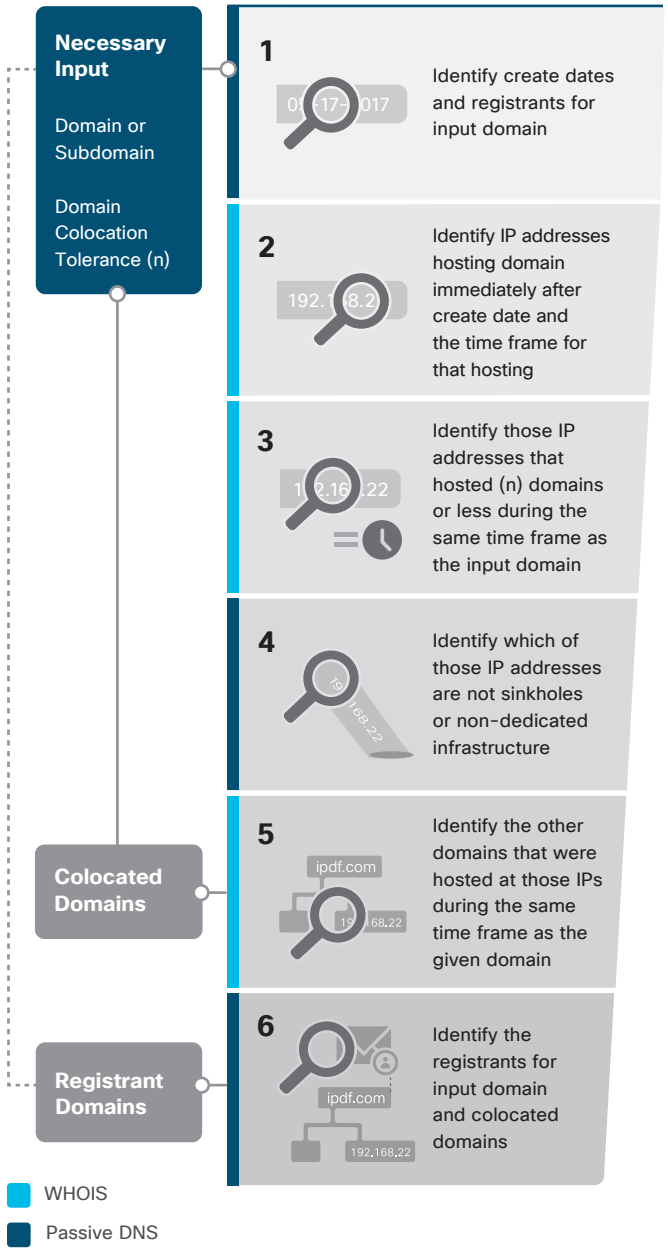
The domains and IP addresses analyzed were associated with spear-phishing attacks against Bellingcat, a citizen journalist organization targeted by the Fancy Bear advanced persistent threat (APT). ThreatConnect theorized that because some threat actors have access to limited IP infrastructure, they'll host more than one of their domains on infrastructure they control. By studying these colocated domains, security experts can identify additional infrastructure (like domains and IP addresses) that adversaries may control, and preemptively block or incorporate them into their defensive strategies.

19 For more information, see "How the ThreatConnect Research Team Used the Platform to Investigate Incidents, Identify Intelligence, and Conduct Pertinent Analysis Regarding Fancy Bear": threatconnect.com/blog/how-to-investigate-incidents-in-threatconnect/.

As the ThreatConnect analysis explains, the process followed these steps:

- Bellingcat provided email headers from spear-phishing messages believed to originate from Russian state-sponsored hackers. ThreatConnect then used knowledge of previous Fancy Bear operations to assess that Fancy Bear most likely conducted the operations targeting Bellingcat.
- ThreatConnect used WHOIS registration information to identify when a domain from the spear-phishing messages was registered and the email address that registered the domain, providing a time frame to use for the investigation.
- Using passive DNS, IP addresses were identified that hosted the domain after it was initially registered. That identifies IP addresses that may be connected to the bad actors.
- Using passive DNS once again, researchers identified which IP addresses hosted less than a given arbitrary number of domains to exclude IPs that may be hosting multiple domains for multiple customers.
- Using WHOIS and passive DNS, ThreatConnect identified the subset of those IP addresses that were probably dedicated to the adversary—narrowing down the list of IP addresses that likely could be attributed to the APT.
- From that subset of IP addresses, ThreatConnect then used passive DNS to identify other domains hosted at the same IP address at the same time as the initial domain. (If the domains are colocated with the initial domain at the same IP address, it identifies those that are possibly controlled by the same APT.)
- ThreatConnect also identified other domains registered using the same email address used to register the original domain. When an email address is used to register a domain associated with APT activity, other domains registered with that email address could also be part of the APT's activities.
- ThreatConnect used newly identified domains—those colocated with the original domain as well as those registered using the same email address—to feed subsequent iterations of the analysis.
- ThreatConnect then used passive DNS to identify any known subdomains for the identified domains. This information can help identify mail servers or other subdomains that were not hosted on the same IPs as the identified domain, providing more avenues for further research.

Figure 28 Colocation methodology



Source: ThreatConnect

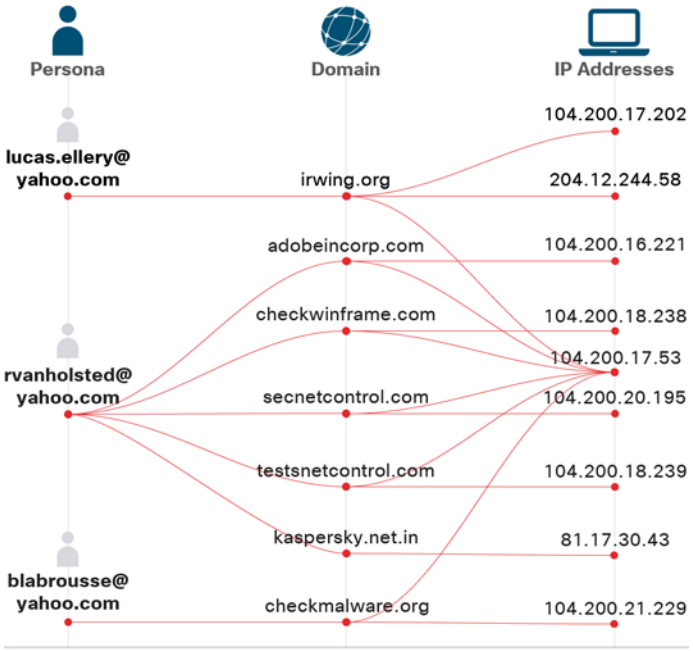
Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Analytic methodologies such as the one in Figure 28 can help to identify an exponentially larger group of email addresses, IP addresses, and domains that could be associated with encountered activity and considered suspect. The investigation described above started with six domains, five IP addresses, and three email registrants identified in the email headers provided by Bellingcat.

Using the process outlined above, 32 email addresses and aliases, more than 180 domains, and more than 50 IP addresses that were likely associated with Fancy Bear APT activity were identified. Figure 29 shows a subset of the associations among the domains, email addresses, and IP addresses, and how they tied back to the Bellingcat spear-phishing incidents.

Organizations that undertake a similar analysis can proactively block domains, IP addresses, and email addresses that could be the source of attacks. Researching and identifying infrastructure allows organizations to identify the following: Tactical intelligence to use in an ongoing incident response effort, infrastructure used by adversaries before it's used against the organization, and historical context or associations between infrastructure and attackers.

Figure 29 Links among infrastructure used by APT group



Source: ThreatConnect

Supply chain attacks: One compromised vector can affect many organizations

Much like any enterprise looking to save time and money, attackers seek out ways to make their operations more efficient. As the Cisco partner RSA discovered, supply chain attacks offer maximum impact for minimal effort on the part of criminals. In the case that RSA examined, the adversaries inserted a Trojan into legitimate software typically used by enterprise system administrators to help analyze Windows system event logs.[20]

The compromised software was available for download at the vendor's site, along with updates. The result was that one compromised vector—the vendor site—could then spread the threat to many more enterprise networks, simply by offering the software and automatic updates.

As part of its research, in which the bad-actor group was dubbed "Kingslayer," RSA tracked the compromised software after observing unidentified beaconing aimed at a URL, which resolved to an IP address that also resolved to a known malicious domain. In tracking the origins of the malware (a variant of PGV_PVID) found at the domain, the RSA team discovered an organization that appeared to have been infected by it—and determined that the malware came from the system administration software.

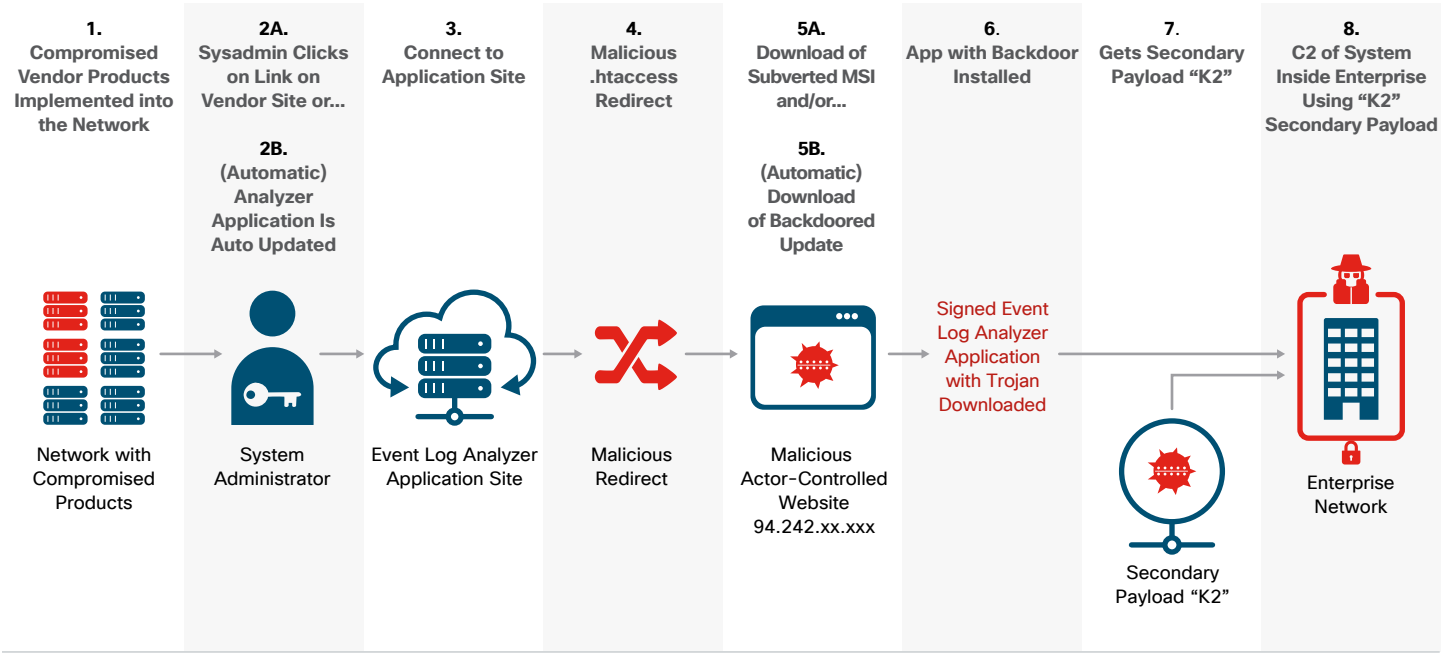
RSA found that the download page for the software had been compromised as well as the software vendor's updates page (see Figure 30 on next page). This meant companies that previously downloaded the uncompromised version of the software could still be in danger if they signed up for automatic updates, since a subsequent update would deliver the malware as well.

20 For more details on this investigation, see the RSA report, "Kingslayer—A Supply Chain Attack": rsa.com/en-us/resources/kingslayer-a-supply-chain-attack.

The period of compromise lasted only about two weeks. But because the vendor did not notify users of the compromised software until months later, the malware could have remained in place until organizations detected it, or until the vendor's notification triggered remediation efforts.

For enterprises seeking to block supply chain threats, detection is challenging. Endpoint security is probably the best defense, as it can alert security teams that one piece of software is communicating with another one. Real-time monitoring can also help detect suspicious activity.

Figure 30 Kingslayer compromise infection chain



Source: RSA

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Although the RSA analysts don't know how many organizations installed the compromised application before RSA informed the vendor of the malware problem, the vendor's customers are listed on its website and subscribed to the vendor's event log information portal service. The list of customers, and therefore potentially compromised organizations, included at least:

- 4 major telecommunications providers
- 10+ military organizations
- 24+ Fortune 500 companies
- 5 major defense contractors
- 24+ banks and financial institutions
- 45+ higher education institutions

Although RSA investigators aren't sure of the end goal of the Kingslayer actors, the size and sophistication of the vendor's customers would make them highly lucrative targets. Adversaries may have sought customer login information from financial services organizations, or may have been engaging in nation-state disruption.

The supply chain attack strategy merits attention from defenders for several reasons. The attackers need to provide only a single compromised vector, yet they can infect many targets. In addition, these attacks are stealthy by nature, giving attackers valuable time to operate undetected. Also, if the software that's being compromised is used primarily by system, network, or security administrators, attackers increase the odds that they've found the ideal staging environment to systematically exploit large enterprises.

Infrastructure harvesting targets academic networks

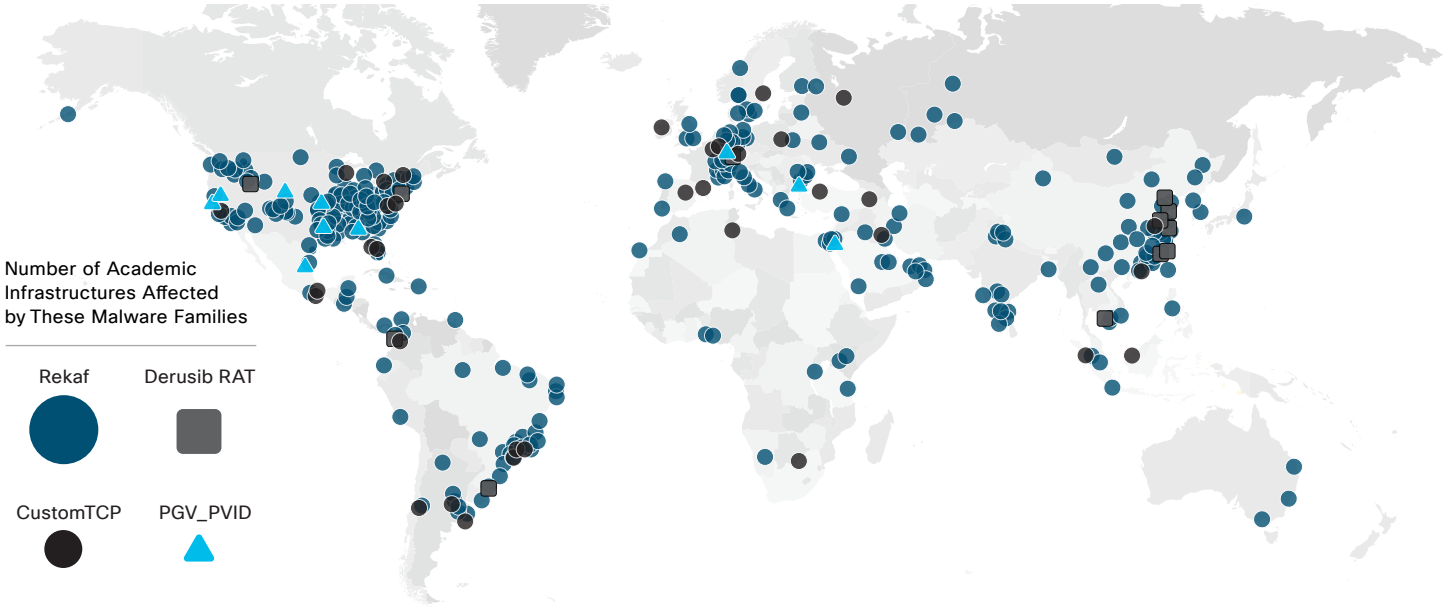
In the Kingslayer case, the adversary's approach to infrastructure harvesting involves hiding in legitimate hardware, giving software users the impression that they're getting a clean product even before they've put it in their network. In the case of the Schoolbell botnet,[21] the adversaries use infrastructure as a launching pad, since the network resources have little or no bad reputation and a seemingly benign location. In both cases, bad actors leverage the good name of the vendor and the location.

Just as endpoint security and real-time monitoring can help organizations avoid supply chain attacks as described above, they can also assist in detecting what RSA calls "infrastructure harvesting." In this kind of attack, adversaries will attempt to take control of an organization's infrastructure, in hopes of using it for large-scale exploits.

The Schoolbell botnet—so named because it targets academic infrastructure—is one example of this adversarial strategy. At its peak activity, RSA identified almost 2000 unique infections in the Schoolbell botnet infrastructure (see Figure 31).

The Schoolbell botnet and the infrastructure harvesting approach offer a warning to organizations that believe they are not targets of cyber attacks because they do not house lucrative data. Academic organizations may have a more relaxed approach to network security than other organizations of similar size in other industries, such as financial services. Therefore, academic networks could be appealing targets for attackers who want an easy "in" as well as time to operate stealthily without being detected. Academia could be an ideal target for bad actors seeking more infrastructure resources.

Figure 31 Schoolbell malware infection worldwide



Source: RSA

21 To learn more about the Schoolbell botnet and infrastructure harvesting, see "Schoolbell: Class Is in Session," by Kent Backman and Kevin Stear, RSA, February 13, 2017: blogs.rsa.com/schoolbell-class-is-in-session/.

The IoT is only just emerging but the IoT botnets are already here

2016 brought a long-feared DDoS threat to fruition: Cyber attacks launched from multiple connected devices turned into botnets. A 665-Gbps attack targeted the security blogger Brian Krebs in September.[22] Shortly thereafter, a 1-TBps attack was launched against the French hosting company OVH.[23] And in October, DynDNS suffered an attack that caused an outage to hundreds of popular websites—the largest of the three Internet of Things (IoT) DDoS attacks.[24]

These attacks propelled us into the 1-TBps DDoS era. They shook traditional DDoS protection paradigms and proved that the IoT DDoS botnet threat is real—and that organizations must be prepared.

Radware, a Cisco partner, recently examined the activity of three large IoT botnets—Mirai, BrickerBot, and Hajime—and provides the following analysis.

Common characteristics of IoT botnets

- Setup is fast and easy; in fact, it can be completed within an hour.
- Distribution is rapid. The infection recurrence mechanism leads to exponential growth in the botnet's size. In fact, perpetrators can have a botnet of more than 100,000 infected devices in 24 hours.
- The malware has a low detection rate. It is very difficult to retrieve samples because the malicious code lives in the device's memory and is wiped out once the device is restarted.

Mirai

The Mirai botnet, which was responsible for the DynDNS attack, has been infecting hundreds of thousands of IoT devices, turning them into a "zombie army" capable of launching powerful volumetric DDoS attacks. Security researchers estimate that millions of vulnerable IoT devices are actively taking part in these coordinated attacks. Source code for Mirai malware was publicly released in late 2016.[25]

How it works

1. Mirai connects to victim machines through a brute-force attack against Telnet servers, using more than 60 factory default credentials of BusyBox software.
2. Every infected device locks itself against additional bots.
3. Mirai sends the victim's IP and credentials to a centralized ScanListen service.[26]
4. The new victim then helps to harvest new bots, spawning a self-replicating pattern.

More About Mirai

In addition to generating traffic volumes above 1-TBps, Mirai features a selection of 10 predefined attack vectors (see Figure 32). Some of the vectors have proven effective in taking down the infrastructure of service providers and cloud scrubbers by attacking their protections.

Figure 32 Menu of Mirai's attack vectors

```
#define ATK_VEC_UDP          0  /* Straight up UDP flood */
#define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS          2  /* DNS water torture */
#define ATK_VEC_SYN          3  /* SYN flood with options */
#define ATK_VEC_ACK          4  /* ACK flood */
#define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP        6  /* GRE IP flood */
#define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY      8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP        10  /* HTTP layer 7 flood */
```

Source: Radware

Among the 10 vectors are highly sophisticated attack vectors, such as GRE floods, TCP STOMP, and Water Torture attacks. Mirai DDoS attacks highlight the challenges that organizations face when it comes to visibility into the legitimacy of GRE traffic or recursive DNS queries.

22 "KrebsOnSecurity Hit with Record DDoS," by Brian Krebs, KrebsOnSecurity blog, September 21, 2016: krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.
23 "150,000 IoT Devices Abused for Massive DDoS Attacks on OVH," by Eduard Kovacs, *SecurityWeek*, September 27, 2016: securityweek.com/150000-iot-devices-abused-massive-ddos-attacks-ovh.
24 "DDoS Attack on Dyn Came from 100,000 Infected Devices," by Michael Kan, IDG News Service, for *ComputerWorld*, October 26, 2016: computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html.
25 "Source Code for IoT Botnet 'Mirai' Released," by Brian Krebs, KrebsOnSecurity blog, October 1, 2016: krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.
26 "BusyBox Botnet Mirai—the Warning We've All Been Waiting For?" by Pascal Geenens, Radware, October 11, 2016: blog.radware.com/security/2016/10/busybox-botnet-mirai/.

BrickerBot

Permanent denial of service (PDoS) attacks are fast-moving bot attacks designed to stop device hardware from functioning. This form of cyber attack is becoming increasingly popular.[27]

Known as "phlashing" in some circles, PDoS attacks damage systems so severely that the hardware must be reinstalled or replaced. By exploiting security flaws or misconfigurations, PDoS attacks can destroy the firmware and basic system functions.

BrickerBot can:

- **Compromise devices:** BrickerBot's PDoS attacks use Telnet brute force—the same exploit vector used by Mirai—to breach users' devices.
- **Corrupt devices:** Once it successfully accesses a device, BrickerBot performs a series of Linux commands that ultimately lead to corrupted storage. It then issues commands to disrupt Internet connectivity and device performance, wiping all files on the device.

Figure 33 shows the exact sequence of commands the BrickerBot performs.

Hajime

Hajime is intriguing, and threat intelligence researchers monitor it very closely. That's because it has not yet taken any action with the hundreds of thousands of devices it has so far infected. It is very large and, therefore, worrisome. The operator of Hajime claims to be a white hat hacker (Figure 34).

Figure 33 Command sequence of BrickerBot.1

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Source: Radware

Figure 34 Message from Hajime's author

```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!
```

Source: Radware

How it works

Hajime is a sophisticated, flexible, thoughtfully designed, and future-proof IoT botnet. It can self-update and extends richer functions to its member bots with efficiency and speed. Like many other IoT botnets, Hajime scans the Internet to discover and infect new victims, looking for open ports TCP 23 (Telnet) and TCP 5358 (WSDAPI). It uses brute force to log in to and gain control of devices.

Interestingly, Hajime can clean malware from the device it wants to infect. It can then secure it from future contamination by controlling its Telnet communications. That way, the device becomes neutral again, although Hajime's author(s) can still access it.

Security researchers have observed Hajime cleaning devices infected with Mirai.[28] (BrickerBot, meanwhile, will destroy devices infected with either Mirai or Hajime.)

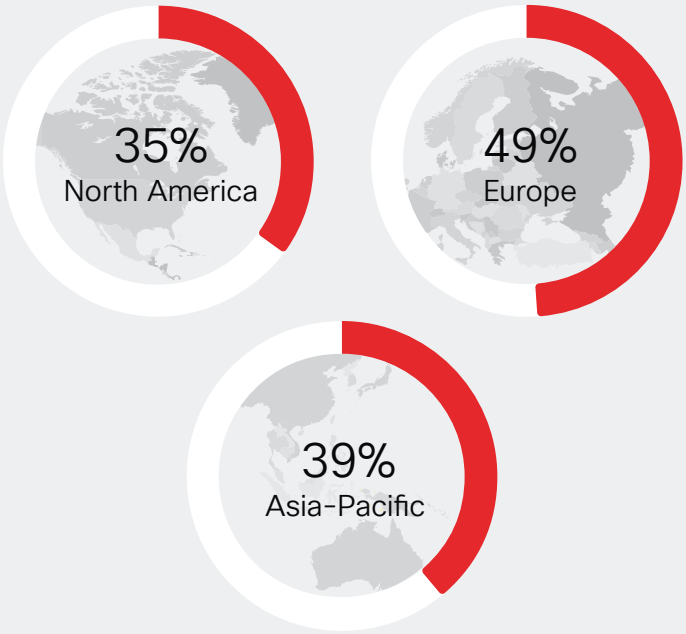
27 For more on this topic, see "BrickerBot PDoS Attack: Back With A Vengeance," Radware, April 21, 2017: security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/.

28 For more on this topic, see "Hajime – Sophisticated, Flexible, Thoughtfully Designed and Future-Proof," by Pascal Geenens, Radware, April 26, 2017: blog.radware.com/security/2017/04/hajime-futureproof-botnet/.

Extortion in cyberspace: Ransom denial of service (RDoS)

In 2016, nearly half of all companies (49 percent) suffered at least one cyber ransom incident—either a ransomware attack (39 percent) or a ransom denial of service (RDoS) attack (17 percent).[29] Figure 35 shows the percentage of companies in specific regions of the world that faced a cyber ransom incident in 2016.[30]

Figure 35 Distribution of cyber ransom attacks by country, 2016



Source: Radware

According to Radware, a gang of cybercriminals known as the Armada Collective have been responsible for most of the RDoS attacks to date. Their typical ransom demand is 10 to 200 bitcoins (about US$3,600 to US$70,000 at current rates). A short "demo" or "teaser" attack usually accompanies the ransom note. When time for payment expires, the attackers take down the target's data centers with traffic volumes typically exceeding 100 Gbps.

Copycats are now using the Armada Collective name. One early tactic involved the attempted extortion of about $7.2 million from three Greek banks.[31] These players issue fake ransom letters, hoping to turn a quick profit with minimal effort. Here are useful tips to detect a fake ransom letter:

1. **Assess the request.** The Armada Collective typically requests 20 bitcoins. Other campaigns have been asking for amounts above and below this amount. In fact, low bitcoin ransom letters are most likely from fake groups hoping their price point is low enough for someone to pay.
2. **Check the network.** Real hackers will run a small attack while delivering a ransom note. If there is a change in network activity, the letter and the threat are probably genuine.
3. **Look for structure.** Real hackers are well organized. Fake hackers, on the other hand, do not link to a website and they lack official accounts.
4. **Consider other targets.** Real hacker collectives may target many companies in a single sector. Check with other industry groups to see if others have also received menaces.

29 The global survey, conducted for Radware by a third-party market research firm, included about 600 respondents.
30 Ibid.
31 "Greek Banks Face DDoS Shakedown," by Mathew J. Schwartz, BankInfoSecurity.com, December 2, 2015: bankinfosecurity.com/greek-banks-face-ddos-shakedown-a-8714.

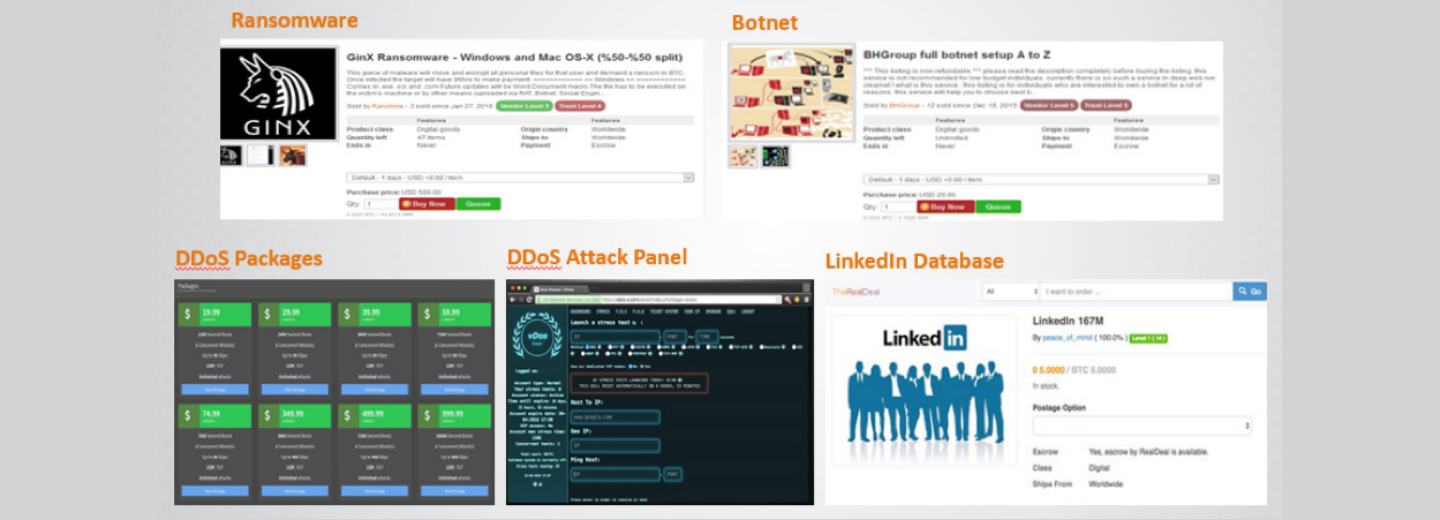
The changing economics of malicious hacking

The dramatic increases in cyber attack frequency, complexity, and size over the past year suggests that the economics of hacking have turned a corner. Radware notes that the modern hacking community is benefiting from:

- Quick and easy access to a range of useful and low-cost resources (see Figure 36)
- A dramatic increase in the number of high-value, increasingly vulnerable targets putting more and more valuable information online
- A level of maturity in the shadow economy, and with the Internet, that provides malicious actors with efficiency, security, and anonymity

Note: Some of the resources that appear in Figure 36 are no longer active.

Figure 36 Examples of cyber attack tools and panels



Source: Radware

Ransomed medical devices: It's happening

To operate effectively in today's increasingly interconnected world, many verticals—including healthcare—must integrate their IT and operational technology (OT). However, as operations become increasingly intertwined, known security weaknesses in devices and systems that were previously "walled off" from each other now present even greater risk to organizations. For example, by using proven tactics like phishing emails to compromise users, adversaries can penetrate a network, establish a foothold in a device with an outdated operating system, and from there, move laterally within the network to steal information, lay the groundwork for a ransomware campaign, and more.

The recent WannaCry ransomware attack illustrated how the increasing interconnectedness of healthcare systems and weak security practices can put both organizations and patients at risk. While it was not the first ransomware attack that appeared to target the healthcare sector, the campaign is notable in that it affected Windows-based radiology devices at two U.S. hospitals.[32]

Threat researchers with TrapX Security, a Cisco partner that develops deception-based cybersecurity defenses, warns that the targeting of medical devices with ransomware and other malware is only going to expand. It refers to this attack vector as MEDJACK, or "medical device hijack."

The potential impact is obvious when you consider that the average small to midsize hospital with five or six operational units has about 12,000 to 15,000 devices. Of those devices, about 10 to 12 percent are IP-connected, according to TrapX.

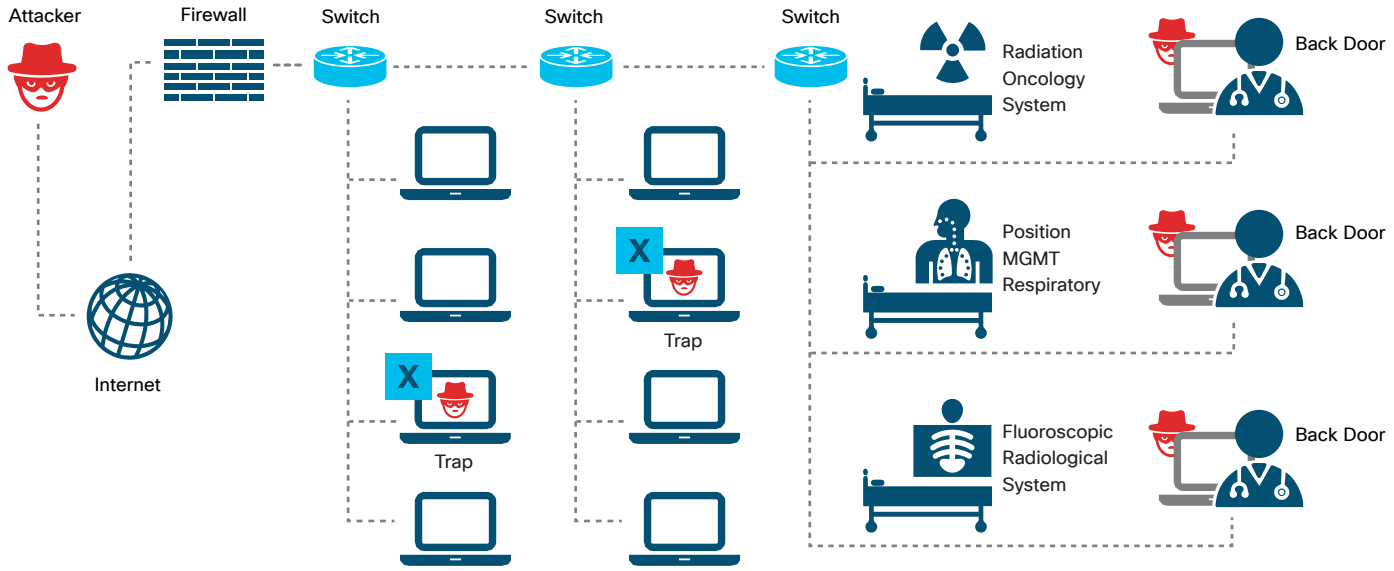
32 "#WannaCry Hits Medical Devices in US," by Tara Seals, *InfoSecurity Magazine*, May 18, 2017: infosecurity-magazine.com/news/wannacry-hits-medical-devices-in-us/.

Like many other IoT devices today, medical devices were not, and are not, designed or built with security in mind. They are often running old and unpatched systems and are rarely monitored by hospital IT staff. Even when security teams are aware of vulnerabilities, they may not be able to act because only the vendor has access to those products. In other cases, security teams must put patching on hold because the business simply cannot afford to take critical equipment offline—even for a short period—or to risk compromising the effectiveness of a device. And sometimes, the vendor and other parties, including government agencies, must approve any modifications to these devices, which can take years. The cost of support for medical devices can also be very high.

Many cybercriminals want to compromise medical devices, which TrapX researchers say have become a key pivot point for attackers to move laterally within hospital networks. Adversaries also know they are likely to see big returns from ransomware campaigns that hold lifesaving medical devices for ransom. More nefarious actors could also, potentially, take control of these devices—including implantable devices—and do harm to patients.

TrapX researchers recently investigated the exploitation of an oncology system with known Windows XP vulnerabilities. The adversaries had infected three machines (one of which was used to control a powerful laser), and turned one into a botnet master that spread malware—a variant of Conficker—across the hospital network (see Figure 37).

Figure 37 Oncology system exploit

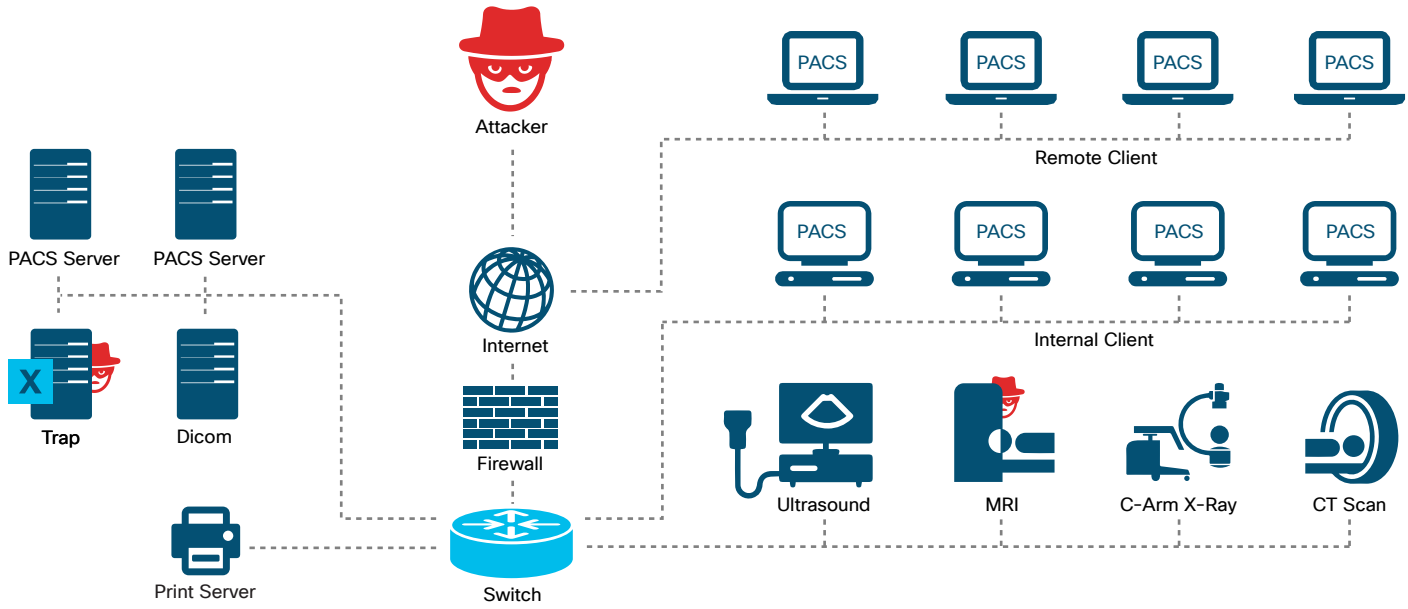


Source: TrapX

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Another MEDJACK incident that TrapX recently investigated involved a compromised MRI system. Here again, a vulnerability in Windows XP was exploited. The attackers found patient data on the system, but soon realized there was opportunity to move laterally to gain control of the hospital's PACS systems. (These systems are used to centralize and archive patient records and other critical information.) Forensics research of the attack showed the adversaries had been able to operate in the hospital's network for more than 10 months.

Figure 38 MRI system exploit



Source: TrapX

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Windows XP is a primary underlying system for operational technology in healthcare, energy, manufacturing, and other verticals. Adversaries know the operating system is an Achilles' heel because it is no longer actively supported by Microsoft, and it is extremely difficult and costly for businesses to update mission-critical devices that run XP. That's what makes these devices an especially enticing target for attackers who use ransomware: They know that businesses would rather pay the ransom than face having the machine offline—or, worse, taken down completely.

Meeting the challenge head on

TrapX researchers suggest that organizations take the following steps to reduce the likelihood, and impact, of a ransomware attack that targets medical devices and other critical OT technology:

- Understand what and how many medical assets in your environment are IP-connected
- Refresh contracts with suppliers, and make sure that they are meeting promises outlined in those contracts to update or replace software, devices, and systems
- Discuss this problem at the senior management and board levels to get their attention and commitment to the process
- Deploy technology tools that provide visibility into the network and automate threat detection and remediation

Vulnerabilities

Vulnerabilities

This section provides an overview of vulnerabilities and other exposures that can leave organizations and users susceptible to compromise or attack. Weak security practices, such as not moving quickly enough to patch known vulnerabilities, not limiting privileged access to cloud systems, and leaving infrastructure and endpoints unmanaged, are discussed. Also examined: How trends in the geopolitical landscape create both challenges and opportunities for technology vendors and businesses.

Geopolitical update: WannaCry attack underscores risk of hoarding knowledge about exploitable vulnerabilities

Even before the massive WannaCry ransomware attack in mid-May, global discussions about cybersecurity were increasing dramatically—and taking on a much more serious tone. WannaCry only underscores how much work the global community has yet to do to reduce the threat, and impact, of future malicious attacks by cybercriminals and nation-state actors.

Cisco sees three key takeaways from this recent global attack:

1. **Governments should report software flaws to vendors in a timely fashion and, to the extent that they exploit those flaws, codify those decisions for independent oversight and review.**

Only by creating greater transparency around exploitable vulnerabilities can we ever hope to minimize their occurrence and global impact. Governments should also adopt a well-structured and ongoing process that allows them to make risk-based decisions regarding how to handle and when to release information about exploitable vulnerabilities to technology developers and the public.

2. **Technology developers should have publicly disclosed, risk-based mechanisms to receive, process, and disclose information about the availability—or absence—of known vulnerabilities, patches, mitigations, and workarounds.**

Beyond providing security through the natural lifecycle of products, technology developers should also communicate to the public the how, what, why, and when of handling vulnerabilities. And they should strive to provide more transparency about co-development processes. Also, they should make sure users know precisely whom to contact to report vulnerabilities so they can be publicized and fixed.

3. **Business leadership must make cybersecurity a top priority.**

Cisco has long encouraged IT leadership in organizations to take every opportunity to educate their senior management and the board of directors about the risks that malicious attacks pose to the business, its employees and customers, and its brand reputation. It's time that message is shared, heard, and acted on: Business leadership should set the tone at the top about cybersecurity and emphasize its importance to the entire organization. They should also ensure that the organization's IT infrastructure is current and regularly updated—and that adequate budget is devoted to those activities (for more on this topic, see "Security leaders: It's time to claim a seat at the top table," on page 83).

There is a legitimate debate to be had regarding how and when governments share vulnerability information with the world. But as we have seen with WannaCry, Shadow Brokers, and WikiLeaks Vault 7 and Year Zero, governments that stockpile exploitable vulnerabilities create the potential for leaks. That, in turn, creates a tremendous opportunity for nation-state actors and cybercriminals alike.

We already see adversaries moving fast to gain a foothold in the emerging Internet of Things (IoT), which is rampant with vulnerabilities—known and unknown. Governments have a clear opportunity to help technology developers build a safer IoT world, but they need to start changing their practices and move toward greater transparency.

Technology developers, meanwhile, should press for the creation of reporting mechanisms that acknowledge government incentives to collect exploits but also encourage timely reporting and information sharing.

As for users, they have an important responsibility here, too: They must be proactive about keeping software patched and up to date and upgrade products that are no longer supported.

Vulnerabilities update: Rise in attacks following key disclosures

Disclosures of higher-profile vulnerabilities discussed in previous Cisco security reports, such as OpenSSL vulnerabilities,[33] have remained stable in recent months (see Figure 39). However, Cisco research shows high vulnerability activity related to key disclosures: The Shadow Brokers group's release of exploits for vulnerabilities affecting Microsoft Windows;[34] the Operation Cloud Hopper campaign involving phishing attacks against managed service providers;[35] and the WikiLeaks Vault 7 release of U.S. intelligence documents purporting to explain how popular software solutions and operating systems can be compromised.[36]

It's important to note that a vulnerability can exist and be exploited without the public becoming aware of it. For example, the vulnerabilities exposed by Shadow Brokers were actively in use for years. Leaking the vulnerabilities allowed more people to exploit them, but also allowed defenders to defend against them.

Figure 39 Critical advisories, November 2016–May 2017

Date	Activity	Date	Activity
05/24/17	Samba Insecure Library Loading CVE-2017-7494	**03/06/17**	Apache Struts2 Remote Code Execution Vulnerability CVE-2017-5638
04/11/17	Microsoft Office CVE-2017-0199 (Dridex Exploiting)	**02/06/17**	OpenSSL Vulnerabilities CVE-2017-3733
04/08/17	Shadow Brokers Group Disclosure of Equation Group Exploits	**01/26/17**	OpenSSL Vulnerabilities
04/06/17	Operation Cloud Hopper Sustained Global Campaigns	**01/18/17**	Oracle CPU Oracle OIT Vulnerabilities (Talos)
03/29/17	Microsoft Internet Information Services (IIS) WebDav CVE-2017-7269	**01/03/17**	PHPMailer Arbitrary Command Injection CVE-2016-10033 CVE-2016-10045
03/21/17	Network Time Protocol	**11/22/16**	Network Time Protocol
03/14/17	Microsoft Windows Graphics CVE-2017-0108	**11/10/16**	BlackNurse - ICMP DOS
03/07/17	WikiLeaks Vault 7 Release	**11/04/16**	Mobile OAuth 2.0 Implementation Issues

Source: Cisco Security Research

33 *Cisco 2015 Annual Security Report*: cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf.
34 "Cisco Coverage for Shadow Brokers 2017-04-14 Information Release," Cisco Talos blog, April 15, 2017: blog.talosintelligence.com/2017/04/shadow-brokers.html.
35 "Operation Cloud Hopper: China-Based Hackers Target Managed Service Providers," by Kevin Townsend, SecurityWeek.com, April 6, 2017: securityweek.com/operation-cloud-hopper-china-based-hackers-target-managed-service-providers.
36 "The WikiLeaks Vault 7 Leak – What We Know So Far," by Omar Santos, Cisco Security Blog, March 7, 2017: blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far.

In examining the vulnerabilities disclosed by WikiLeaks, an issue of concern for defenders is that they did not have knowledge of the exploits developed by government agencies—and therefore, the relevant vulnerabilities. Defenders may rightly worry about what other vulnerabilities exist and have not been disclosed.

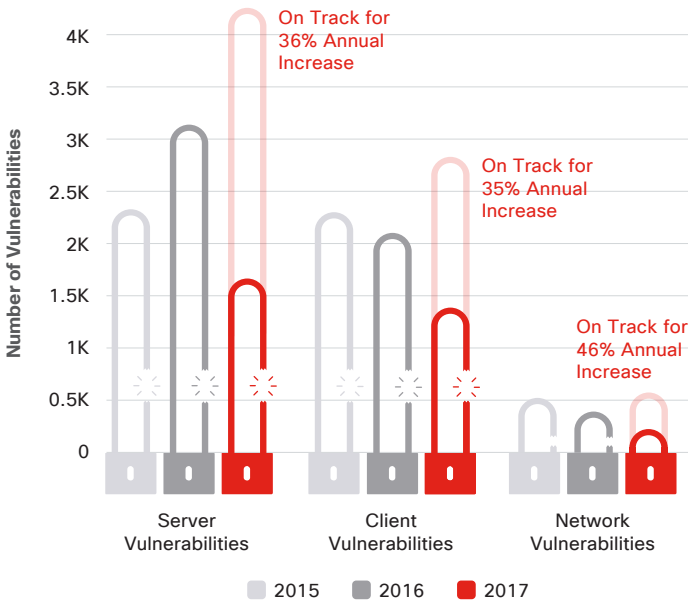
Also of note on the list in Figure 39: The vulnerabilities disclosed for Microsoft Office, which were quickly exploited by the Dridex botnet.[37] As Cisco reported, exploitation of the Microsoft vulnerability was observed in email-based attacks with malicious attachments. In addition, the Apache Struts2 vulnerability was quickly exploited.[38]

Client-server vulnerabilities increasing

As discussed in the *Cisco 2016 Midyear Cybersecurity Report*, server-side vulnerabilities have been on the increase: Adversaries have realized that by exploiting vulnerabilities in server software, they can gain greater access to enterprise networks.[39] In the first several months of 2017, server-side vulnerabilities appear to be on track to show an increase of 36 percent from the number of 2016 vulnerabilities; client-side vulnerabilities show a probable increase of 35 percent from 2016 (see Figure 40).

One reason for the increase in server-side vulnerabilities is that third-party software vulnerabilities require manual patching. If manual patching is not done in a timely manner, the window of exploitation for server-side vulnerabilities is large. And although client-side vulnerabilities are also increasing, they can be patched by auto-updates, which helps to close the window of exploitation very quickly.

Figure 40 Client-server vulnerabilities



Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

37 "Cisco Coverage for CVE-2017-0199," Cisco Talos blog, April 14, 2017: blog.talosintelligence.com/2017/04/cve-2017-0199.html.
38 "Content-Type: Malicious - New Apache Struts2 0-Day Under Attack," by Nick Biasini, Cisco Talos blog, March 8, 2017: blog.talosintelligence.com/2017/03/apache-0-day-exploited.html.
39 "Adversaries See Value in Server-Based Campaigns," *Cisco 2016 Midyear Cybersecurity Report*: cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.

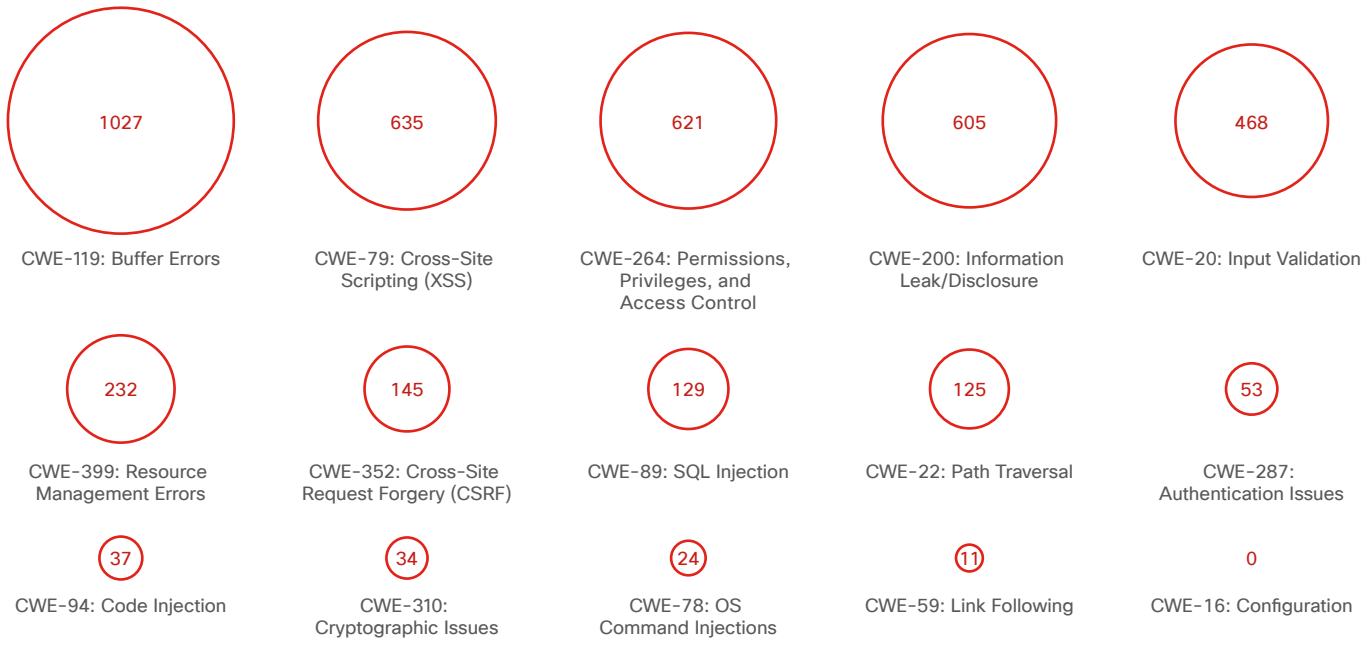
Exploit kit activity down significantly

Exploit kit activity involving vulnerabilities shows a noticeable decline, in line with the overall drop in use of exploit kits by adversaries (see page 9). As software vendors, especially web browsers, have blocked use of common threat vectors such as content created with Adobe Flash and Java, adversaries have increasingly turned toward easier tactics such as ransomware, DDoS, and business email compromise (BEC) (see page 22).

Vulnerability categories: Buffer errors remain in the lead

In examining Common Weakness Enumeration (CWE) threat categories, buffer errors remain the most common type of coding error exploited by criminals (see Figure 41). This is a coding error repeatedly made by software developers. To prevent this error, developers should ensure that buffers are restricted so they can't be exploited.

Figure 41 Top threat categories, November 2016–May 2017



Source: Cisco Security Research

Don’t let DevOps technologies leave the business exposed

In January 2017, attackers began encrypting public MongoDB instances and demanding ransom payments for decryption keys and software. Attackers have since expanded their targets of server-targeted ransomware to other databases such as CouchDB and Elasticsearch.[40] These DevOps services are often exposed because they were deployed improperly or left open intentionally for convenient access by legitimate users.

Rapid7, a Cisco partner and provider of security data and analytics solutions, classifies attacks on MongoDB, CouchDB, and Elasticsearch as “DevOps ransomware attacks.” The company includes technologies such as Docker, MySQL, and MariaDB, and other popular DevOps components in its definition.

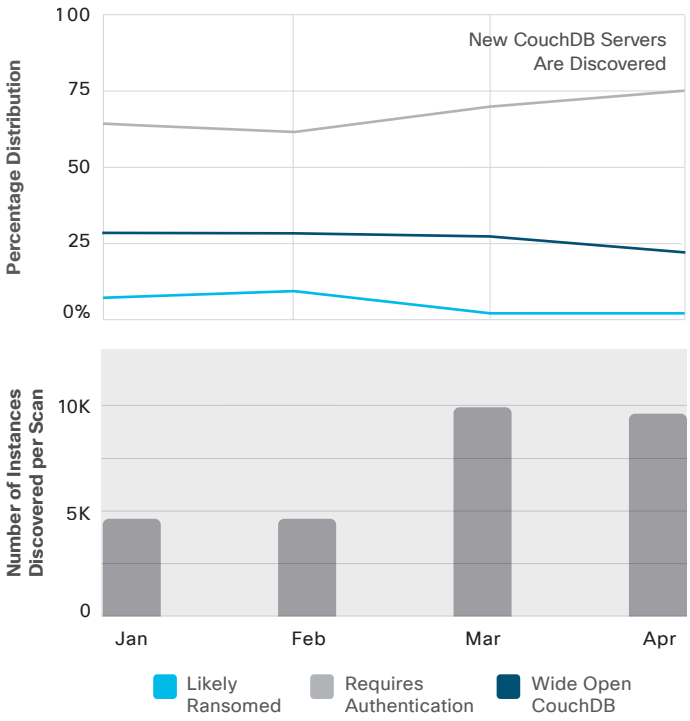
Since January 2017, Rapid7 has been performing regular Internet sweeps for these technologies and cataloging both open instances and ransomed instances. Judging from the names of the tables exposed to the Internet, some of these DevOps services may contain personally identifiable information (PII).

Following is an overview of select findings from Rapid7’s sweeps.

CouchDB

About 75 percent of CouchDB servers can be categorized as wide open (exposed to the Internet and having no authentication). Just under one-quarter require authentication (at least some credentials). About 2 to 3 percent have likely been ransomed. That may not sound like much, but consider that about 2 percent of CouchDB servers that Rapid7 discovered appear to contain PII. That PII includes clinical drug trial information, credit card numbers, and personal contact information.

Figure 42 CouchDB status distribution



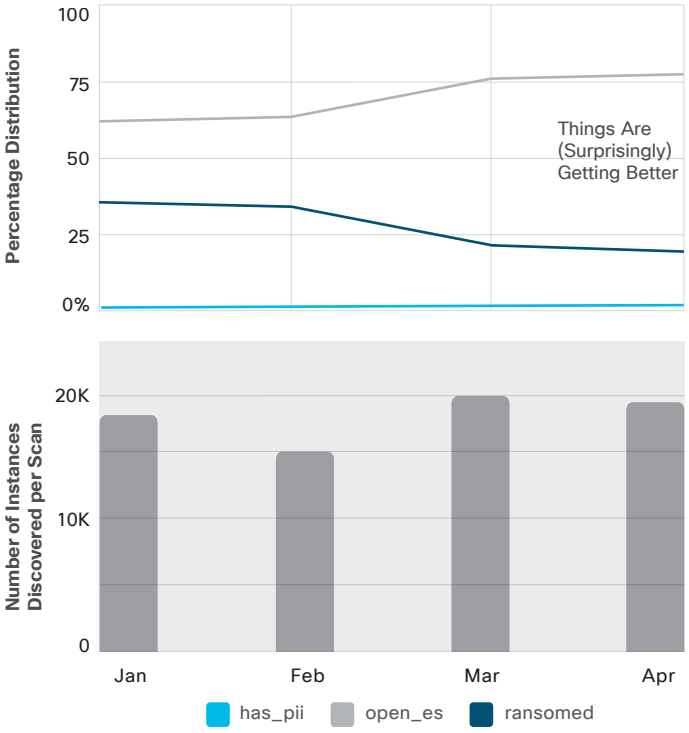
Source: Rapid7

Elasticsearch

Like CouchDB, more than 75 percent of Elasticsearch servers can be categorized as wide open. About 20 percent have likely been ransomed. The good news is that a very low percentage of these servers likely contain PII, according to Rapid7’s analysis.

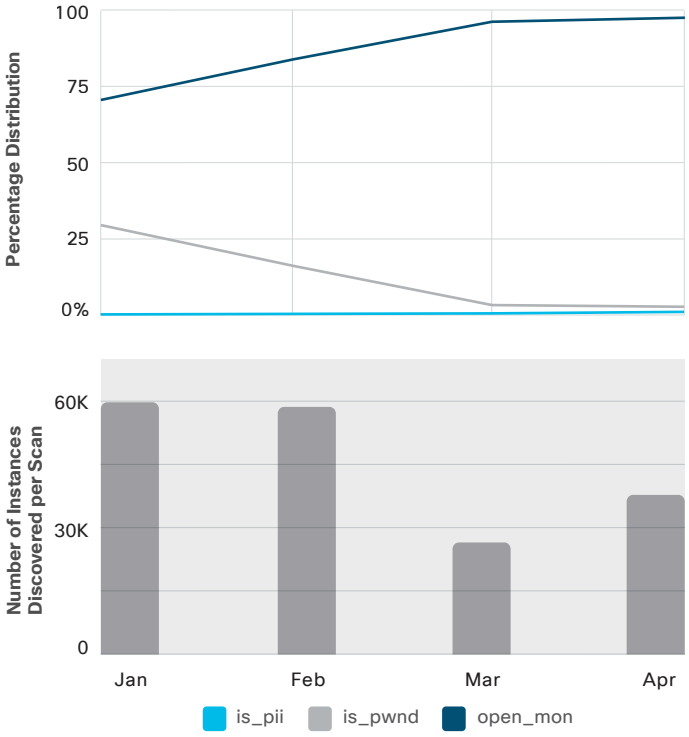
40 “After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters,” by Lucian Constantin, IDG News Service, January 13, 2017: pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html.

Figure 43 Elasticsearch status distribution



Source: Rapid7

Figure 44 MongoDB status distribution



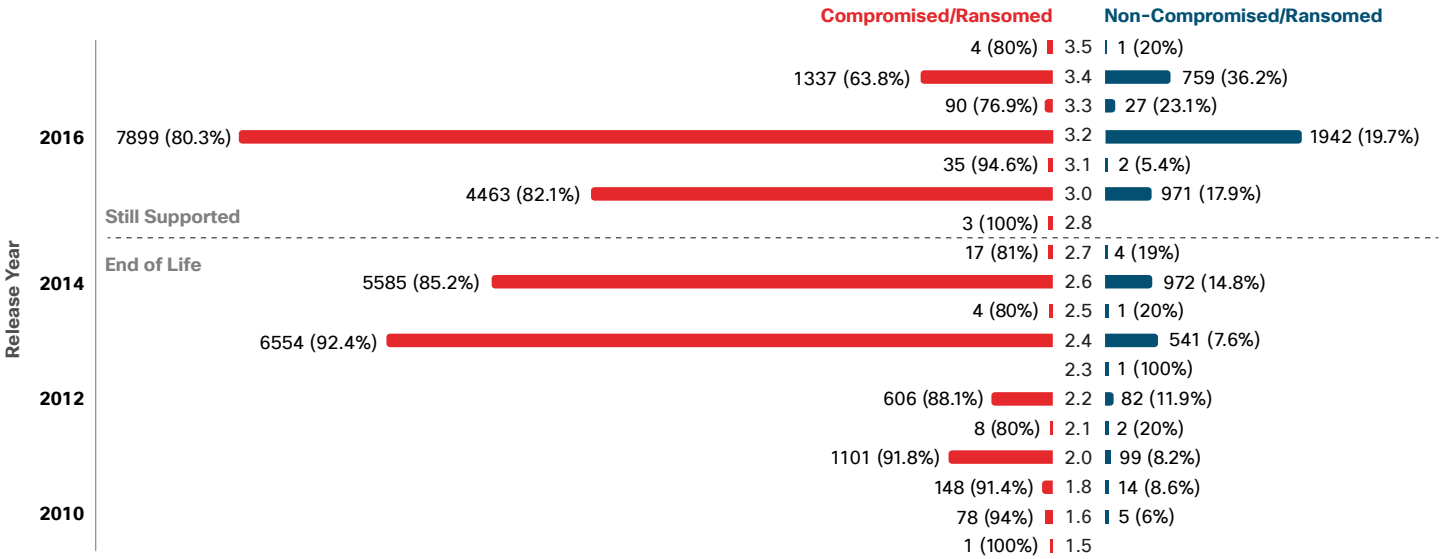
Source: Rapid7

MongoDB

Despite the January ransomware attack that targeted thousands of MongoDB servers, people and organizations using these servers still need to improve their security practices. Nearly 100 percent of the servers Rapid7 encountered during its sweeps could be categorized as wide open. The good news is that very few of these servers appear to contain sensitive information.

Rapid7 also found that many of the MongoDB servers that likely had been compromised by ransomware were at their end-of-life stage. However, a sizable portion were newer and still supported versions that probably have not been updated or patched recently—if ever (see Figure 45 on the next page).

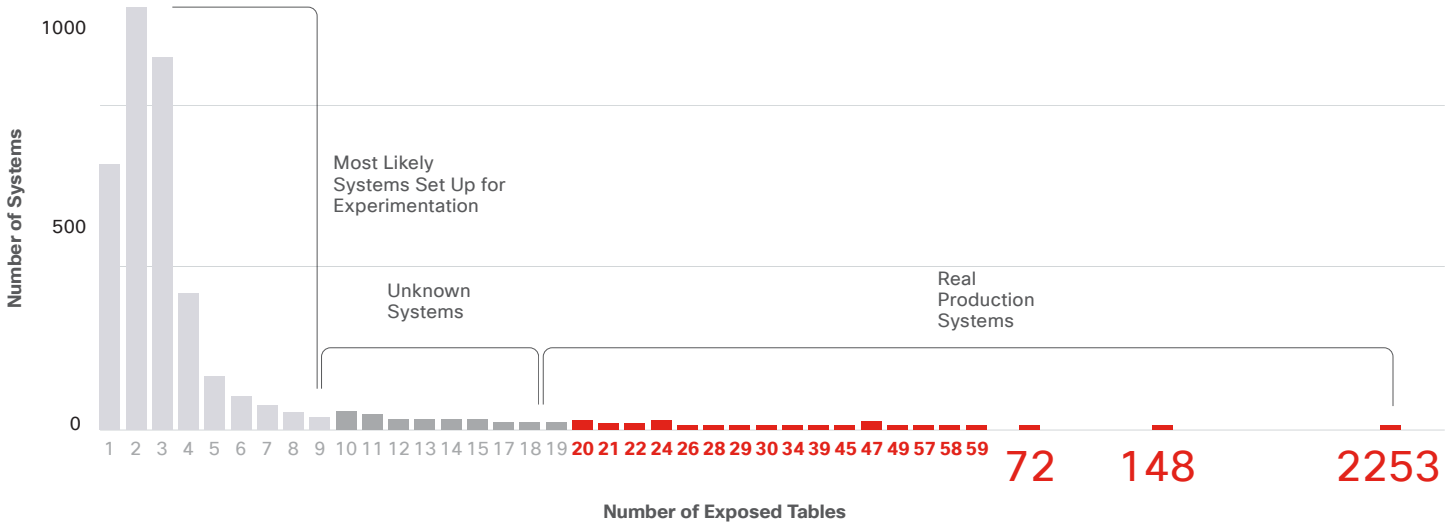
Figure 45 MongoDB versions



Source: Rapid7

Figure 46 shows the number of exposed tables across the MongoDB servers that Rapid7 identified in its study. Most have fewer than 10 tables and are most likely servers that were set up for experimentation. However, some servers have 20 tables or more, indicating that these are real production systems. One server exposed to the Internet had more than 2200 tables.

Figure 46 MongoDB database size distribution by number of exposed tables, January–April 2017



Source: Rapid7

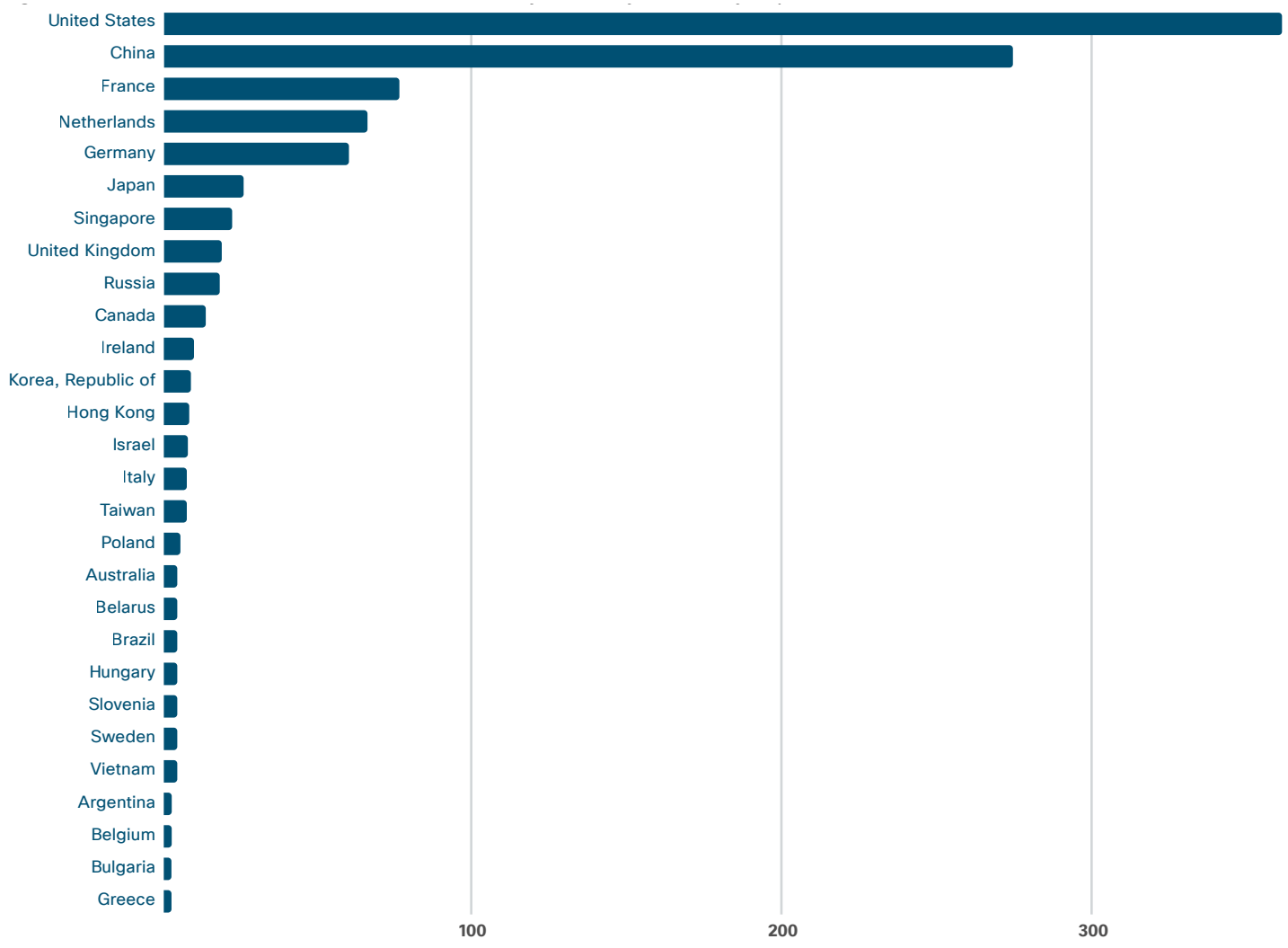
Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Docker

Rapid7 also researched Docker, an orchestration framework whose operators have been very security-minded from the outset. However, despite their efforts, more than 1000 Docker instances are wide open, according to Rapid7's analysis. Most Docker instances that were identified are in the United States or China (see Figure 47).

Many of the open Docker instances are likely abandoned or forgotten test systems. But 245 of the 1000 open instances have at least 4 GB of memory allocated and are likely live production systems (see Figure 48 on the next page).

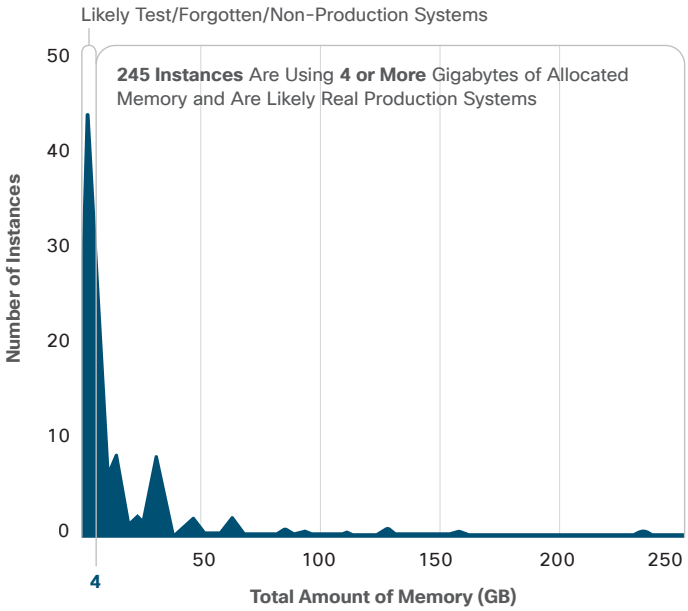
Figure 47 Distribution of Docker instances by country, January–April 2017



Source: Rapid7

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

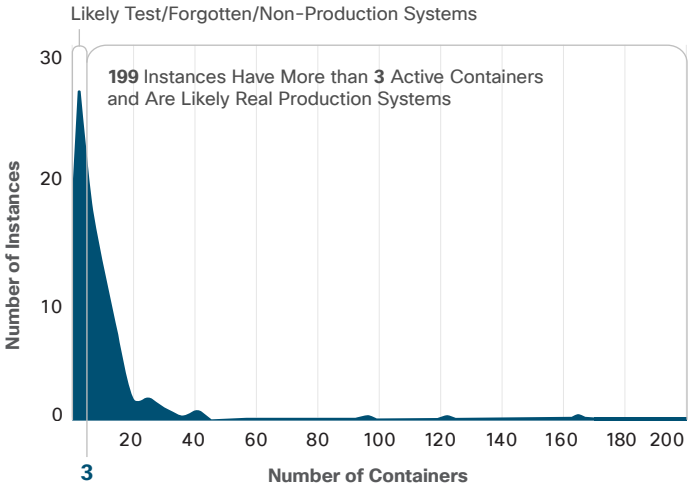
Figure 48 Distribution of total memory allocated for Docker use, January–April 2017



Source: Rapid7

In addition, Rapid7 found that 199 of the wide-open Docker instances have at least three active containers running. Some have up to 160 (Figure 49). The organizations using these insecure production systems are at tremendous risk. An adversary could potentially create a shell connection from the Internet to every one of these systems and take control of them.

Figure 49 Distribution of total running containers per instance, January–April 2017



Source: Rapid7

Organizations that use public Internet instances of these and other DevOps technologies need to take steps now to ensure they are not at risk. Security teams should:

- Develop solid standards for secure deployment of DevOps technologies
- Maintain active awareness of public infrastructure owned by the company
- Keep DevOps technologies up to date and patched
- Conduct vulnerability scans

Organizations not moving fast enough to patch known Memcached server vulnerabilities

Malicious actors are actively seeking out insecure databases exposed to the Internet that they can compromise, steal data from, or hold for ransom. The latter approach has been gaining ground rapidly since the launch of a ransomware attack in January that affected thousands of MongoDB databases.[41]

Services like MongoDB were never meant to be exposed to untrusted environments and typically lack strong (or any) authentication. Cisco threat researchers have been studying the vulnerabilities in similar services. In late 2016, for example, we conducted a code audit to assess the security of Memcached caching servers. Organizations use Memcached to improve the speed and performance of their web services and applications.

41 "MongoDB Databases Actively Hijacked for Extortion," by Ionut Arghire, *SecurityWeek*, January 4, 2017: securityweek.com/mongodb-databases-actively-hijacked-extortion.

We discovered three remote code-execution vulnerabilities as part of that investigation.[42] One of the vulnerabilities was in the server's authentication mechanism, meaning that even servers with authentication enabled could still be exploited. Cisco threat researchers reported the vulnerabilities to the vendor, who quickly issued a patch.

A few months after the vulnerabilities were reported, we performed Internet-wide scans to check on the status of the patch deployment. Even though the vendor was quick to patch, and Linux distributions were swift to issue updates, we found that 79 percent of the nearly 110,000 exposed Memcached servers were still vulnerable to the remote code-execution vulnerabilities that we had reported (see Figure 50).

In addition, only 22 percent of the servers have authentication enabled. And virtually all the servers requiring authentication were still vulnerable (23,707 out of 23,907 (see Figure 50). The servers included in our study are located all over the globe, but most are in the United States and China. Most of the vulnerable servers are in those two countries, as well, as of our last scan in March (see Figure 51).

The bottom line: Although Cisco threat researchers did not find that any of the servers had been compromised due to these three vulnerabilities, it is likely only a matter of time. Information about the vulnerabilities, and the patch to fix them, have been public knowledge for months.

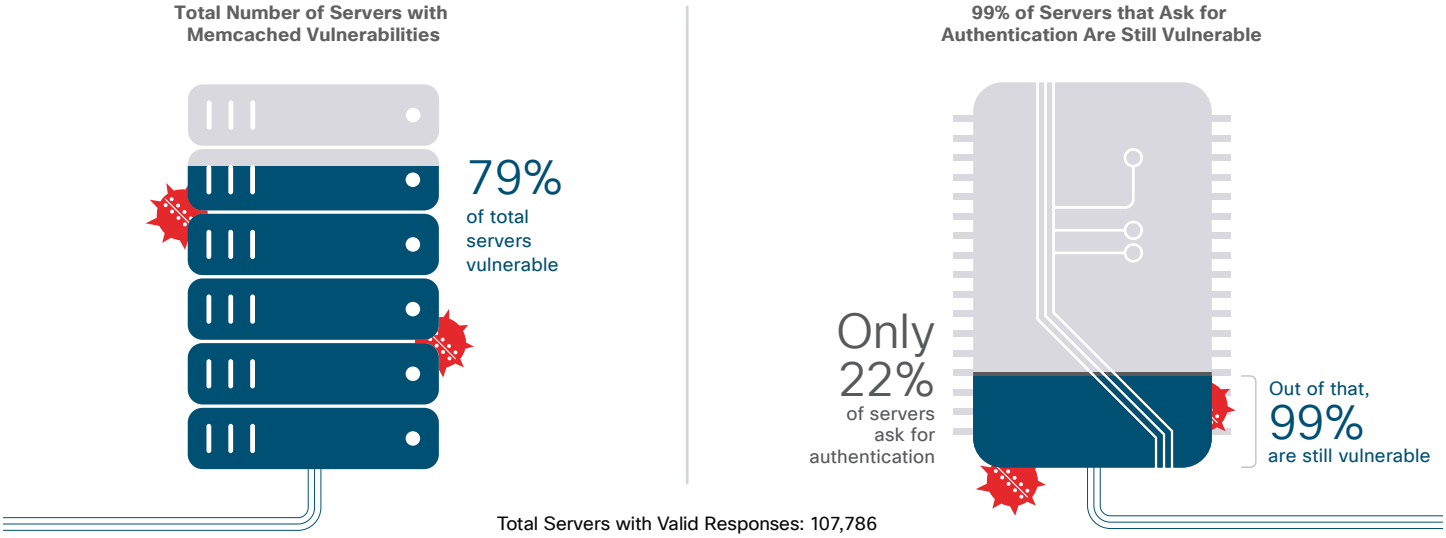
The trend in the shadow economy to attack databases and other infrastructure exposed to the Internet makes the need to patch these known vulnerabilities even more urgent. And even with authentication, DevOps services still pose a risk, which is why they should be isolated from trusted environments (for more about this risk, see "Don't let DevOps technologies leave the business exposed," page 50).

Figure 51 Memcached servers by country, February-March 2017

Country	Vulnerable Servers	Total Servers
United States	29,660	36,937
China	16,917	18,878
United Kingdom	4713	5452
Germany	3047	3698
France	3209	5314
Japan	3003	3607
Netherlands	2556	3287
India	2460	3464
Russia	2266	3901
Hong Kong	1820	1939

Source: Cisco Security Research

Figure 50 Vulnerabilities: Memcached



Source: Cisco Security Research

42 For more information, see the following 2016 Talos Vulnerability Reports: "Memcached Server Append/Prepend Remote Code Execution Vulnerability," talosintelligence.com/vulnerability_reports/TALOS-2016-0219; "Memcached Server Update Remote Code Execution Vulnerability," talosintelligence.com/vulnerability_reports/TALOS-2016-0220; and "Memcached Server SASL Authentication Remote Code Execution Vulnerability," talosintelligence.com/vulnerability_reports/TALOS-2016-0221.

Malicious hackers head to the cloud to shorten the path to top targets

The cloud is a whole new frontier for hackers, and they are exploring its potential as an attack vector in earnest. They understand that cloud systems are mission-critical for many organizations now. They also recognize that they can infiltrate connected systems faster by breaching cloud systems.

Since the end of 2016, Cisco has observed an increase in hacker activity targeting cloud systems, with attacks ranging in sophistication.

In January 2017, our researchers caught hackers hunting for valid breached corporate identities. Using brute-force attacks, the hackers were creating a library of verified corporate user credentials (usernames and passwords), potentially using known lists of compromised accounts on the web. They were attempting to log in to multiple corporate cloud deployments using servers on 20 highly suspicious IPs.

Using behavioral analytics and other tools, our researchers analyzed thousands of customers' corporate cloud environments from December 2016 through mid-February 2017. We identified similar patterns of suspicious login attempt activity targeting more than 17 percent of the organizations in our study. The hackers had been randomly recycling through the 20 IPs to evade detection.

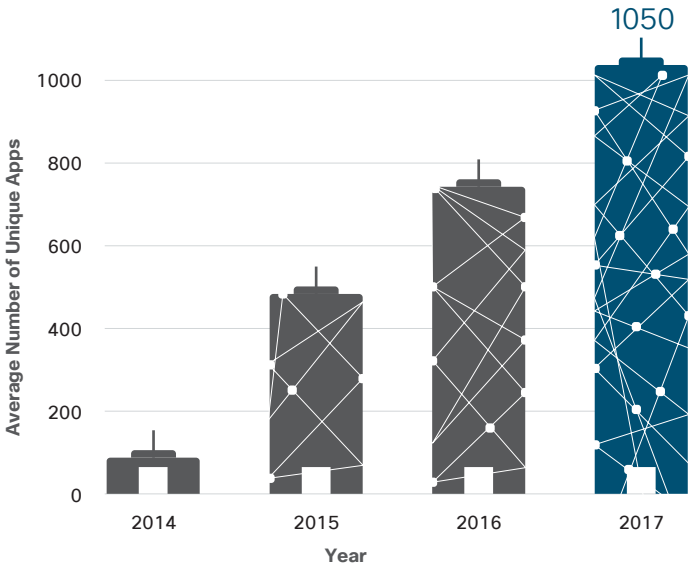
We alerted customers to the issue and blacklisted the suspicious IPs. What the hackers wanted to use the library of verified corporate user credentials for is not known. Preparation for the launch of a spear-phishing or social engineering campaign is one potential scenario. The malicious actors may also have wanted to sell the working username and password combinations, or use the credential themselves to log in to users' accounts to try to exfiltrate sensitive data or compromise other collaborators. What is known is that most of the credentials the hackers were trying to use to access corporate cloud systems were associated with corporate accounts that had been compromised in previous breaches.

OAuth powering the cloud, but also creating risk

In the *Cisco 2017 Annual Cybersecurity Report*, we examined the risk of connected third-party cloud applications introduced into the enterprise by employees. These apps touch the corporate infrastructure and can communicate freely with the corporate cloud and software-as-a-service (SaaS) platforms as soon as users grant access through open authorization (OAuth).

As Figure 52 shows, the number of unique connected cloud apps per organization has increased dramatically since 2014, according to our research. The average enterprise today has more than 1000 unique apps in its environment and more than 20,000 different installations of those apps.

Figure 52 Number of unique connected cloud apps per organization



Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

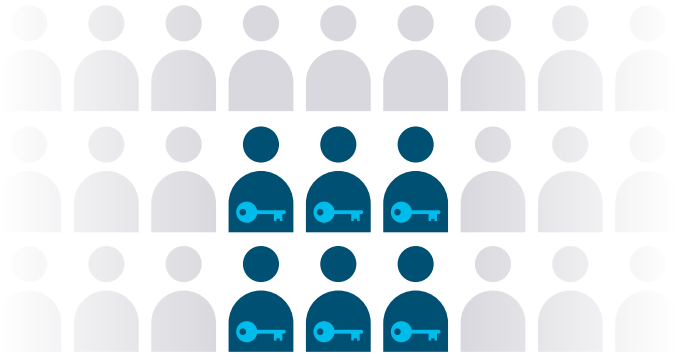
The recent phishing campaign that targeted Gmail users and attempted to abuse the OAuth infrastructure underscored the OAuth security risk.[43] The attackers sought to gain control of users' email accounts and spread the phishing worm to their contacts. Google reported that about 0.1 percent of its 1 billion users were affected by the campaign.[44] Cisco threat researchers conservatively estimate that more than 300,000 corporations were infected by the worm.[45]

Cloud is the ignored dimension: The single privileged cloud user presents great risk

Some of the largest breaches to date began with the compromise and misuse of a single privileged user account. Gaining access to a privileged account can provide hackers with the virtual "keys to the kingdom" and the ability to carry out widespread theft and inflict significant damage. However, most organizations aren't paying enough attention to this risk.

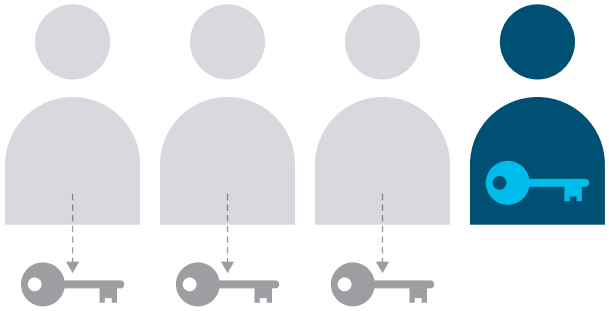
To better assess the scope of this security issue, Cisco threat researchers examined 4410 privileged user accounts at 495 organizations and found that six in every 100 end users per cloud platform have privileged user accounts (see Figure 53). However, in most organizations, only two privileged users, on average, carry out most of the administrative tasks (88 percent). We also determined that organizations could remove "super admin" privileges from 75 percent of their admin accounts with little or no business impact.

Figure 53 Inflation of privileged user accounts

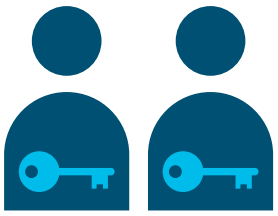


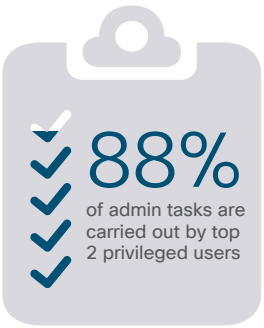
6/100

end users per cloud platform have privileged user accounts



75% of privileges can be removed from admin accounts with **little or no business impact**





88% of admin tasks are carried out by top 2 privileged users

Source: Cisco Security Research

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

43 "Google Docs Phishing Attack Underscores OAuth Security Risks," by Michael Kan, IDG News Service, May 5, 2017: pcworld.com/article/3194816/security/google-docs-phishing-attack-underscores-oauth-security-risks.html.

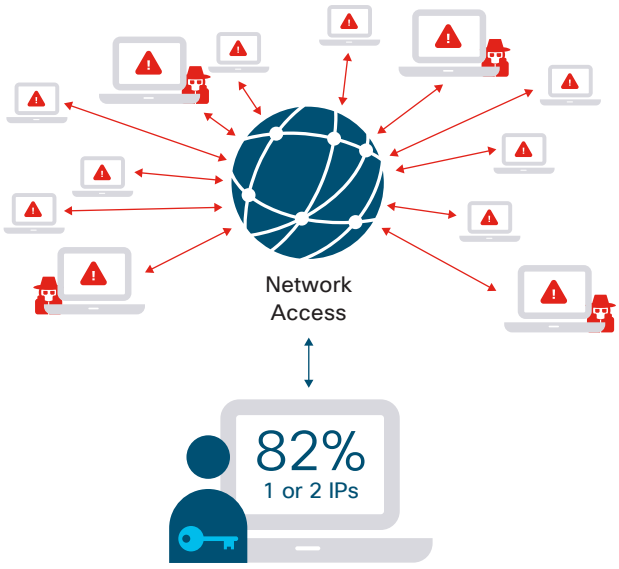
44 "A Massive Google Docs Phish Hits 1 Million Gmail Accounts—UPDATED," by Thomas Fox-Brewster, *Forbes*, May 3, 2017: forbes.com/sites/thomasbrewster/2017/05/03/massive-google-gmail-phish-many-victims/#219602e142a1.

45 Cisco's estimate is based on the number of businesses paying for Google's cloud-based productivity tools (see "More than 3M businesses now pay for Google's G Suite," by Frederic Lardinois, TechCrunch, January 26, 2017: techcrunch.com/2017/01/26/more-than-3m-businesses-now-pay-for-googles-g-suite/) and the number of customers that use Cisco's cloud access security broker (CASB) solutions and were affected by the phishing campaign that targeted Gmail users (about 10 percent).

According to our research, about 82 percent of privileged users log in from just one or two IP addresses per month (Figure 54). Activity outside those normal patterns should be investigated.

We also found that 60 percent of privileged users never log out of active sessions, making it easier for unauthorized users to gain access and to do so undetected (Figure 55). Users should log in daily to take administrative actions, and log out when work is complete.

Figure 54 Privileged user activity (monthly login activity from IP addresses)



Source: Cisco Security Research

Embracing shared responsibility for cloud security

As companies look to expand their use of the cloud, they need to understand their role in ensuring cloud security. Cloud service providers are responsible for the physical, legal, operational, and infrastructure security of the technology they sell. However, businesses are responsible for securing the use of underlying cloud services. Applying the same best practices that they use to ensure security in on-premises environments can go a long way toward preventing unauthorized access of cloud systems.

Figure 55 60% privileged users never log out of active sessions

Source: Cisco Security Research

Unmanaged infrastructure and endpoints leave organizations at risk

Today's dynamic networks enable a greater attack surface by introducing new security risks and gaps and reducing visibility. The cloud is a major contributor to this issue. So, too, are rogue and so-called shadow IT devices and applications. Networks and endpoints that age out of network- and asset-management solutions can also create unknown and unmanaged security gaps.

Many companies underestimate the risk (and the number) of blind spots in their enterprise network, endpoint, and cloud infrastructure. According to research by Lumeta, a Cisco partner that provides cyber situational-awareness technology, a lack of visibility can lead to 20 to 40 percent of network and endpoint infrastructure, on average, becoming unknown or unmanaged by an organization. This issue affects companies across verticals, including government, healthcare, financial services, and technology.

Unmanaged network infrastructure and endpoints can be easily compromised by attackers looking to gain a foothold that will enable them to move laterally within an organization and breach specific targets. They can also be used to exfiltrate data or send unauthorized Tor traffic, or can become part of a botnet. Even a simple router, network firewall, or segmentation misconfiguration can provide an attacker with an opportunity to penetrate infrastructure and gain access to sensitive data.

To achieve visibility, organizations need access to real-time, context-driven security intelligence. Without solutions that enable real-time monitoring and leak path detection, attackers can successfully move around a network unchecked and undetected. In addition, organizations should review their segmentation policies and employ robust tools that can test their effectiveness.

Organizations must also inventory devices and systems connecting to the network. If security teams have only snapshot views or old lists of managed devices to reference, they can miss at least 20 percent of what is physically hardwired to the network. Such inventories should be conducted regularly and automatically, because enterprise network, endpoint, and cloud infrastructure changes constantly and cannot be monitored effectively by security personnel alone.

Security Challenges and Opportunities for Defenders

Security Challenges and Opportunities for Defenders

In this section, we explore vertical-specific findings from Cisco's latest Security Capabilities Benchmark Study in a series of short case studies. We also present data that suggests that organizations can improve their security by reducing the number of security vendors that they work with, and discuss how company size can have an impact on security. Lastly, we explore the opportunity that security leaders have to engage business leadership in discussions about cybersecurity—and claim a seat at the "top table."

Security Capabilities Benchmark Study: Focus on verticals

Using data from the 2017 study, we examined several verticals.[46] The findings are paired with insights on such key industry challenges as protecting customer data, dealing with regulatory constraints, and integrating newer connected systems with legacy software.

Although each industry faces its own unique security challenges—and although security maturity varies from industry to industry—there are common concerns. Security professionals in every industry are aware of the evolving sophistication of threats, and the need to stay a step ahead of adversaries. Many organizations have experienced public breaches, so mitigating damage (such as a loss of customers) and preventing similar breaches are high on the list of worries.

In many of the verticals, the need to integrate information technology (IT) and operational technology (OT) is critical—and, especially, ensuring that the integrated systems are protected. The recent WannaCry ransomware attack caused shutdowns at the Renault-Nissan auto plants in Europe, an example of how connected systems can be affected by an attack. If connectivity is not done securely and in a coordinated fashion, then even untargeted ransomware can affect OT systems.[47]

In the past, these technologies and their respective teams worked separately: The OT staff managed machines and plants, while IT managed enterprise business applications. Today, many OT sensors and systems are being accessed from the business side. As an example, manufacturing execution systems (MES) now seek the streams of telemetry from those sensors to better optimize and predict operations.

As connected systems come to the OT world, IT and OT can no longer be walled off from each other. They can benefit by sharing data for analysis to help improve safety and product quality. They can also work together to manage cybersecurity threats. But to do so, they must develop their defense-in-depth capabilities, since disconnected and siloed systems won't provide a comprehensive view of IT and OT.

To learn more about IT and OT convergence, read the Cisco white paper, IT/OT Convergence: Moving Digital Manufacturing Forward.

46 *Cisco 2017 Annual Cybersecurity Report*, p. 49: b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153.
47 "Renault-Nissan Is Resuming Production After a Global Cyberattack Caused Stoppages at 5 Plants," by Laurence Frost and Naomi Tajitsu, BusinessInsider.com, May 15, 2017: businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5.

Company size affects approach to security

When attackers breach networks and steal information, small and medium-sized businesses (SMBs) are less resilient in dealing with the impacts than larger organizations. If a public breach damages a brand and causes customers to switch to a competitor, a larger business can weather the impact better than a smaller business. Given the increased risk of business disruption, SMBs can strengthen their position by ensuring they have security processes and tools that minimize the impact of threats and breaches.

In examining data from the 2017 Security Capabilities Benchmark Study, SMBs (defined as organizations with 250 to 499 employees) exhibit shortfalls in their defenses compared with larger organizations. SMBs are naturally tasked to secure their organizations with fewer resources and limited expertise, so they are also more likely to view certain threats or functions to be high risks. When asked about areas they view to be high risks to their organizations, 29 percent of SMBs reported ransomware, compared with 21 percent of organizations with more than 10,000 employees; 30 percent of SMBs view regulatory compliance constraints as a high risk, while only 20 percent of the largest companies do (see Figure 56).

Figure 56 Perceived risk of threats by size of organization

Risk: Which—if any—of the following do you consider to be HIGH security risks for your company?	**Percentages** Organization Size 250-499	500-999	1000-9999	10,000+
Proliferation of BYOD and smart devices	29	28	29	25
Viability of disaster recovery and business continuity	28	25	26	21
Regulatory compliance constraints	30	25	24	20
Advanced persistent threats	34	33	34	30
Ransomware	29	25	25	21

Source: Cisco 2017 Security Capabilities Benchmark Study

Due to smaller budgets and expertise, SMBs are also somewhat less likely to have key security defenses in place. For example, only 34 percent of SMBs reporting using email security, compared with 45 percent of large organizations (see Figure 57); 40 percent of SMBs use data loss prevention defenses, compared with 52 percent of large organizations.

Figure 57 Likelihood of using key threat defenses by size of organization

Complexity: Which—if any—of these types of security threat defenses does your organization currently use?	**Percentages** Organization Size 250-499	500-999	1000-9999	10,000+
Data loss prevention	40	43	47	52
DDoS defense	33	35	42	39
Email/messaging security	34	41	45	45
Encryption/privacy/data protection	39	38	49	52
Endpoint protection/antivirus, anti-malware	36	37	45	45
Patching and configuration	26	28	32	35
Web security	37	39	44	45
Secured wireless	32	35	40	42

Source: Cisco 2017 Security Capabilities Benchmark Study

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Larger organizations are also more likely to have written, formal strategies in place than SMBs (66 percent versus 59 percent), and are more likely than SMBs to require their vendors to have ISO 27018 certifications (36 percent versus 30 percent).

SMBs looking to improve their security posture could focus on improving security policies and procedures, and on adopting common threat defenses more widely to reduce the risk of suffering adverse impacts from attacks. Working with external security services can provide the expertise needed to implement an effective, formal security strategy to develop best practices while augmenting their staff with expertise around monitoring and incident response.

To adopt a security infrastructure that fits business needs and budgets, security teams should work with vendors to provide solutions that integrate to simplify the security environment to a manageable yet effective level. Likewise, growing organizations can follow standards such as the NIST Cybersecurity Framework to build out their security. For businesses of every size, a more holistic approach to security will offer more effective protection against evolving threats.

Using services to bridge knowledge and talent gaps

Within security departments, the debate continues as to which defense approach is preferred: Best-in-class solutions or an integrated architecture. However, security teams face another challenge that affects all security decisions: The lack of in-house security expertise. As threats continue to evolve and technology choices proliferate, organizations should increase their reliance on security services to fill talent gaps.

The struggle to find and retain qualified talent still impacts security teams; the Security Capabilities Benchmark Study found that in many industries, a shortage of trained personnel is considered a major obstacle in adopting advanced security processes and technology. Indeed, the shortage of talent is a global problem. Here again, outside services can bridge the talent gap.

According to Cisco security services experts, knowledge of the security landscape is often the missing element in a defensive framework. The expertise of long-term security professionals provides an analysis that products can't always offer—even the best automated solutions.

"Alert fatigue" is an ongoing problem for in-house security teams. As discussed in many of the vertical-focused articles in the 2017 Security Capabilities Benchmark Study, many security personnel see far more daily alerts than they can investigate, leaving potentially serious threats unremediated. When many low-level alerts are generated, they can be automated, an opportunity that many organizations are failing to take advantage of—perhaps simply because of a resource deficiency or an absence of skill. By automating as many of the low-level alerts as possible, organizations can concentrate on higher-priority concerns that are more likely to have a greater impact to the rest of the organization's environment.

The causes of alert fatigue are several. Siloed systems may create duplicate alerts, or teams may not have the knowledge to distinguish between low- and high-priority alerts, or false positives. They may lack tools such as auditing that can determine the source of potential threats. This is where out-of-the-box thinking from outside services teams can cut through the "fatigue" and offer nuanced counsel on threats that need response.

A lack of product knowledge can also thwart security teams' efforts to get the most value from their technology purchases. Products are often implemented by product specialists, not security specialists. Security teams may not understand how to integrate products to provide a holistic view on threats—the "single pane of glass" that is desirable for a true picture of security effectiveness. Experienced managed-security teams can also assist security professionals in managing cloud solutions and understanding how their data is protected (or not). Cloud providers may not be using security protections such as two-factor authentication; experts can help organizations study SLAs and contracts to determine the defenses that cloud providers are using.

Outsourcing service and threat alert data by country

In examining the use of outsourced services by country, SMBs in certain countries show a greater likelihood of using outsourced services than their enterprise counterparts. For example, in Australia, 65 percent of SMBs use outsourced incident response services, compared with 41 percent of enterprises. In Japan, 54 percent of SMBs use outsourced monitoring services, compared with 41 percent of enterprises (see Figure 58).

In examining alerts investigated and remediated based on region and company size, SMBs in India, Brazil, and the United States show the highest percentages. When it comes to remediated alerts, SMBs in China, Russia, and Great Britain show the highest percentages (see Figure 59).

Figure 58 Percent of SMBs and enterprises outsourcing services by country

When it comes to security, which—if any—of the following types of services are outsourced fully or in part to third parties?	US		BR		DE		IT		GB		AU		CN	
Advice and consulting	49	47	40	44	41	47	45	44	43	51	63	52	50	57
Audit	51	48	48	56	45	49	40	44	49	48	39	30	28	44
Incident response	43	46	43	32	45	41	61	42	45	40	65	41	32	42
Monitoring	54	44	44	38	38	41	50	39	46	41	47	36	33	35
Remediation	34	34	26	21	45	42	32	23	30	34	38	28	46	47
Threat intelligence	43	40	33	37	38	40	44	36	29	42	54	34	28	42
None of the above are outsourced	14	15	7	13	6	15	2	10	11	20	5	14	20	12
	IN		JP		MX		RU		FR		CA			
Advice and consulting	56	62	60	59	58	63	46	50	52	51	48	50		
Audit	43	50	35	25	57	64	37	43	44	56	44	50		
Incident response	53	55	69	55	39	41	37	35	54	42	49	45		
Monitoring	42	51	54	41	44	46	34	44	51	57	49	50		
Remediation	44	43	40	28	12	24	31	50	34	35	36	45		
Threat intelligence	50	60	41	31	36	38	39	39	43	45	45	42		
None of the above are outsourced	6	5	1	6	5	5	6	7	2	5	10	11		

Figure 59 Alert averages by country

	US		BR		DE		IT		GB		AU		CN	
On average, what percent of the total number of alerts are investigated?	59.7	62.8	61	65.5	44.4	52	45.8	61.3	47.4	44.2	55.6	60.8	44.8	42.5
Of those investigated alerts, what percent are legitimate incidents?	30.6	25.7	27.1	26.2	20.2	28.2	22.8	15.2	26.3	23	27.2	28.6	30.6	44.5
Of those legitimate incidents, what percent are remediated?	40.9	45.3	35.4	46.3	43.7	50.4	34.8	40.9	47.3	45.6	40.6	46.2	53.5	67.9
	IN		JP		MX		RU		FR		CA			
On average, what percent of the total number of alerts are investigated?	60.5	65.1	50.6	58.1	59.1	60.6	59.3	65.9	49.1	51.3	49.3	48.8		
Of those investigated alerts, what percent are legitimate incidents?	37.1	39.7	25.4	33.8	27.8	20.5	23.4	33.2	21.8	25.5	22.2	23.8		
Of those legitimate incidents, what percent are remediated?	45.8	48.3	44.3	38.4	43.8	48.6	47.3	60.5	41.6	52.4	35.8	37.6		

Organization Size Small/Medium (299-500 employees) Enterprise (1000+ employees)

Source: Cisco 2017 Security Capabilities Benchmark Study

IoT security risks: Preparing for the future—and the now

The Internet of Things (IoT), as Cisco defines it, is the inter-networking of physical devices, vehicles, buildings, and other items (also referred to as "connected devices" and "smart devices") that are embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. Cisco views the IoT as being made up of three main contexts: Information technology (IT), operational technology (OT), and consumer technology (CT).

The Industrial Internet of Things (IIoT), meanwhile, refers specifically to connected devices within an industrial control network, as opposed to a corporate IT network or data center.

The IoT holds great promise for business collaboration and innovation. But as it grows, so too does the security risk it presents to organizations and users.

Lack of visibility is one problem. Most defenders are not aware of what IoT devices are connected to their network. IoT devices, which include everything from cameras to thermostats to smart meters, are generally not built with security in mind. Many of these devices lag well behind desktop security capabilities and have vulnerability issues that can take months or years to resolve. In addition, they typically:

- Have little or no CVE reporting or updating
- Run on specialized architectures
- Have unpatched or outdated applications that are vulnerable, like Windows XP
- Are rarely patched

Also, IoT devices cannot be accessed easily or at all by their direct owners, making it difficult to impossible to remediate when systems have been compromised. In short, these devices can serve as strongholds for adversaries (see "Ransomed medical devices: It's happening," on page 42, for examples of this situation).

Compounding the security problems with IoT devices is the fact that defenders may have difficulty understanding the nature of the alerts coming from these devices. In addition, it is not always clear who inside the organization is responsible for addressing IoT compromises. Teams responsible for implementing these technologies typically leave, or are let go by, the organization following completion of the project.

Defenders need to start focusing on potential IoT weaknesses because adversaries want to target them to launch ransomware campaigns, steal sensitive information, and move laterally across networks. IoT devices are the type of vulnerable "low-hanging fruit" that threat actors are quick to exploit.

In the big picture, a massive compromise of these devices has the potential to severely disrupt businesses and governments—and the Internet itself. DDoS attacks involving IoT devices have already occurred, and the rise of IoT botnets (see page 39) suggests threat actors are already working to lay the groundwork for destructive campaigns of unprecedented magnitude.

To meet the security challenges of the IoT—an attack surface that is both growing rapidly and becoming increasingly difficult to monitor and manage—defenders will need to:

- Keep older signatures active
- Surround IoT devices with IPS defenses
- Closely monitor network traffic (this is especially important to do in IIoT environments, where network traffic patterns are very predictable)
- Track how IoT devices are touching the network and interacting with other devices (for example, if an IoT device is scanning another device, that is likely a red flag signaling malicious activity)
- Implement patches in a timely manner
- Work with vendors that have a product security baseline and issue security advisories

In an IoT world, a proactive and dynamic approach to security, and a layered defense strategy, are the keys to protecting IoT devices from infection and attack—or at least, mitigating the impact when some are inevitably compromised by adversaries.

Security Capabilities Benchmark Study: Focus on select verticals

Service providers

Key industry concerns

The service provider market, as surveyed by Cisco, is a diverse industry, including businesses such as telecommunications, cloud- and web-scale infrastructure and hosting, media companies, and applications provided under the software-as-a-service (SaaS) model. In addition, service providers are often selling managed security services: 71 percent of the service providers surveyed said they provide managed security services to end customers.

Service providers have myriad challenges, such as protecting their IT and production infrastructure as well as their customers' data. Fifty-nine percent of the service provider security professionals said their top priority is securing their own data centers or core production networks.

These challenges are exacerbated by the scale of service provider businesses. Security professionals are concerned that the scale of their organizations, and the expanding threat surface, increase the chances that attackers may interrupt their core business, providing service to their customers. In an industry with high customer churn, public breaches can damage the bottom line: 34 percent of the service providers said they'd lost revenue due to attacks in the past year.

The key challenge for many service providers is understanding how to integrate security tools and processes for maximum effectiveness—and reducing the sprawl of services and tools they have on hand.

The economic reality for service providers is that unless provided as a managed service, security is a cost center, not a profit center, and therefore needs to be kept lean—but the pressures of competition and the threat landscape have forced an increased focus on security.

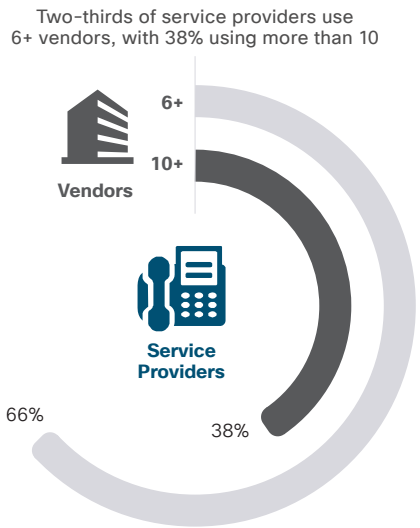
Service provider scale creates challenges

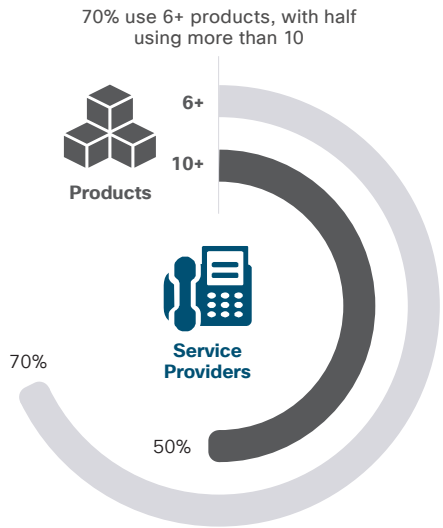
As in every industry, the proliferation of security vendors and tools is a problem, because solutions are often not integrated and don't provide an actionable view of the threats facing the provider. In the service provider space, this problem is magnified by the scale of the market. Two-thirds of service provider security professionals said they rely on six or more vendors; 38 percent said they rely on more than 10 vendors (Figure 60).

When asked about products in use, 70 percent said they use at least 6 security products, and half use more than 10 products. In many cases, say Cisco experts in this market, there isn't much integration among products, which means they experience an exponential increase in complexity for each incremental gain in security.

Figure 60 Percentage of service providers that use solutions from 6 or more vendors and products

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**





Source: Cisco 2017 Security Capabilities Benchmark Study

Breaches can increase customer churn

More than half (57 percent) of the service providers said they had dealt with public scrutiny due to a data breach. Of those who'd suffered a public breach, nearly half said the breach drove improvements in security to a great extent; 90 percent said the breaches drove improvement to at least a modest extent. On this basis, service provider security professionals appear to rapidly incorporate the lessons learned from breaches.

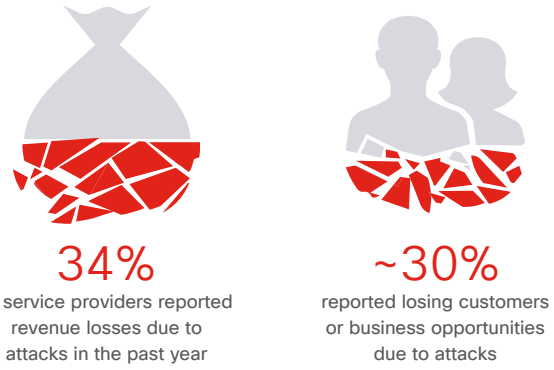
Thirty-four percent of the service providers reported revenue losses due to attacks in the past year; about 30 percent reported losing customers or business opportunities due to attacks (see Figure 61). Service providers said that operations, brand reputation, and customer retention were the business functions harmed the most by public security breaches.

In a large and competitive market, service providers have much to lose from security breaches. Customers have many choices and will be quick to switch providers if they believe their data or their own customers can't be protected.

High adoption of standards

Service providers appear to be quite a bit ahead of other industries in terms of adopting standards—which may be a result of their ability to manage the scope and scale of their businesses. About two-thirds said they have written formal security strategies, and follow a standardized information security policy practice. In addition, nearly all service providers surveyed agree that security processes and procedures are clear and well-understood in their organizations.

Figure 61 Revenue losses from attacks



Source: Cisco 2017 Security Capabilities Benchmark Study

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Public sector

Key industry concerns

Because of various constraints, public sector organizations tend to be more reactive than proactive about security threats. Limited budgets, a struggle to attract talent, and lack of visibility into threats all affect the public sector's ability to defend networks against attackers.

However, the public sector is also beholden to regulations that require close attention to cyber-risk management—more so than most of the private sector. For example, in the United States, federal agencies must comply with the Federal Information Security Management Act (FISMA) to protect the confidentiality and integrity of mission-critical information systems. There are similar requirements on the state and local levels: A bewildering array of new and old regulations cover state and local utility organizations depending on the services delivered.

Public sector organizations are also struggling to manage the transition to the cloud, a process that is also affected by regulations. At the federal level, the Federal Risk and Authorization Management Program (FedRAMP) provides standards for the use of cloud products and services; state and local governments also require certification for cloud providers housing government data.

Managing data in the cloud

The transition to the cloud presents many advantages as well as challenges to public sector organizations that need to maintain consistent protection against threats. One-third of public sector organizations said that targeted attacks, APTs, and insider exfiltration are high security risks. In addition, public sector security professionals said that public cloud storage and cloud infrastructure are the most challenging elements to defend against attacks.

The issue, say Cisco public sector security experts, is that cloud storage offers a different set of tools to protect data, forcing security teams to rethink how they will configure tools and processes to keep data safe. For example, the features in the NetFlow analysis tool don't map precisely to analysis tools in cloud services, so processes and outcomes won't be the same.

Budget, talent shortages affect threat analysis

Budget, talent, and regulatory constraints may also be getting in the way of security goals within the public sector. For example, organizations may be slow in adopting certain tools because they require knowledgeable staff to implement them, and to analyze results. Only 30 percent of the public sector security professionals said their organizations use penetration testing and endpoint or network forensics tools (see Figure 62). These tools are considered key pillars of a defense-in-depth security strategy, so their lack of adoption is worrisome. Organizations without these services baked into security can expect to see network breaches repeatedly.

Figure 62 Percentage of public sector organizations using various defenses

Roughly only 30% use pen testing and endpoint or network forensics

Source: Cisco 2017 Security Capabilities Benchmark Study

Advanced persistent threats

Advanced persistent threats, or APTs, are attacks that are intended to give the adversary time to operate. The threat is designed so that the attacker can remain in a network undetected for a long period of time, usually with the intent to steal data.

Without enough security experts on hand, public sector organizations may also fall short on threat investigation. Nearly 40 percent of the public sector organizations report that of the thousands of alerts they see daily, only 65 percent are investigated. Of those threats investigated, 32 percent are identified as legitimate threats, but only 47 percent of those legitimate threats are eventually remediated.

The number of threats that go uninvestigated is evidence of the need for tools that share information about alerts and provide analysis. Such tools add texture and understanding to alerts (making them more valuable), so that staff can determine which ones need immediate attention. In addition, automation can help resolve some threats, reducing the burden on security teams.

To truly examine a large number of daily alerts, Cisco security experts say, a public sector organization might need dozens of security staffers—yet they rarely have the headcount. Thirty-five percent of the public sector organizations said they have fewer than 30 employees dedicated to security. In addition, 27 percent said they believe a lack of trained personnel is a major obstacle to adopting advanced security processes and technology. This is another reason why automation tools can be essential to building a security defense system to process the amount of threat alerts generated daily.

Breaches drive security improvements

The shortage of people and tested security tools in the public sector has an impact on breaches. Fifty-three percent of the public sector organizations said they have dealt with public scrutiny due to data breaches. It should be assumed that breaches *will* happen, not that organizations might get lucky and be spared an attack. A related problem is that security direction is driven by the response to attacks—not by a holistic approach to risk-based security. So much effort is needed to respond to incoming threats that there are no resources left for long-term planning.

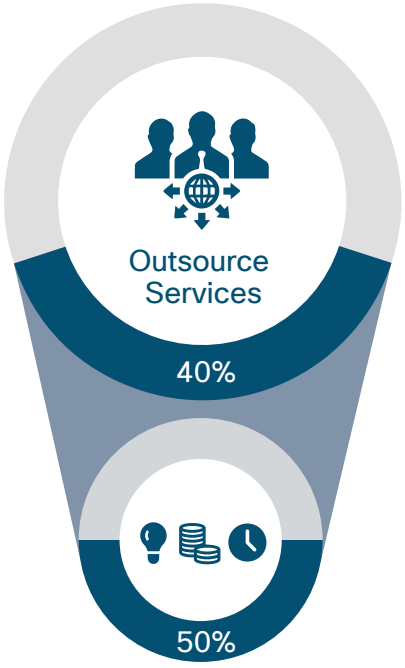
Public sector organizations do indicate that when breaches happen, security teams learn from the experience: 46 percent said breaches drove security improvements to a great extent. However, organizations need to invest in technology that gets them out in front of security breaches, so they can better minimize risk and more effectively manage security systems.

Outsourcing adds value, but doesn't increase in-house expertise

Outsourcing is a key strategy for public sector organizations looking to gain more resources. Over 40 percent said they fully or partially outsource services such as monitoring and audits. Of those organizations that outsource security services, roughly half cite unbiased insight, cost efficiency, and timely incident response as the top reasons to do so (see Figure 62).

Penetration and other audit services should be done by an outside organization, but there is a downside to full reliance on outsourced services: It means that public services organizations do not build in-house expertise over time. This in-house knowledge is critical in defending networks against sophisticated attacks. Automated solutions can be cost-effective and timely, but should strike a balance between outsourcing and on-sight experts in order to gain essential insights and analysis.

Figure 63 Outsourcing adds much-needed services



Source: Cisco 2017 Security Capabilities Benchmark Study

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Retail

Key industry concerns

When security breaches hit the retail industry, the news quickly becomes high-profile. Since attacks on retailers often involve the exposure of customer financial data or other personal information, they receive media attention and require outreach to consumers. Attacks and data breaches in retail affect brand reputation in a much more concrete fashion than in other industries like healthcare or utilities. Customers have many choices among retail providers, and if they perceive that a retailer is careless about security, they can easily switch to others.

High-profile attacks on major retailers, such as those in which malware is used to steal customer credit card data, worry security professionals who don't want their organization to suffer the same fate. However, it's not clear that enough retailers have taken the message to heart. Retail leaders may believe that if they simply protect credit card data within their own firewalls, they're keeping information secure. But if they're transmitting that data unencrypted to banks and other partners, then protection within retailer networks doesn't matter much.

Perceptions of safety might be signs of overconfidence

Retailers have a somewhat rosy view of their security protections—a view that may not jibe with the number of breaches covered in the media on an almost daily basis. For example, 61 percent of the retail security professionals strongly agree they maintain full PCI compliance, and 63 percent strongly agree that confidential customer data stays secure throughout its lifecycle in the organization.

To focus on protecting data, retail organizations should fully adopt chip-and-PIN technology for customers paying with credit and debit cards—especially in the United States, where adoption has been slow. Now that banks and credit card providers are guaranteeing reimbursement for fraudulent charges only for purchases made with chip-and-PIN systems, retailers may need to step up adoption of this payment technology—or they'll be liable for those charges.[48]

Targeted attacks and insider exfiltration are biggest concerns

In keeping with concerns about revenue loss and brand damage, retail security professionals said targeted attacks (38 percent) and insider exfiltration (32 percent) pose the highest security risks to their organizations (Figure 64). They are right to be concerned: Often, attacks begin inside an organization. That means security built around examining indicators of compromise (IOCs) isn't enough. Organizations also need tools for reviewing indicators of attacks.

To detect sophisticated targeted attacks, like APTs or phishing attacks, retailers need to distinguish between normal and abnormal traffic patterns, which can vary by day, week, or shopping season.

Figure 64 Targeted attacks and insider exfiltration are biggest concerns

Source: Cisco 2017 Security Capabilities Benchmark Study

48 "New Credit Card Chips Shift Liability to Retailers," by Andrew Cohn, *Insurance Journal*, December 7, 2015: insurancejournal.com/news/national/2015/12/07/391102.htm.

Filling gaps in staffing

Retailers feel the pinch when it comes to building out their security resources—both in terms of people and tools. Twenty-four percent of the retail security professionals said they see a lack of trained personnel as a major obstacle to adopting advanced security processes and technology. In tandem with the lack of staff, retailers also see a steady stream of security alerts that they can't address in full: 45 percent see several thousand daily alerts, but only 53 percent of those are investigated. Twenty-seven percent of the alerts are deemed legitimate, and only 45 percent of legitimate alerts are remediated.

When staffing is an issue, automated security solutions become more important. Automation can help fill the gap caused by staffing shortfalls—for example, solutions that allow for the automatic segmentation of an infected device to a quarantined location. This way, the infection can't spread and the device will no longer have access to confidential information.

Automation can also help overcome the problem of distributed environments, a unique challenge in retail—such as reducing the number of security alerts that staff must respond to and mitigate. Physical locations (and therefore data) are geographically dispersed, so security leaders must assume (or hope) that these locations are adhering to security best practices in use at headquarters. Without constant communications with remote locations, stores could be operating security solutions that remain unpatched or outdated for years at a time.

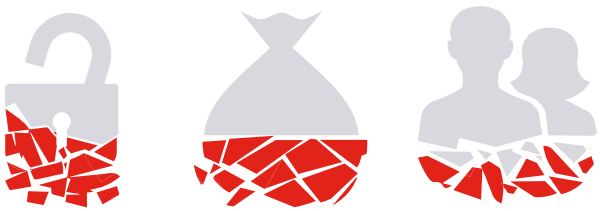
Retailers may be using outsourcing to close the staffing shortage gap, at least in part. Nearly half of retail security professionals said they outsource advice and consulting services at least partially; 45 percent said they outsource auditing to some extent. Of the retail organizations that outsource, about half cite cost efficiency, unbiased insight, and timely incident response as their top reasons for doing so.

Revenue and brand reputation suffer after public breaches

Retailers are aware that security breaches have a real-world impact on their businesses. In the past year, retail security professionals said that operations, finance, and brand reputation were the areas of their businesses most negatively impacted by security breaches. Fifty-four percent said they'd dealt with public scrutiny due to data breaches. In addition, 32 percent said they'd lost revenue due to attacks in the past year (see Figure 65). About one-fourth said they'd lost customers or business opportunities due to attacks.

Breaches may be the tipping point in terms of bringing about change in retail organizations' security posture. While only 29 percent said that public breaches drove improvements to a "great extent," nearly 90 percent said breaches drove improvements to at least a "modest extent."

Figure 65 Percentage of organizations that dealt with various consequences of data breaches



54%
dealt with public scrutiny due to data breaches

32%
lost revenue due to attacks in the past year

25%
lost customers or business opportunities due to attacks

Source: Cisco 2017 Security Capabilities Benchmark Study

Manufacturing

Key industry concerns

Eighty percent of U.S. factories are more than 20 years old,[49] which raises concerns as to whether they are equipped with updated defenses. Because machinery is often phased in over time, unlike office systems, unknown vulnerabilities may have been dormant for years—and are just now coming to life. As manufacturers add connected devices to these outdated machines, security professionals raise concerns that attackers may find the combination ripe for exploitation.

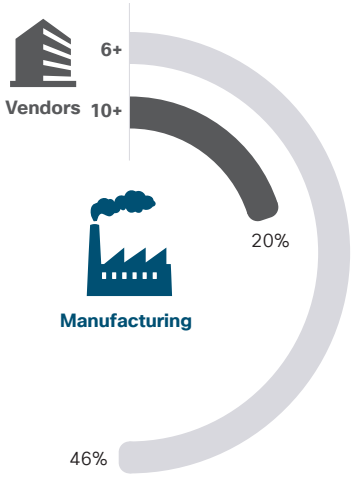
Vulnerable systems could lead to factory floor downtime, another key worry for automation professionals. Manufacturers want to avoid unplanned downtime at all costs, as well as product quality problems that could be caused by compromised machines not working properly.

For manufacturing security professionals, the challenge is upgrading aging systems to prevent easy intrusions by attackers, as well as integrating technologies like IIoT systems. The good news is that there are simple steps that manufacturers can take to improve security: The process should be viewed as a gradual one, rather than addressing all threats at once. For example, a written security policy can provide a framework for improvements, yet according to the Cisco survey, 40 percent of the manufacturing security professionals said they do not have a formal security strategy, nor do they follow standardized information security policy practices such as ISO 27001 or NIST 800-53. There's room for improvement by addressing these best practices.

The need for simpler systems

To get to the point where manufacturing systems are updated and integrated, manufacturers must resolve the security solution complexity problem. Forty-six percent of the manufacturing security professionals said they use six or more security vendors; 20 percent said they use more than 10 vendors (see Figure 66). Asked specifically about products, 63 percent of security professionals said they use six or more products, while 30 percent said they use more than 10 products.

Figure 66 Percentage of manufacturers that use solutions from 6 or more vendors



Source: Cisco 2017 Security Capabilities Benchmark Study

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

The multitude of products and vendors in manufacturing settings creates a confusing picture for security experts. The complexity speaks to the need for both IT and OT teams to narrow their focus on security threats—for example, using only those products than can address the most immediate concerns. Manufacturers could look toward implementing a defense-in-depth policy that includes simple protections for physical assets, such as blocking access to ports in unmanaged switches, or using managed switches in their plant network infrastructure.

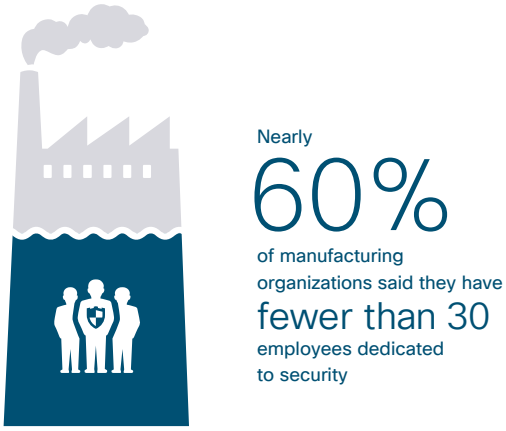
49 "America Is Aging in More Ways Than One," by Sho Chandra and Joran Yadoo, Bloomberg, October 6, 2016: bloomberg.com/news/articles/2016-10-06/america-is-aging-in-more-ways-than-one.

Combining the expertise of IT and OT teams

The composition of security teams may also be a hurdle to overcome in terms of protecting assets on the manufacturing floor. As experts with knowledge of manufacturing proprietary systems retire, they may not be replaced, causing a brain drain in terms of expertise. Nearly 60 percent of the manufacturing organizations said they have fewer than 30 employees dedicated to security (see Figure 67); in addition, 25 percent said that a lack of trained personnel is a major obstacle to adopting advanced security processes and technology.

In addition to beefing up security talent in-house, manufacturers also need their IT and OT departments to share knowledge. Traditionally, the involvement of IT ended at the factory floor edge, where OT would take over. Conflicts are common. For example, IT's patching processes might inadvertently shut down equipment running on older, proprietary networks, causing downtime and headaches for OT staff. Forward-looking manufacturers are working harder to combine IT and OT teams to foster greater understanding of security threats, as well as best practices for managing newer technologies such as IoT and connected devices.

Figure 67 Number of trained security personnel in manufacturing organizations



Source: Cisco 2017 Security Capabilities Benchmark Study

Avoiding breaches can improve competitive position

Given the aging systems in use in the industry, manufacturers are conscious of the need to improve and upgrade them not only for security reasons, but to boost their competitive advantage. According to a study by the Global Center for Digital Business Transformation,[50] four out of 10 manufacturers will suffer market disruption over the next 5 years, in part because they do not modernize to meet offerings from more advanced competitors. Security plays a key role in competitive advantage because it can help maintain brand reputation and avoid revenue and customer losses.

Public security breaches can negatively affect manufacturing brands, according to Cisco's survey findings. Forty percent of the manufacturing organizations reported having dealt with public scrutiny due to a data breach; in addition, 28 percent said they suffered loss of revenue due to attacks in the past year. However, these breaches may provide the incentive needed to improve security: 95 percent of the manufacturing security professionals said public breaches drove improvements to at least a modest extent.

50 "Life in the Digital Vortex: The State of Digital Disruption in 2017," Global Center for Digital Business Transformation: imd.org/dbt/digital-business-transformation.

Utilities

Key industry concerns

The 2016 takedown of Ukrainian power grids by Russian hackers highlighted the challenges faced by utilities in protecting critical infrastructure from attack.[51] Utilities no longer operate closed supervisory control and data acquisition (SCADA) networks; the same control center workstations that remotely monitor and control electricity generation, transmission, and distribution equipment are simultaneously connected to business networks and IT systems. These OT systems, which monitor and control physical processes, are being targeted because of their known cybersecurity weakness and the physical damage that can be caused by compromises.

In June 2017, researchers discovered that this attack used tools with a new level of sophistication. The attackers used specialized modules that utilized the control protocols directly. In prior attacks, remote manipulation of control tools was done manually. With these new extensions, attacks could be scheduled and run autonomously.

The pervasive connectivity and complexity of modern IT and OT systems, combined with security weaknesses in deployed OT firmware and software, increases the attack surface that needs to be protected. As utilities look to digitize their businesses, they are increasingly adopting newer software technologies that sense, monitor, and actuate physical processes without human intervention. This cyber-physical convergence—the integration of software and embedded systems into physical devices—is increasing the challenges faced by security professionals.

Security concerns around cyber-physical convergence extend to the supply chain. The Federal Energy Regulatory Commission (FERC) recently directed the North American Energy Reliability Corporation (NERC) to develop new standards for critical infrastructure protection, specifically directed at the utility supply chain. The standards are expected to address supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.[52]

Targeted attacks and APTs are key concern

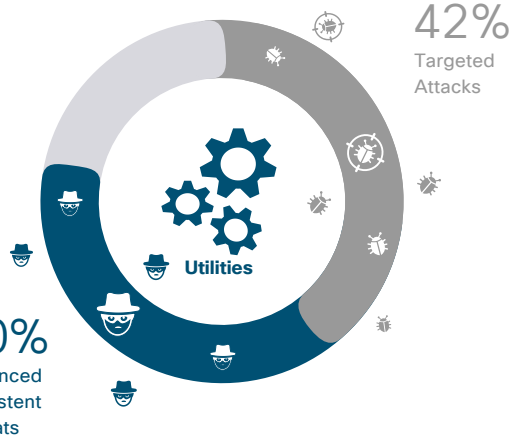
Targeted attacks are high on the list of worries for utility and energy security professionals. Security professionals said targeted attacks (42 percent) and advanced persistent threats, or APTs (40 percent) were the most critical security risks to their organizations (Figure 68). In addition, they cited mobile devices, user behavior, public cloud storage, and customer data as the top challenges to their defender strategies.

APTs are of concern because they have the potential to remain undetected in critical networks for longer periods of time, increasing the damage that attackers can cause. Because data networks are converging, and connected devices are increasing, the potential for harm—such as a utility shutdown—is greater than before.

Because of the high public profile of utilities, their security teams are acutely aware of threat technologies in the market, but they need guidance on the proper way to integrate such technologies to effectively protect against APTs and targeted attacks. They understand the "why" of security. What they need from security vendors is the "how"—that is, how to implement a layered approach to value-chain security that includes elements such as physical security and cybersecurity standards.

The complexity of their networks means utility and energy organizations must also assess the impact of threat alerts, and decide which ones deserve mitigation resources. Nearly half of the utility and energy security professionals said of the thousands of daily alerts they see, only 63 percent of those alerts are investigated. Of the alerts that are investigated, 41 percent are deemed legitimate threats, and 63 percent of those threats are remediated.

Figure 68 Targeted attacks and APTs are most critical concerns



Source: Cisco 2017 Security Capabilities Benchmark Study

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

51 "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," by Jamie Condliffe, MIT Technology Review, December 2, 2016: technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

52 "Revised Critical Infrastructure Protection Reliability Standards," U.S. Federal Energy Regulatory Commission: ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf.

Although this may seem as though only a fraction of legitimate alerts are investigated, the utility and energy industries show the highest rate of alert mitigation among the industries surveyed. In addition, an alert does not necessarily equal a threat. Security professionals may steer resources toward mitigating only those threats that could have a severe impact on network safety.

Strict budget controls can impact reliance on outsourcing

Because they are tightly regulated, utility and energy organizations can't add budget for security. Adding funds can require extensive and time-consuming approvals. This may explain the reliance on outsourced security, according to the survey. Over 60 percent of the utility security professionals said they outsource security advice and consulting services to some extent. In addition, nearly half said they outsource monitoring and threat intelligence services. Of those utilities that outsource security, over half of the security professionals named cost efficiency and unbiased insight as the top reasons to do so.

In keeping with the need to operate under strict regulatory control, utilities are likely to abide by formal security polices and standardized procedures. Nearly two-thirds of utility security professionals said they have written formal security strategies and follow standardized information security policy practices such as ISO 27001 or NIST 800-53.

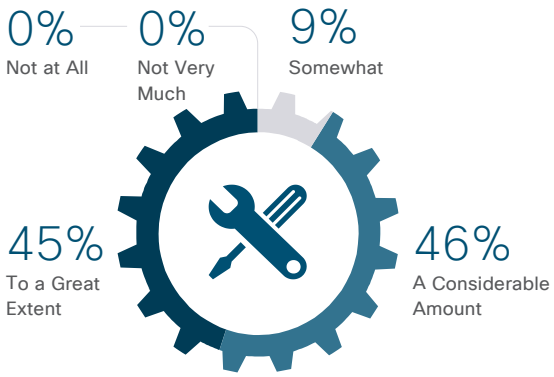
Public breaches drive improvements

When utilities suffer public breaches, awareness of these incidents is high. The public recognizes that utilities are part of the critical infrastructure, and that breaches put key services at risk. Sixty-one percent of the utilities reported that they have dealt with public scrutiny due to a data breach.

The good news is that such breaches may have triggered changes in security: 91 percent of the security professionals said the breaches drove improvements at least to a modest extent (see Figure 69). This may be an example of "making lemons into lemonade": A breach can offer useful insights into how attackers got into the networks, showing security professionals the chain of entry points—and therefore offering a roadmap of where to place security controls.

Attacks can also affect utility revenues and customer loyalty. Twenty-nine percent of the security professionals said their utilities lost revenue due to attacks in the past year, and 21 percent said they lost customers. Since many consumers can't comparison-shop for utility services because their regions may only offer one provider, the loss of customers (and therefore, the loss of revenue) is not as significant as in other industries where competition drives business decisions.

Figure 69 Percentage of security professionals who say breaches drove improvements



Source: Cisco 2017 Security Capabilities Benchmark Study

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Attack simulations and drills are commonplace

Utility security professionals indicate that they conduct frequent drills and simulations to detect weaknesses in their security infrastructure. Ninety-two percent said they conduct semiannual or annual drills or exercises to test incident response plans. When performing these drills, 84 percent of the organizations include their security partners.

In addition, 78 percent run attack simulations on their organizations at least once a quarter. In slightly less than half the organizations (45 percent), security professionals said attack simulations helped drive improvement to a great extent—for example, changes in security policies, procedures, and technologies. The high number of organizations conducting attack simulations may indicate that security professionals are using more automated tools, which allows them to accomplish simulations with less time and manpower.

Although utilities face some of the most complex cybersecurity challenges, they are also one of the most mature verticals regarding their cybersecurity methodologies, practices, and adoption of technology security controls. As threats evolve, so must critical infrastructure providers evolve to identify, protect, detect, respond, and recover from security incidents.

Healthcare

Key industry concerns

In healthcare, most decisions about security are driven by patient safety, outside of regulatory requirements and the protection of corporate assets. Leaders of healthcare organizations fear the attacks that could take down mission-critical equipment, endangering patients' lives. They're also concerned that security measures designed to monitor online traffic and detect threats can slow down the flow of data in critical systems, undermining medical professionals' ability to diagnose and treat patients. Beyond critical care, healthcare organizations also recognize that they must focus security systems on protecting private patient data—for example, as required in the United States by the Health Insurance Portability and Accountability Act (HIPAA).

As healthcare organizations bring more connectivity to their facilities and devices, security leaders are also raising concerns about the safety of converged networks. In the past, complex medical devices—such as the Picture Archiving Collection System (PACS), infusion pumps, and patient monitoring devices—typically arrived with data networks managed by vendors, so the devices were physically isolated from other networks. Today, with ample bandwidth available, healthcare organizations believe it's practical to simply flow data through one network, and use logical segmentation to separate various network traffic types such as clinical devices and administrative and guest wireless networks. However, if this segmentation is not done properly, the risks of attackers gaining access to critical data or devices increases.

Targeted attacks concern healthcare security teams

Ransomware attacks have already done damage to healthcare organizations. They're an attractive target for online criminals, since criminals know healthcare providers need to protect patient safety at all costs. In the Cisco study, 37 percent of the healthcare organizations said that targeted attacks are high-security risks to their organizations (see Figure 70). Targeted cyber attacks have also become more worrisome than breaches involving lost or stolen hardware, demanding a more precise approach to detecting and mitigating threats.

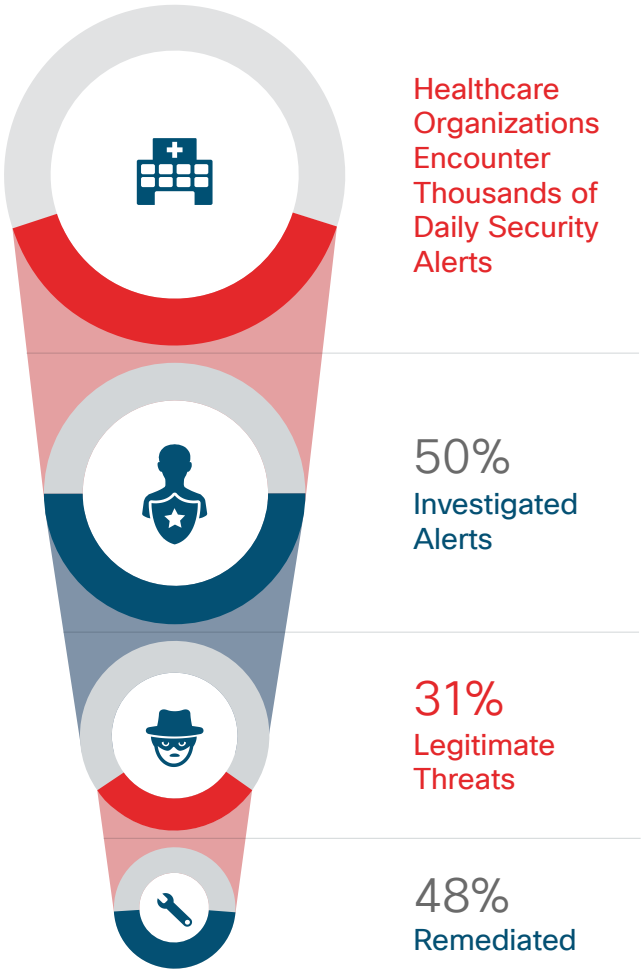
Figure 70 Targeted attacks are high security risk

Source: Cisco 2017 Security Capabilities Benchmark Study

Unfortunately, as is true in many industries, there are more threats than there are time and staff to investigate. Over 40 percent of the healthcare organizations said they come across thousands of security alerts daily, and only 50 percent of those are investigated (see Figure 71 on next page). Of the alerts that healthcare security teams investigate, 31 percent of those investigated are legitimate threats—but only 48 percent of those legitimate incidents are remediated.

According to Cisco security experts, it is likely that far fewer alerts are being investigated than healthcare security leaders may believe—or it's likely that by simply blocking threats from entering the network, they believe the threats have been remediated. It's also not surprising that these organizations can address so few of the alerts that raise red flags, since investigating a high number of alerts would cause security and IT activity to slow to a crawl and impact other business functions.

Figure 71 Thousands of alerts are encountered, but fewer than half are remediated



Source: Cisco 2017 Security Capabilities Benchmark Study

Management challenges: Lack of trained personnel, complexity of solutions

Many healthcare organizations respond to security challenges with a complex mix of solutions. Almost 60 percent said their organizations use solutions from more than six vendors, while 29 percent use solutions from more than 10 vendors. In addition, two-thirds of security professionals said they use six or more security products while 41 percent said they use more than 10 products.

The apparent profusion of vendors and products used by healthcare security professionals may result from confusion, or a lack of visibility, about exactly what tools are in place. As the Security Capabilities Benchmark Study showed in its overall findings, chief information security officers (CISOs) and security operations managers often have different perspectives on their security tools. Security executives higher up on the leadership ladder—that is, not on the front lines of day-to-day security management—may not have a deep understanding of all the tools on their networks.

Responding to day-to-day threats while managing a complex web of solutions is more challenging for healthcare organizations because of a lack of trained personnel. About half of the security professionals said they have fewer than 30 employees dedicated to security; 21 percent said they consider the lack of trained personnel to be a major obstacle in adopting advanced security processes and technology.

Large security teams are uncommon in all but the largest health organizations. According to Cisco healthcare industry experts, the definition of a security staffer can be fluid from organization to organization, which may affect perceptions about the size of the security team. For example, IT staff may be considered part of security team, or may join it on a temporary basis.

The value of segmenting traffic

The need for exceptions in healthcare, which allow certain systems or devices to adhere to different security protocols, ties back to concerns about patient well-being and safety. Healthcare devices are costly and are intended to remain in place for several years, so their software and operating systems are often not updated as frequently—hence the exceptions that allow them to operate reliably. The better approach, say security experts, is for healthcare organizations to isolate and segment traffic between the network and mission-critical devices. Alternately, organizations should improve their security infrastructure and network segmentation to better handle exceptions requiring compensating controls.

Healthcare organizations have an average of 34 significant security administrative exceptions in place; 47 percent of these exceptions also have compensating controls. Ideally, healthcare organizations should strive to have as few exceptions requiring compensating controls as possible, because they can create weaknesses in security defenses.

Transportation

Key industry concerns

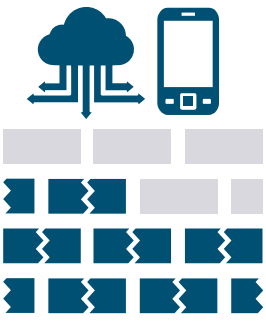
The transportation industry's technology infrastructure was traditionally built on closed, proprietary systems. The industry is on a journey to switch to modern connected networks, but security leaders fear the exposure to attackers during this transition period. Nevertheless, the change to connected IP systems must happen, due to the increasing maintenance cost and complexity of existing systems.

Additionally, consumers are demanding new safety and mobility services that cannot be met with the existing communications infrastructure. For example, customers want the ability to interact with airports, airlines, passenger and freight railroads, roadways, or connected vehicle fleets and transit authorities within social networks; buy tickets using mobile devices; or use mobility applications in their vehicles. Transportation organization workforces want the ease of use of connected systems as well—and as millennials move into these organizations, this demand will grow.

Advanced persistent threats and connected devices named top threats

As transportation organizations build complex and connected infrastructure—and see the impact of the growing network surface—different threats come to light. More than a third of transportation security professionals said that advanced persistent threats (APTs) and the proliferation of BYOD and smart devices were high security risks to their organizations. In addition, 59 percent of the security professionals said that cloud infrastructure and mobile devices are among the most challenging risks to defend against attacks (see Figure 72).

Figure 72 Cloud infrastructure and mobile devices are most challenging to defend



59%

of security professionals said that cloud infrastructure and mobile devices are among the most challenging to defend against attacks

Source: Cisco 2017 Security Capabilities Benchmark Study

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

To meet demands for information access, transportation security teams recognize that data must sit at the network edge, and be made available in real time. Controlling access to the data, and making sure it's available to those who need it, is a key concern for security practitioners.

They also recognize that this problem will only loom larger as they do away with closed, proprietary systems—and they expect to have to manage a higher number of more complex threats. Thirty-five percent of the transportation security professionals said they see thousands of daily alerts, of which only 44 percent are investigated. Of the alerts investigated, 19 percent are deemed legitimate threats—but only 33 percent of legitimate incidents are remediated.

Lack of security talent may drive outsourcing

Experienced security personnel can help transportation navigate through security challenges, but it's unclear if these organizations can attract the right talent. Over half of transportation security staffers said they have fewer than 30 employees dedicated to security. They recognize the impact of the dearth of expertise: 29 percent said they believe a lack of trained personnel is a major obstacle to adopting advanced security processes and technology.

As security operations capabilities become more sophisticated and specific, the likelihood of transportation organizations attracting this talent declines. Transportation authorities need to be able to recruit, compensate, and retain the type of high-caliber talent necessary to protect critical national and local infrastructure.

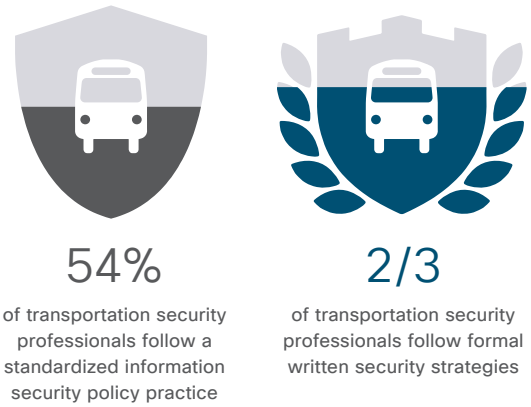
Without adequate in-house expertise, many transportation organizations call on outside help. Nearly half said they outsource some or all security tasks. Of the organizations that outsource, cost efficiency (52 percent) and unbiased insight (44 percent) were the top reasons for doing so.

Adherence to standardized information security practices, such as ISO 27001 or NIST 800-53, can help transportation organizations follow established benchmarks for security. Fifty-four percent of the transportation security professionals

follow a standardized information security policy practice, while two-thirds said they follow formal written security strategies (see Figure 73).

There are also signs that transportation organizations recognize the value of embedding security throughout the organization, not just simply buying point solutions. Seventy-five percent of the transportation organizations have a security operations center (SOC), and 14 percent said they plan to create an SOC. In addition, nearly 90 percent of the security professionals said their organizations participate in a security standards body or industry organization, such as PT-ISAC or ST-ISAC.

Figure 73 Percentage of transportation security professionals who follow standardized practices



Source: Cisco 2017 Security Capabilities Benchmark Study

Attack simulations lead to improvements

The fact that transportation, like other heavily regulated industries, is deemed to be critical infrastructure may drive decisions about security. For example, nearly 80 percent of the transportation security professionals run attack simulations in their organizations at least once every quarter. In addition, almost half said that the results of attack simulations drove significant improvements in security policies, procedures, and technologies.

Public data breaches can also drive change. Forty-eight percent of the transportation security professionals have dealt with public scrutiny due to a data breach. Although only 34 percent said that the breaches drove improvements to a "great extent," 83 percent said they drove improvements to at least a "modest extent."

Breaches can also have lasting impact in the industry beyond the mitigation efforts. Thirty-one percent of the security professionals said their organizations lost revenue due to attacks in the past year, with the average revenue loss at 9 percent. In addition, 22 percent said they lost customers and 27 percent said they lost opportunities due to attacks.

Finance

Key industry concerns

Financial services organizations are lucrative targets for online criminals. The wealth of customer financial data, plus access to account usernames and passwords, encourages criminals to launch an array of attacks on financial services businesses. In fact, some malware authors design their attacks specifically to compromise financial services networks. Examples are the Dridex credential-stealing malware[53] and the Zeus Trojan.[54]

In this environment, financial service security professionals recognize that their threat defenses should be effective against attackers using sophisticated malware. However, they also know they are hampered by a complicated mix of security vendors and products, which obfuscates threats instead of providing insight. Security teams also face the daunting task of integrating legacy applications with emerging technologies, while ensuring that no security gaps occur.

As some financial services organizations partner with fintech (financial technology) firms, they find the attack surface potentially expands and becomes more complex. How can these partnerships provide adequate protection of customer data? How do financial services organizations partner with outside firms while also meeting strict regulatory requirements? These questions factor into how the industry will approach its security challenges in the coming years.

Financial services organizations must also ensure they are "compliant" as well as "secure." In various heavily regulated industries, there's a tendency to believe that meeting compliance requirements will resolve security issues. Compliance requirements, such as network segmentation, certainly help protect data, but they are only part of the solution for stopping security breaches and providing threat analysis.

Multivendor environment adds confusion, not clarity

It's common for financial services organizations to have a multivendor environment. Fifty-seven percent of the financial services organizations said they use solutions from at least six vendors, while 29 percent use more than 10 vendors (see Figure 74). Two-thirds of the financial services organizations said they use at least six security products; 33 percent use more than 10 products.

Figure 74 Percentage of financial services organizations that use solutions from 6 or more vendors

Source: Cisco 2017 Security Capabilities Benchmark Study

Cisco security experts say that in this industry, it would be common to see products from as many as 30 vendors at a single organization. To respond to emerging threats rapidly and effectively, these organizations should focus on simplifying their security architectures: Fewer tools, more integration. Multiple products often operate in silos: Individually, they may be effective, but without integration to share and correlate security information, security teams will be left to manage conflicting alerts and reports.

The proliferation of products also hampers how security professionals can investigate threats. Forty-six percent of the financial services organizations said they see thousands of daily alerts, of which only 55 percent are investigated. Twenty-eight percent of the investigated threats are considered legitimate—yet only 43 percent of the legitimate threats are remediated.

The high number of alerts likely maps back to the problem of nonintegrated products from multiple vendors. Incident response teams may not know which alerts are duplicates, or which ones are low priority. Without integration, security teams are limited in their ability to correlate and analyze threats.

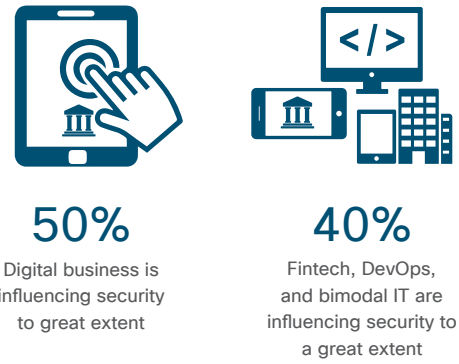
53 "Dridex Attacks Target Corporate Accounting," by Martin Nystrom, Cisco Security blog, March 4, 2015: blogs.cisco.com/security/dridex-attacks-target-corporate-accounting.
54 "Zeus Trojan Analysis," by Alex Kirk, Cisco Talos Blog: talosintelligence.com/zeus_trojan.

Digital business may drive improvements

As financial services organizations continue to partner with fintech companies, they will explore new strategies to improve security—such as formalizing responsibilities for securing data. Nearly half of the financial services organizations said that digital business is influencing security to great extent. Also, about 40 percent said that fintech, DevOps, and bimodal IT are influencing security to a great extent (see Figure 75).

For example, a financial services company working with a fintech partner must establish how customer data will remain protected, particularly in a cloud environment. The partners would also need to determine joint processes to avoid security incidents; and if one occurs, how both parties will respond.

Figure 75 Impact of digital business on security



Source: Cisco 2017 Securities Capabilities Benchmark Study

Download the 2017 graphics at: **cisco.com/go/mcr2017graphics**

Standards adoption should pick up speed

If financial services organizations are to securely meet customer demands in the digital world, they will need to speed up adoption efforts for new policies and processes. To date, 63 percent of financial organizations have written formal security strategies. Only 48 percent follow a standardized information security policy practice, such as ISO 27001 or NIST 800-53. Financial services is a conservative industry, and security and IT leaders move slowly when considering new standards and their fit for the current security strategy.

Another area where financial services organizations could use improvement: Asking vendors to adhere to established business practices. For example, only 37 percent said they require vendors to employ ISO 27001 so they can work with their organizations.

According to Cisco security experts, the security maturity level of an organization may dictate how stringent vendors' requirements are: Large, established financial services organizations may be better equipped to vet vendors in this fashion than smaller businesses.

Conclusion

Conclusion

Cisco has been publishing annual and midyear cybersecurity reports for nearly a decade. The primary goal of every one of these reports is to keep security teams and the businesses they support apprised of known and emerging threats and vulnerabilities—and informed about the steps they can take to make their organizations more secure and cyber resilient.

The diversity of content that our threat researchers and technology partners have presented in this latest report reflects the complexity of the modern threat landscape. Much of the research also shows that defenders not only have been gaining ground on adversaries, but also developing a much better understanding of how and where threat actors operate.

However, we expect that defenders will struggle to maintain ground as the IoT expands. As discussed in the introduction to this report, there are signs that new types of attacks—more sinister and destructive than campaigns of the past—are in development. Adversaries are devising high-impact, well-planned attacks that are designed to prevent any organization, big or small, from operating. They know that no business has a contingency plan that outlines how to rebuild all their IT or OT from scratch, and they are determined to use that weakness to their advantage.

That is why it has never been more important for organizations to make cybersecurity a top priority. They must invest in automated tools that can help security teams stay on top of alerts, gain visibility into and manage their dynamic networks, and detect and respond swiftly to true threats. And they must devote the time and resources to ensure they always know exactly what is in their IT environment, and that everything within it is deployed correctly and securely and kept up to date.

The security community, meanwhile, needs to expand its thinking and dialogue about how to create an open ecosystem that will allow customers to implement security solutions that will work best for their organization and make the most of existing investments. In this ecosystem, all security solutions can communicate with each other, and work together to protect users and businesses. A unified effort from defenders is needed to meet the challenge of potent threats meant to disrupt the IoT world and inflict devastating impact on the organizations operating within it.

Security leaders: It's time to claim a seat at the top table

Cisco's latest Security Capabilities Benchmark Study found that security is a high priority for the top levels of many organizations. Also, security professionals believe that executive teams keep security high on the list of key organizational goals. However, the number of security professionals who strongly agreed that their executive leadership considers security a high priority was 59 percent in 2016—down slightly from 61 percent in 2015 and 63 percent in 2014.

That decline in confidence may be misplaced, however. Chief information security officers (CISOs), in particular, may not realize that senior management and boards of directors not only view cybersecurity as a high priority for the business, but also are eager to hear more about the issue. In fact, they are likely looking for better and more information.

According to the National Association of Corporate Directors' (NACD) 2016-2017 Public Company Governance Survey,[55] almost one-quarter of boards are dissatisfied with the reporting that management delivers on cybersecurity. They report that the information they receive does not allow for effective benchmarking, is not transparent about problems, and is difficult to interpret. In the same report, only 14 percent of the respondents felt that their board has a high level of understanding about cyber risks.

Security experts with SAINT Corporation, a security solutions company and Cisco partner, suggest that CISOs have a clear opportunity to help fill that knowledge gap. However, they must:

- Strive to provide information in a way that will be meaningful and actionable for the business. Reports about the organization's cyber risks or security needs should not be overly technical. Try to align the discussion about these issues with traditional risks that the company faces, and tie them to business priorities and desired outcomes. Also, be sure to emphasize how cybersecurity can be a growth enabler and competitive differentiator for the business.
- When alerting management and the board to a cyber attack, explain in clear terms what the impact is to the organization (for example, how many employees or customers are affected, what high-value information has been compromised), what measures the security team is taking to contain and investigate the threat, and how long it will take to resume normal operations.
- Seek to engage other leaders in the organization, including those outside of the technology department. By collaborating regularly with a range of leaders in the organization—the chief information officer, chief technology officer, chief audit executive, and the chief risk officer, to name a few—CISOs can gain a direct line to senior management and the board. This will also provide a better opportunity to secure a seat at the "top table" to discuss cybersecurity strategy and help develop a comprehensive security program for the organization.

CISOs often struggle to secure funding for security initiatives. But here again, they may not realize that now may be the ideal time to discuss budgets with leadership. The 2017 IT Trends Study from the Society for Information Management (SIM) reports that cybersecurity is the third largest area of investment for organizations today.[56] In 2013, it ranked 14th. Respondents to the SIM survey (IT leaders) also ranked cybersecurity second among areas of IT that should receive more investment, and first on the list of information technologies that they find "most personally worrisome."[57]

55 Data, information and content sourced directly from, and with permission from, the National Association of Corporate Directors' 2016-2017 Public Company Governance Survey. The survey is available for download from the NACD at nacdonline.org/Resources/publicsurvey.cfm?ItemNumber=36843.

56 Society for Information Management IT Trends Study, Kappelman, L. A., et al. (2017). This study is available for download from SIM at simnet.org/members/group_content_view.asp?group=140286&id=442564.

57 Ibid.

About Cisco

About Cisco

Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced-threat protection portfolios of solutions across the broadest set of attack vectors. Cisco's threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection before, during, and after an attack.

Threat researchers from the Cisco Collective Security Intelligence (CSI) ecosystem bring together, under a single umbrella, the industry's leading threat intelligence, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open-source community. This amounts to a daily ingest of billions of web requests and millions of emails, malware samples, and network intrusions.

Our sophisticated infrastructure and systems consume this telemetry, helping machine-learning systems and researchers to track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, email, and from the cloud to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our products and services offerings that are immediately delivered globally to Cisco customers.

To learn more about Cisco's threat-centric approach to security, visit cisco.com/go/security.

Cisco 2017 Midyear Cybersecurity Report contributors

Cisco Cloudlock

Cisco Cloudlock provides cloud access security broker (CASB) solutions that help organizations securely use the cloud. It delivers visibility and control for software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) environments across users, data, and applications. It also provides actionable cybersecurity intelligence through its data scientist-led CyberLab and crowd-sourced security analytics.

Cisco Computer Security Incident Response Team (CSIRT)

Cisco CSIRT forms part of the investigative branch of Cisco's Corporate Security Programs Office. It provides Cisco with tailored security monitoring services in order to protect Cisco from cyber attacks and the loss of its intellectual assets, and serves as Cisco's internal cyber investigations and forensics team. The primary mission of CSIRT is to help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents, and to contribute to the prevention of such incidents by engaging in proactive threat assessment, mitigation planning, incident trend analysis, and security architecture review.

Cisco Security Incident Response Services (CSIRS)

The Cisco Security Incident Response Services (CSIRS) team is made up of world-class incident responders who are tasked with assisting Cisco's customers before, during, and after they experience an incident. CSIRS leverages best-in-class personnel, enterprise-grade security solutions, cutting-edge response techniques, and best practices learned from years of combating adversaries to ensure our customers are able to more proactively defend against, as well as quickly respond to and recover from, any attack.

Cognitive Threat Analytics

Cisco's Cognitive Threat Analytics is a cloud-based service that discovers breaches, malware operating inside protected networks, and other security threats by means of statistical analysis of network traffic data. It addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection. Cognitive Threat Analytics relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees, and adapt over time.

Commercial West Sales

The Commercial West Sales organization is focused on elevating the conversations around security with Cisco customers, holding SAFE workshops for customers, and advising customers' security leadership on how to better protect their organizations and reduce overall risk.

Global Government Affairs

Cisco engages with governments at many different levels to help shape public policy and regulations that support the technology sector and help governments meet their goals. The Global Government Affairs team develops and influences pro-technology public policies and regulations. Working collaboratively with industry stakeholders and association partners, the team builds relationships with government leaders to influence policies that affect Cisco's business and overall ICT adoption, looking to help shape policy decisions at a global, national, and local level. The Government Affairs team is composed of former elected officials, parliamentarians, regulators, senior U.S. government officials, and government affairs professionals who help Cisco promote and protect the use of technology around the world.

Global Industrial Marketing

Cisco's Global Industrial Marketing team is focused on the manufacturing, utility, and oil and gas industries. The team is responsible for shaping industry-specific global thought leadership with industry-differentiated value proposition messaging, solutions, and go-to-market campaigns to help customers digitally transform their businesses. The team also collaborates with customers, peers, account teams, analysts, press, and other external and internal audiences, and utilizes real-time analytics to lead Cisco industry-specific strategy, go-to-market strategy, plans, and targeted messaging.

IPTG Connected Car

The IPTG Connected Car team is focused on helping automotive original equipment manufacturers (OEMs) connect, converge, secure, and digitize their in-vehicle networks to IP.

IoT

The Security Technology Group develops tools, processes, and content to identify and mitigate threats in connected environments.

Portfolio Solutions Marketing Team

The Portfolio Solutions Marketing Team focuses on creating and delivering security messaging and content that presents and advocates the Cisco Security portfolio as an integrated, end-to-end security solution.

U.S. Public Sector Organization

Cisco's U.S. Public Sector Organization transforms how Cisco customers protect, serve and educate the people of the United States. Focused on the federal government, state and local government, and education markets, we connect people and technology, and we innovate in all facets of our work—from customer satisfaction to operational excellence and mission success. We lead our customers by understanding their business challenges, by tailoring solutions to their unique needs, by building relationships, by simplifying technology, and by delivering profound impact on their mission in the United States and across the globe.

Security Business Group Technical Marketing

The Security Business Group's Technical Marketing team provides deep technical and industry subject-matter expertise to all of Cisco's security product management decisions. As a highly experienced team of technical experts, the team supports numerous Cisco teams in engineering, marketing, sales and services, solving and explaining the most sophisticated and complex technology challenges that help secure Cisco's customers. Highly sought-after for their knowledge, team members contribute to numerous publications and speaking engagements.

Security Research and Operations (SR&O)

Security Research and Operations (SR&O) is responsible for threat and vulnerability management of all Cisco products and services, including the industry-leading Product Security Incident Response Team (PSIRT). SR&O helps customers understand the evolving threat landscape at events such as Cisco Live and Black Hat, as well as through collaboration with its peers across Cisco and the industry. Additionally, SR&O delivers new services such as Cisco's Custom Threat Intelligence (CTI), which can identify indicators of compromise that have not been detected or mitigated by existing security infrastructures.

Security and Trust Organization

Cisco's Security and Trust Organization underscores Cisco's commitment to address two of the most critical issues that are top of mind for boardrooms and world leaders alike. The organization's core missions include protecting Cisco's public and private customers, enabling and ensuring Cisco Secure Development Lifecycle and Trustworthy Systems efforts across Cisco's product and service portfolio, and protecting the Cisco enterprise from ever-evolving threats. Cisco takes a holistic approach to pervasive security and trust, which includes people, policies, processes, and technology. The Security and Trust Organization drives operational excellence, focusing across InfoSec, Trustworthy Engineering, Data Protection and Privacy, Cloud Security, Transparency and Validation, and Advanced Security Research and Government. For more information, visit trust.cisco.com.

Talos Security Intelligence and Research Group

Talos is Cisco's threat intelligence organization, an elite group of security experts devoted to providing superior protection for Cisco customers, products, and services. Talos is composed of leading threat researchers supported by sophisticated systems to create threat intelligence for Cisco products that detect, analyze, and protect against known and emerging threats. Talos maintains the official rule sets of Snort.org, ClamAV, and SpamCop, and is the primary team that contributes threat information to the Cisco CSI ecosystem.

Cisco 2017 Midyear Cybersecurity Report technology partners

ANOMALI™

The Anomali suite of threat intelligence solutions empowers organizations to detect, investigate, and respond to active cybersecurity threats. The award-winning ThreatStream threat intelligence platform aggregates and optimizes millions of threat indicators, creating a "cyber no-fly list." Anomali integrates with internal infrastructure to identify new attacks, searches forensically over the past year to discover existing breaches, and enables security teams to quickly understand and contain threats. Anomali also offers STAXX, a free tool to collect and share threat intelligence, and provides a free, out of the box intelligence feed, Anomali Limo. To learn more, visit anomali.com and follow us on Twitter: @anomali.

FLASHPOINT

Flashpoint delivers Business Risk Intelligence (BRI) to empower business units and functions across organizations to make better decisions and mitigate risk. The company's unique Deep & Dark Web data, expertise, and technology enable customers to glean intelligence that informs risk and protects their ability to operate. For more information, visit flashpoint-intel.com.

LUMETA
DETECT WITH A HIGHER SENSE

Lumeta provides critical cyber-situational awareness that helps security and network teams prevent breaches. Lumeta offers unmatched discovery of known, unknown, shadow, and rogue network infrastructure, as well as real-time network and endpoint monitoring and segmentation analytics for dynamic network elements, endpoints, virtual machines, and cloud-based infrastructure. For more information, visit lumeta.com.

QUALYS®
CONTINUOUS SECURITY

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand, and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations worldwide. For more information, visit qualys.com.

radware
Every second counts

Radware (NASDAQ: RDWR) is a global leader of application delivery and cybersecurity solutions for virtual, cloud, and software-defined data centers. Its award-winning solutions portfolio delivers service-level assurance for more than 10,000 enterprise and carriers worldwide. For additional expert security resources and information, visit Radware's online security center, which offers a comprehensive analysis of DDoS attack tools, trends, and threats: security.radware.com.

Rapid7 (NASDAQ: RPD) is trusted by IT and security professionals around the world to manage risk, simplify modern IT complexity, and drive innovation. Rapid7 analytics transform today's vast amounts of security and IT data into the answers needed to securely develop and operate sophisticated IT networks and applications. Rapid7 research, technology, and services drive vulnerability management, penetration testing, application security, incident detection and response, and log management for more than 6300 organizations across more than 120 countries, including 39 percent of the Fortune 1000. For more information, visit rapid7.com.

RSA's business-driven security solutions help customers comprehensively and rapidly link security incidents with business context to respond effectively and protect what matters most. With award-winning solutions for rapid detection and response, identity and access assurance, consumer fraud protection, and business risk management, RSA customers can thrive in an uncertain, high-risk world. For more information, visit rsa.com.

SAINT Corporation, a leader in next-generation, integrated vulnerability management solutions, helps corporations and public sector institutions pinpoint risk exposures at all levels of the organization. SAINT does it right so access, security, and privacy can coexist to the benefit of all. And SAINT enables clients to strengthen InfoSec defenses while lowering total cost of ownership. For more information, visit saintcorporation.com.

ThreatConnect® arms organizations with a powerful defense against cyber threats and the confidence to make strategic business decisions. Built on the industry's only intelligence-driven, extensible security platform, ThreatConnect provides a suite of products designed to meet the threat intelligence aggregation, analysis and automation needs of security teams at any maturity level. More than 1600 companies and agencies worldwide deploy the ThreatConnect platform to fully integrate their security technologies, teams, and processes with actionable threat intelligence resulting in reduced detection to response time and enhanced asset protection. For more information, visit threatconnect.com.

TrapX Security provides an automated security grid for adaptive deception and defense that intercepts real-time threats while providing the actionable intelligence to block attackers. TrapX DeceptionGrid™ allows enterprises to detect, capture, and analyze zero-day malware in use by the world's most effective advanced persistent threat (APT) organizations. Industries rely on TrapX to strengthen their IT ecosystems and reduce the risk of costly and disruptive compromises, data breaches, and compliance violations. TrapX defenses are embedded at the heart of the network and mission-critical infrastructure, without the need for agents or configuration. Cutting-edge malware detection, threat intelligence, forensics analysis, and remediation in a single platform help remove complexity and cost. For more information, visit trapx.com.

Download the graphics

All the graphics in this report are downloadable at: cisco.com/go/mcr2017graphics.

Updates and corrections

To see updates and corrections to the information in this project, visit cisco.com/go/errata.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published July 2017