Cisco 2018
Annual Cybersecurity Report

Table of contents

Executive summary

What if defenders could see the future? If they knew an attack was coming, they could stop it, or at least mitigate its impact and help ensure what they need to protect most is safe. The fact is, defenders *can* see what's on the horizon. Many clues are out there—and obvious.

Adversaries and nation-state actors already have the expertise and tools necessary to take down critical infrastructure and systems and cripple entire regions. But when news surfaces about disruptive and destructive cyber attacks—such as those in Ukraine, for example, or elsewhere in the world—some security professionals might initially think, "Our company's market/region/technology environment wasn't a target, so, we're probably not at risk."

However, by dismissing what seem like distant campaigns, or allowing the chaos of daily skirmishes with attackers to consume their attention, defenders fail to recognize the speed and scale at which adversaries are amassing and refining their cyber weaponry.

For years, Cisco has been warning defenders about escalating cybercriminal activity around the globe. In this, our latest annual cybersecurity report, we present data and analysis from Cisco threat researchers and several of our technology partners about attacker behavior observed over the past 12 to 18 months. Many of the topics examined in the report align with three general themes:

1. **Adversaries are taking malware to unprecedented levels of sophistication and impact.**

   The evolution of malware (page 6) was one of the most significant developments in the attack landscape in 2017. The advent of network-based ransomware cryptoworms eliminates the need for the human element in launching ransomware campaigns. And for some adversaries, the prize isn't ransom, but obliteration of systems and data, as Nyetya—wiper malware masquerading as ransomware—proved (see page 6). Self-propagating malware is dangerous and has the potential to take down the Internet, according to Cisco threat researchers.

2. **Adversaries are becoming more adept at evasion—and weaponizing cloud services and other technology used for legitimate purposes.**

   In addition to developing threats that can **elude increasingly sophisticated sandboxing environments** (page 22), malicious actors are widening their **embrace of encryption to evade detection** (page 9). Encryption is meant to enhance security, but it also provides malicious actors with a powerful tool to conceal command-and-control (C2) activity, affording them more time to operate and inflict damage.

   Cybercriminals are also adopting **C2 channels that rely on legitimate Internet services** like Google, Dropbox, and GitHub (see page 24). The practice makes malware traffic almost impossible to identify.

   Also, many attackers are now **launching multiple campaigns from a single domain** (page 26) to get the best return on their investments. They are also reusing infrastructure resources, such as registrant email addresses, autonomous system numbers (ASNs), and nameservers.

3. **Adversaries are exploiting undefended gaps in security, many of which stem from the expanding Internet of Things (IoT) and use of cloud services.**

   Defenders are deploying IoT devices at a rapid pace but often pay scant attention to the security of these systems. **Unpatched and unmonitored IoT devices** present attackers with opportunities to infiltrate networks (page 34). Organizations with IoT devices susceptible to attack also seem **unmotivated to speed remediation**, research suggests (page 42). Worse, these organizations probably have many more vulnerable IoT devices in their IT environments that they don't even know about.

Meanwhile, **IoT botnets are expanding** along with the IoT and becoming more mature and automated. As they grow, attackers are using them to launch more advanced distributed-denial-of-service (DDoS) attacks (page 31).

Attackers are also taking advantage of the fact that security teams are **having difficulty defending both IoT and cloud environments**. One reason is the lack of clarity around who exactly is responsible for protecting those environments (see page 42).

Recommendations for defenders

When adversaries inevitably strike their organizations, will defenders be prepared, and how quickly can they recover? Findings from the **Cisco 2018 Security Capabilities Benchmark Study**—which offers insights on security practices from more than 3600 respondents across 26 countries—show that defenders have a lot of challenges to overcome (see page 46).

Even so, defenders will find that making strategic security improvements and adhering to common best practices can reduce exposure to emerging risks, slow attackers' progress, and provide more visibility into the threat landscape. They should consider:

- Implementing first-line-of-defense tools that can scale, like cloud security platforms.
- Confirming that they adhere to corporate policies and practices for application, system, and appliance patching.
- Employing network segmentation to help reduce outbreak exposures.
- Adopting next-generation endpoint process monitoring tools.
- Accessing timely, accurate threat intelligence data and processes that allow for that data to be incorporated into security monitoring and eventing.
- Performing deeper and more advanced analytics.
- Reviewing and practicing security response procedures.
- Backing up data often and testing restoration procedures—processes that are critical in a world of fast-moving, network-based ransomware worms and destructive cyber weapons.
- Reviewing third-party efficacy testing of security technologies to help reduce the risk of supply chain attacks.
- Conducting security scanning of microservice, cloud service, and application administration systems.
- Reviewing security systems and exploring the use of SSL analytics—and, if possible, SSL decryption.

Defenders should also consider adopting advanced security technologies that include machine learning and artificial intelligence capabilities. With malware hiding its communication inside of encrypted web traffic, and rogue insiders sending sensitive data through corporate cloud systems, security teams need effective tools to prevent or detect the use of encryption for concealing malicious activity.

About the report

The ***Cisco 2018 Annual Cybersecurity Report*** presents our latest security industry advances designed to help organizations and users defend against attacks. We also look at the techniques and strategies that adversaries use to break through those defenses and evade detection.

The report also highlights major findings from the **Cisco 2018 Security Capabilities Benchmark Study**, which examines the security posture of enterprises and their perceptions of their preparedness to defend against attacks.

Part I:
The attack landscape

Part I: The attack landscape

Adversaries are taking malware to unprecedented levels of sophistication and impact. The growing number and variety of malware types and families perpetuate chaos in the attack landscape by undermining defenders' efforts to gain and hold ground on threats.

THE EVOLUTION OF MALWARE

One of the most important developments in the attack landscape in 2017 was the evolution of ransomware. The advent of network-based ransomware worms eliminates the need for the human element in launching ransomware campaigns. And for some adversaries, the prize isn't ransom, but the destruction of systems and data. We expect to see more of this activity in the year ahead.

They're out there: Defenders should prepare to face new, self-propagating, network-based threats in 2018

In 2017, adversaries took ransomware to a new level—although it had been expected. After the SamSam campaign of March 2016[1]—the first large-scale attack that used the network vector to spread ransomware, thereby removing the user from the infection process—Cisco threat researchers knew it would only be a matter of time before threat actors found a way to automate this technique. Attackers would make their malware even more potent by combining it with "worm-like" functionality to cause widespread damage.

This malware evolution was swift. In May 2017, WannaCry—a ransomware cryptoworm—emerged and spread like wildfire across the Internet.[2] To propagate, it took advantage of a Microsoft Windows security vulnerability called EternalBlue, which was leaked by the hacker group Shadow Brokers in mid-April 2017.

WannaCry had earned more than US$143,000 through bitcoin payments at the point the wallets were cashed out. Given the timeline, and calculating accrual of the value on the bitcoin originally paid into the wallets at $93,531, Cisco threat researchers estimate that roughly 312 ransom payments were made. As a comparison, the exploit kit Angler, when it was active, was earning about $100 million per year as a global business.

WannaCry did not track encrypted damage to and the payments made by affected users. The number of users who received decryption keys after making a payment is also unknown. (WannaCry is still propagating, and users continue to pay ransoms—in vain.) Due to the very low performance of WannaCry as ransomware, the U.S. government and many security researchers believe the ransom component is effectively a smokescreen to conceal WannaCry's true purpose: wiping data.

Nyetya (also known as NotPetya) arrived in June 2017.[3] This wiper malware also masqueraded as ransomware and it too used the remote code execution vulnerability nicknamed "EternalBlue," as well as the remote code execution vulnerability "EternalRomance" (also leaked by Shadow Brokers), and other vectors involving credential harvesting

1 *SamSam: The Doctor Will See You, After He Pays the Ransom,* Cisco Talos blog, March 2016: blog.talosintelligence.com/2016/03/samsam-ransomware.html.
2 *Player 3 Has Entered the Game: Say Hello to 'WannaCry,'* Cisco Talos blog, May 2017: blog.talosintelligence.com/2017/05/wannacry.html.
3 *New Ransomware Variant 'Nyetya' Compromises Systems Worldwide,* Cisco Talos blog, June 2017: blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html.

unrelated to the Shadow Brokers release.[4] Nyetya was deployed through software update systems for a tax software package used by more than 80 percent of companies in the Ukraine, and installed on more than 1 million computers.[5] Ukraine cyber police confirmed that it affected more than 2000 Ukrainian companies.[6]

Before the rise of self-propagating ransomware, malware was distributed in three ways: drive-by download, email, or physical media such as malicious USB memory devices. All methods required some type of human interaction to infect a device or system with ransomware. With these new vectors being employed by attackers, an active and unpatched workstation is all that is needed to launch a network-based ransomware campaign.

Security professionals may see worms as an "old" type of threat because the number of worm-like Common Vulnerabilities and Exposures (CVEs) has declined as product security baselines have improved. However, self-propagating malware not only is a relevant threat, but also has the potential to bring down the Internet, according to Cisco threat researchers. WannaCry and Nyetya are only a taste of what's to come, so defenders should prepare.

WannaCry and Nyetya could have been prevented, or their impact muted, if more organizations had applied basic security best practices such as patching vulnerabilities, establishing appropriate processes and policies for incident response, and employing network segmentation.

For more tips on meeting the threat of automated network-based ransomware worms, read *Back to Basics: Worm Defense in the Ransomware Age* on the Cisco Talos blog.

Security weak spot: the supply chain

The Nyetya campaign was also a supply chain attack, one of many that Cisco threat researchers observed in 2017. One reason Nyetya was successful at infecting so many machines so quickly is that users did not see an automated software update as a security risk, or in some cases even realize that they were receiving the malicious updates.

Another supply chain attack, which occurred in September 2017, involved the download servers used by a software vendor to distribute a legitimate software package known as CCleaner.[7] CCleaner's binaries, which contained a Trojan backdoor, were signed using a valid certificate, giving users false confidence that the software they were using was secure. The actors behind this campaign were targeting major technology companies where the software was in use, either legitimately or as part of shadow IT.

Supply chain attacks appear to be increasing in velocity and complexity. They can impact computers on a massive scale, and can persist for months or even years. Defenders should be aware of the potential risk of using software or hardware from organizations that do not have a responsible security posture. Look for vendors that issue CVEs, are quick to address vulnerabilities, and consistently strive to ensure that their build systems can't be compromised. Also, users should take time to scan new software before downloading it to verify that it doesn't contain malware.

Network segmentation of software that is not backed by a comprehensive security practice can help contain damage from supply chain attacks, preventing them from spreading throughout an organization.

4 Ibid.
5 *Ukraine scrambles to contain new cyber threat after 'NotPetya' attack,* by Jack Stubbs and Matthias Williams, Reuters, July 2017: reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P.
6 *The MeDoc Connection,* Cisco Talos blog, July 2017: blog.talosintelligence.com/2017/07/the-medoc-connection.html.
7 *CCleaner Command and Control Causes Concern,* Cisco Talos blog, September 2017: blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html.

Why integrity in threat intelligence reporting matters

All organizations that share threat information to customers or the public through any channel should employ guidelines that help them ensure accuracy in their reporting. Even if all the facts aren't clear, organizations can still communicate what they know—and avoid guessing. Being right is better than being first.

For example, when the WannaCry attack unfolded in May 2017, there was initial confusion within the security community about how the ransomware worm was infiltrating systems. Multiple organizations in both the public and private sector were reporting that the attack stemmed from a phishing campaign and malicious email attachment. But the network-based threat was, in fact, scanning for and infecting vulnerable, public-facing Microsoft Windows Server Message Block (SMB) Server ports.

Cisco threat researchers quickly alerted the security community that the emails they thought were connected to the WannaCry campaign were likely spam emails from the Necurs bot that were spreading "Jaff" ransomware. It was several days before the security community was in agreement that the suspicious emails contained Jaff—not WannaCry. And during that time, users were acting on information that could not help them to avoid the fast-moving WannaCry campaign.

The chaos following the advent of the WannaCry campaign serves as a reminder that the security community must avoid communicating inaccurate facts about the origin and nature of cyber attacks. In the early hours of a campaign, the sense of urgency to quickly stop adversaries and protect users can easily result in the publishing—especially on social media—of information that may create confusion and prevent users from defending their systems.

For more on this topic, read the post *On Conveying Doubt* on the Cisco Talos blog.

ENCRYPTED MALICIOUS WEB TRAFFIC

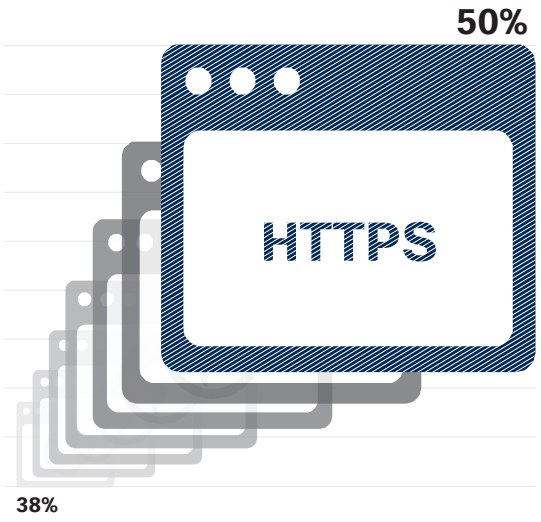
The expanding volume of encrypted web traffic—both legitimate and malicious—creates even more challenges and confusion for defenders trying to identify and monitor potential threats. Encryption is meant to enhance security, but it also provides malicious actors with a powerful tool to conceal command-and-control (C2) activity, affording them more time to operate and inflict damage. Cisco threat researchers expect to see adversaries increase their use of encryption in 2018. To keep pace, defenders will need to incorporate more automation and advanced tools like machine learning and artificial intelligence to complement threat prevention, detection, and remediation.

A dark spot for defenders: encrypted malicious web traffic

Cisco threat researchers report that 50 percent of global web traffic was encrypted as of October 2017. That is a 12-point increase in volume from November 2016 (see Figure 1). One factor driving that increase is the availability of low-cost or free SSL certificates. Another is Google Chrome's stepped-up practice of flagging unencrypted websites that handle sensitive information, like customers' credit card information, as "non-secure." Businesses are motivated to comply with Google's HTTPS encryption requirement unless they want to risk a potentially significant drop in their Google search page rankings.

As the volume of encrypted global web traffic grows, adversaries appear to be widening their embrace of encryption as a tool for concealing their C2 activity. Cisco threat researchers observed a more than threefold increase in encrypted network communication used by inspected malware samples over a 12-month period (see Figure 2). Our analysis of more than 400,000 malicious binaries found that about 70 percent had used at least some encryption as of October 2017.

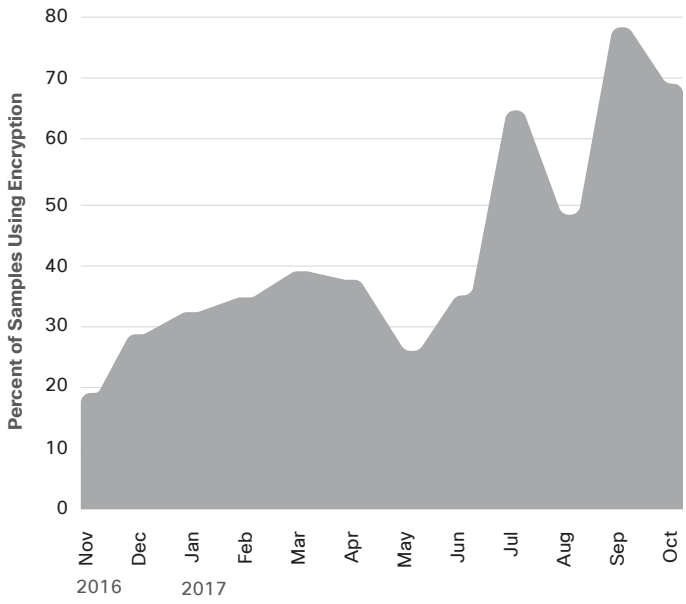
Figure 1 Increase in volume of encrypted global web traffic



12-Point Increase in Global Web Traffic from November 2016–October 2017

Source: Cisco Security Research

Figure 2 Increase in volume of malicious binaries leveraging some encrypted network communication



Source: Cisco Security Research

Download the 2018 graphics at: cisco.com/go/acr2018graphics

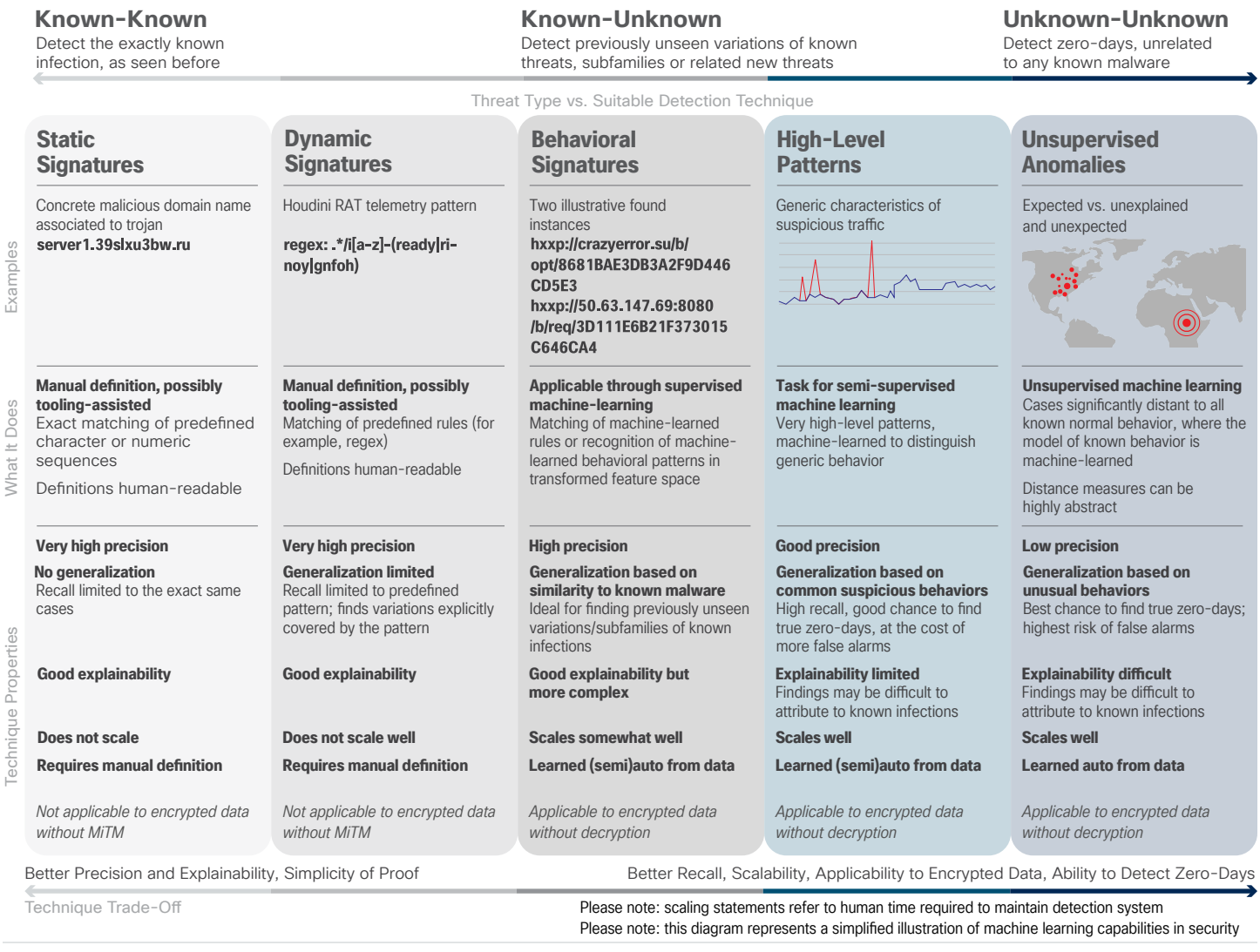
Applying machine learning to the threat spectrum

To overcome the lack of visibility that encryption creates, and reduce adversaries' time to operate, we see more enterprises exploring the use of machine learning and artificial intelligence. These advanced capabilities can enhance network security defenses and, over time, "learn" how to automatically detect unusual patterns in web traffic that might indicate malicious activity.

Machine learning is useful for automatically detecting "known-known" threats—the types of infections that have been seen before (see Figure 3). But its real value, especially in monitoring encrypted web traffic, stems from its ability to detect "known-unknown" threats (previously unseen variations of known threats, malware subfamilies, or related new threats) and "unknown-unknown" (net-new malware) threats. The technology can learn to identify unusual patterns in large volumes of encrypted web traffic and automatically alert security teams to the need for further investigation.

That latter point is especially important, given that the lack of trained personnel is an obstacle to enhancing security defenses in many organizations, as seen in findings from the Cisco 2018 Security Capabilities Benchmark Study (see page 35). Automation and intelligent tools like machine learning and artificial intelligence can help defenders overcome skills and resource gaps, making them more effective at identifying and responding to both known and emerging threats.

Figure 3 Machine learning in network security: taxonomy



Source: Cisco Security Research

Download the 2018 graphics at: cisco.com/go/acr2018graphics

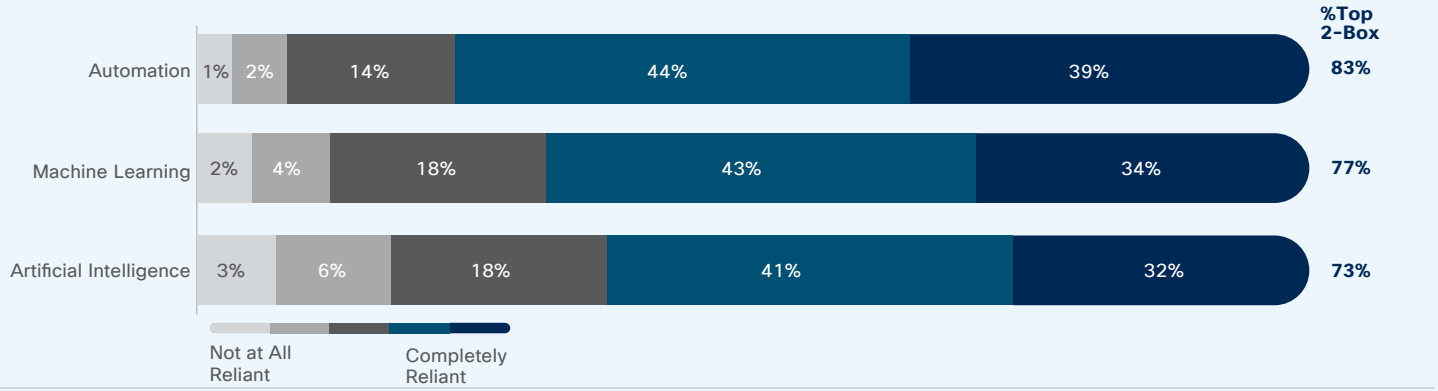
Cisco 2018 Security Capabilities Benchmark Study: Defenders report greater reliance on automation and artificial intelligence

Chief information security officers (CISOs) interviewed for the Cisco 2018 Security Capabilities Benchmark Study report that they are eager to add tools that use artificial intelligence and machine learning, and believe their security infrastructure is growing in sophistication and intelligence. However, they are also frustrated by the number of false positives such systems generate, since false positives increase the security team's workload. These concerns should ease over time as machine learning and artificial intelligence technologies mature and learn what is "normal" activity in the network environments they are monitoring.

When asked which automated technologies their organizations rely on the most, 39 percent of security professionals said they are completely reliant on automation, while 34 percent are completely reliant on machine learning; 32 percent said they are completely reliant on artificial intelligence (Figure 4).

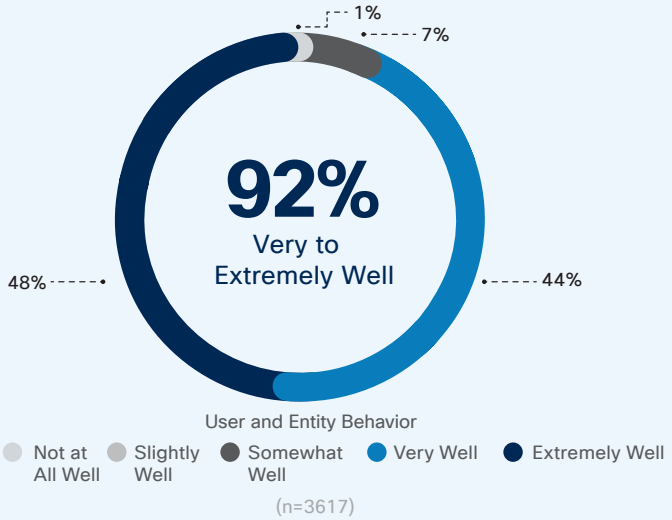
Behavior analytics tools are also considered useful when locating malicious actors in networks; 92 percent of security professionals said these tools work very to extremely well (Figure 5).

Figure 4 Organizations rely heavily on automation, machine learning, and artificial intelligence



Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 5 Most security professionals see value in behavioral analytics tools



Extremely Well
69%

2/3 of Healthcare Organizations Believe That Behavioral Analytics/Forensics Help Identify Malicious Actors

(n=358)

Extremely Well
38-39%

Fewer in Transportation and Government Agree That Behavioral Analytics/Forensics Work Extremely Well

(Transportation: n=175; Government: n=639)

Source: Cisco 2018 Security Capabilities Benchmark Study

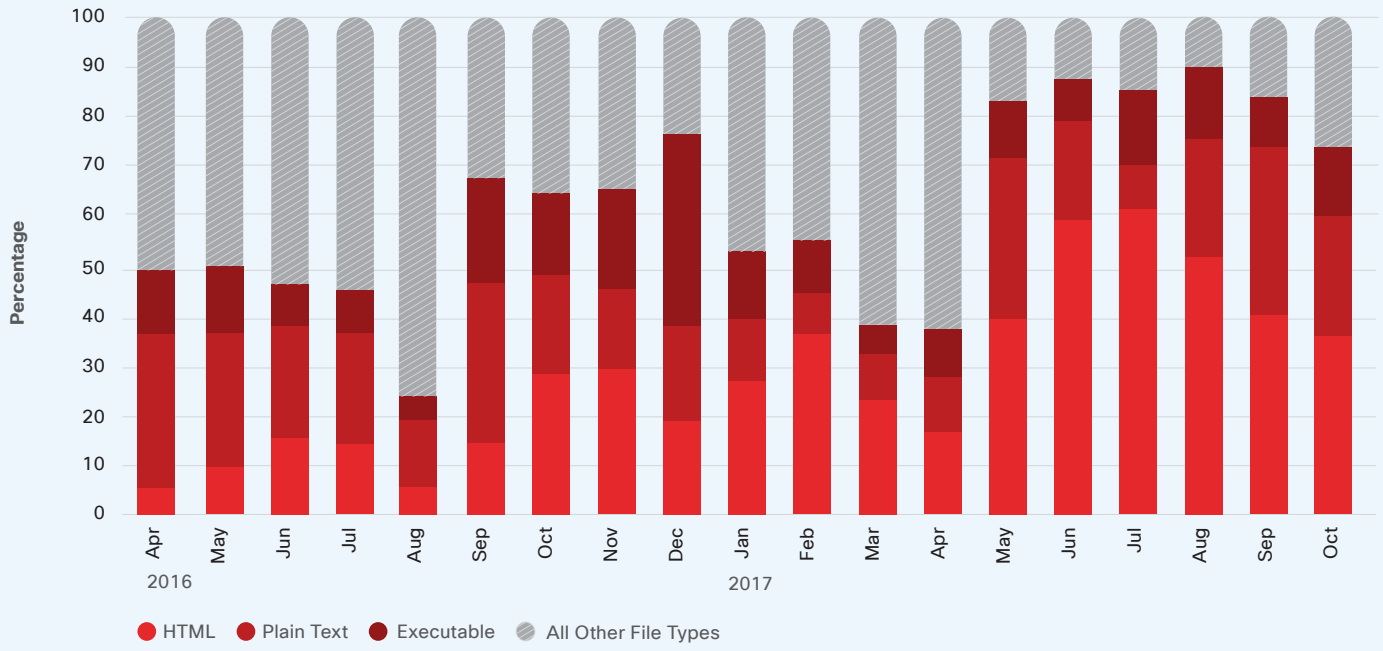
Download the 2018 graphics at: cisco.com/go/acr2018graphics

Web attack methods show adversaries' intense focus on browser compromise

An analysis of web attack methods over an 18-month period from April 2016 to October 2017 shows an increase in adversaries' use of malicious web content (Figure 6). That trend aligns with the aggressive targeting of the Microsoft Internet Explorer web browser by still-active exploit kits.

Cisco threat researchers observed that the number of detections of malicious JavaScript web content was significant and consistent during this period. That underscores the effectiveness of this strategy for infecting vulnerable browsers to facilitate other nefarious activity such as browser redirection or Trojan downloads.

Figure 6 Malware-based block activity by content type, April 2016 – October 2017

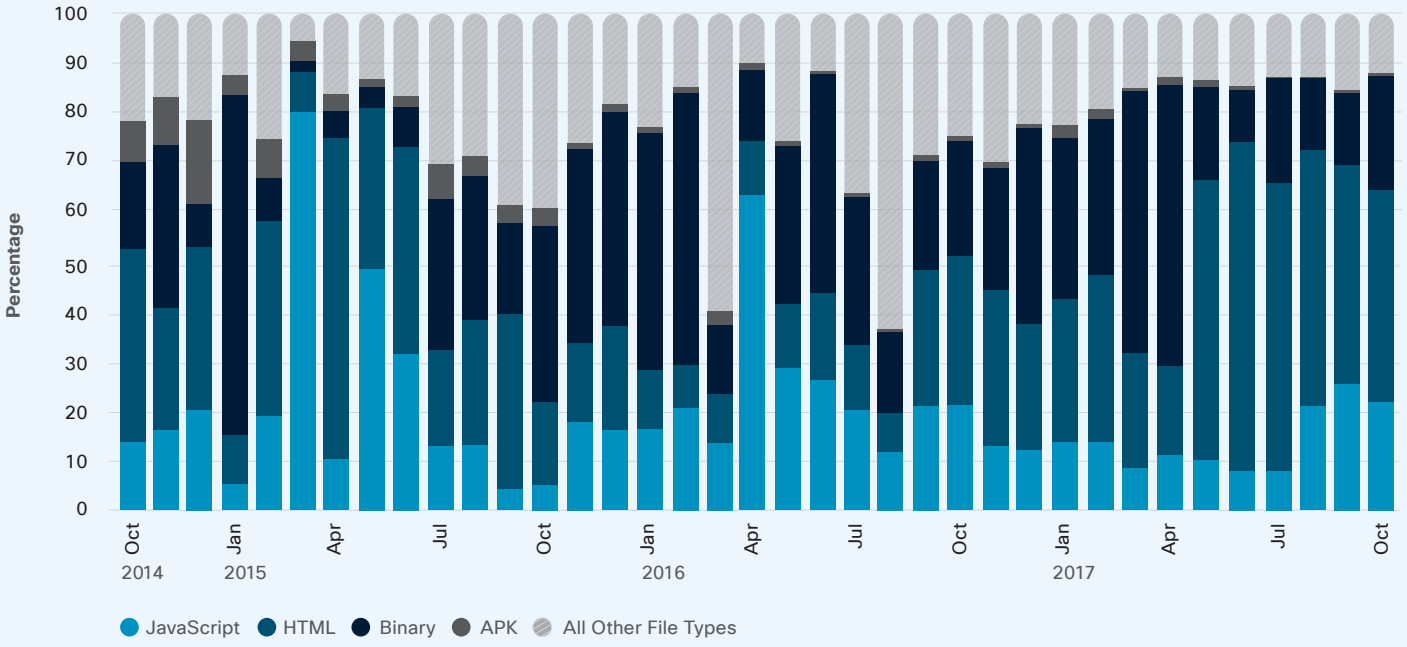


Source: Cisco Security Research

Figure 7 is an overview of web attack methods over a three-year period, from October 2014 to October 2017. Adversaries consistently employed suspicious binaries during this period, primarily to deliver adware and spyware. As discussed in the *Cisco 2017 Midyear Cybersecurity Report*, these types of potentially unwanted applications (PUAs) can present security risks, such as increased malware infections and theft of user or company information.[8]

The three-year view in Figure 7 also shows that the volume of malicious web content fluctuates over time as attackers launch and end campaigns and change their tactics to evade detection.

Figure 7 Malware-based block activity by content type, October 2014 – October 2017



Source: Cisco Security Research

Download the 2018 graphics at: cisco.com/go/acr2018graphics

8 *Cisco 2017 Midyear Cybersecurity Report*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

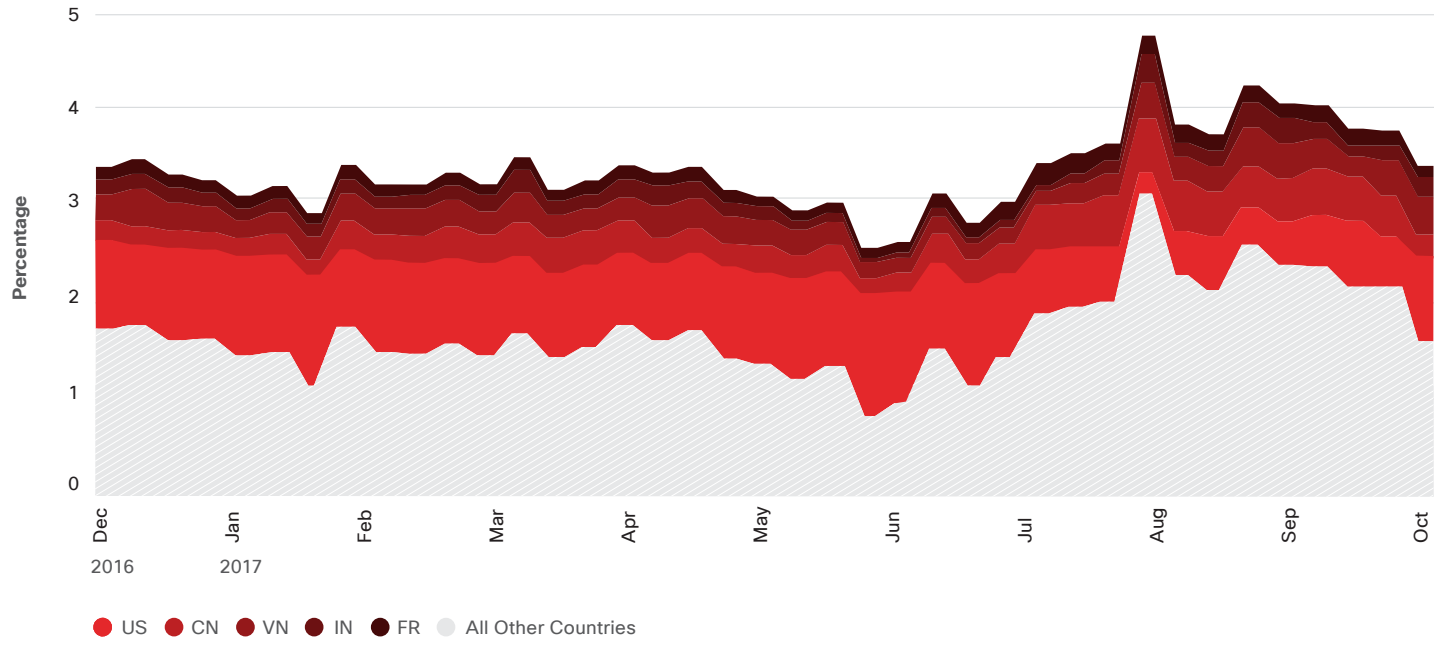
EMAIL THREATS

No matter how much the threat landscape changes, malicious email and spam remain vital tools for adversaries to distribute malware because they take threats straight to the endpoint. By applying the right mix of social engineering techniques, such as phishing and malicious links and attachments, adversaries need only to sit back and wait for unsuspecting users to activate their exploits.

Fluctuations in spam botnet activity impact overall volume

In late 2016, Cisco threat researchers observed a noticeable increase in spam campaign activity that appeared to coincide with a decline in exploit kit activity. When leading exploit kits like Angler abruptly disappeared from the market, many users of those kits turned—or returned—to the email vector to maintain profitability.[9] However, after that initial rush back to email, global spam volume declined and leveled during most of the first half of 2017. Then, in late May and early June 2017, global spam volume dipped before spiking considerably during mid- to late summer (see Figure 8).

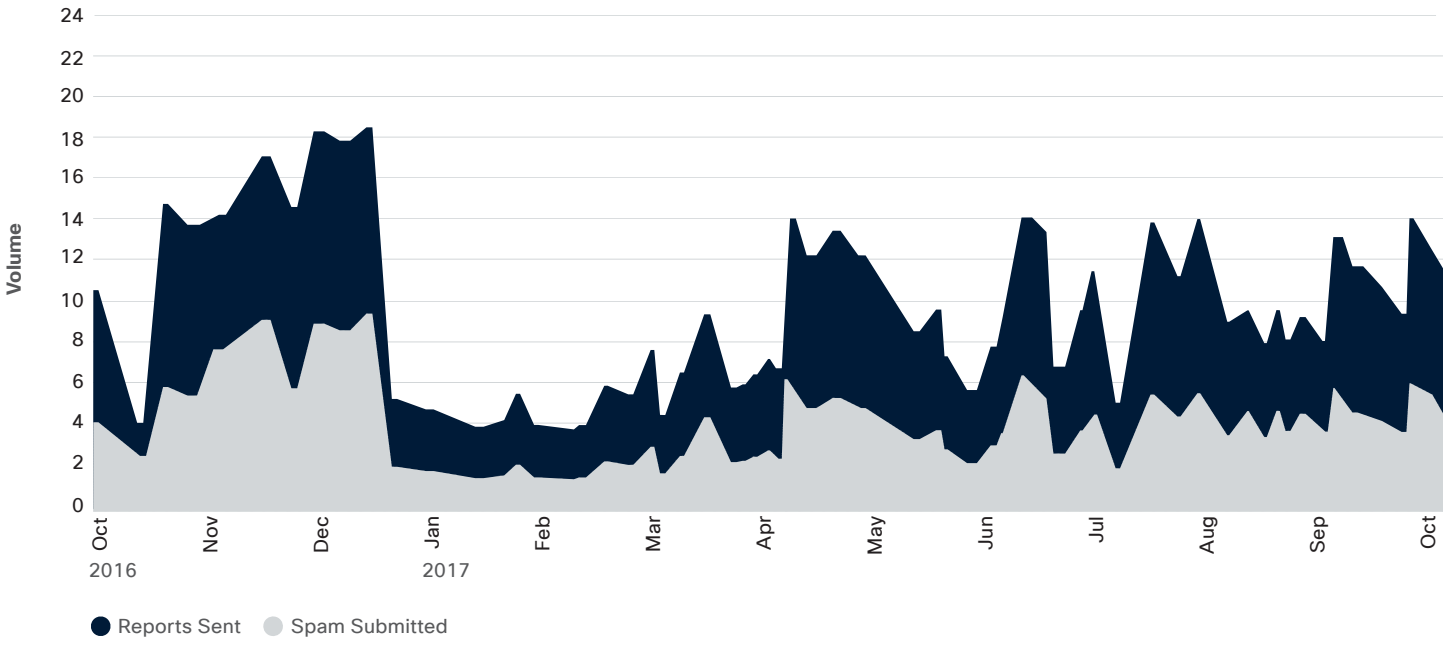
Figure 8 IP reputation blocks by country, December 2016 – October 2017



Source: Cisco Security Research

9 See "Decline in exploit kit activity likely influencing global spam trends," p. 18, *Cisco 2017 Midyear Cybersecurity Report*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Figure 9 Spam botnet activity, October 2016 – October 2017



Source: Cisco SpamCop

Download the 2018 graphics at: cisco.com/go/acr2018graphics

The reduced spam volume from January through April 2017 coincides with a lull in spam botnet activity, as an internal graph generated by the Cisco® SpamCop service shows (Figure 9).

Cisco threat researchers report that the Necurs botnet, a major contributor to overall spam volume globally, was active but distributing less spam during the January to April time frame. In May, the botnet was spreading Jaff ransomware through massive spam campaigns. The campaigns featured a PDF file with an embedded malicious Microsoft Office document, and the initial downloader for the Jaff ransomware.[10] Security researchers discovered a vulnerability in Jaff that allowed them to create a decryptor that forced Necurs' operators to make a quick return to distributing its usual threat, Locky ransomware.[11] The time that the actors behind Necurs needed to pivot back to Locky coincides with the significant dip in global spam volume observed during the first two weeks of June (Figure 9).

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

11 *Player 1 Limps Back Into the Ring—Hello Again, Locky!* by Alex Chiu, Warren Mercer, and Jaeson Schultz, with contributions from Sean Baird and Matthew Molyett, Cisco Talos blog, June 2017: blog.talosintelligence.com/2017/06/necurs-locky-campaign.html.

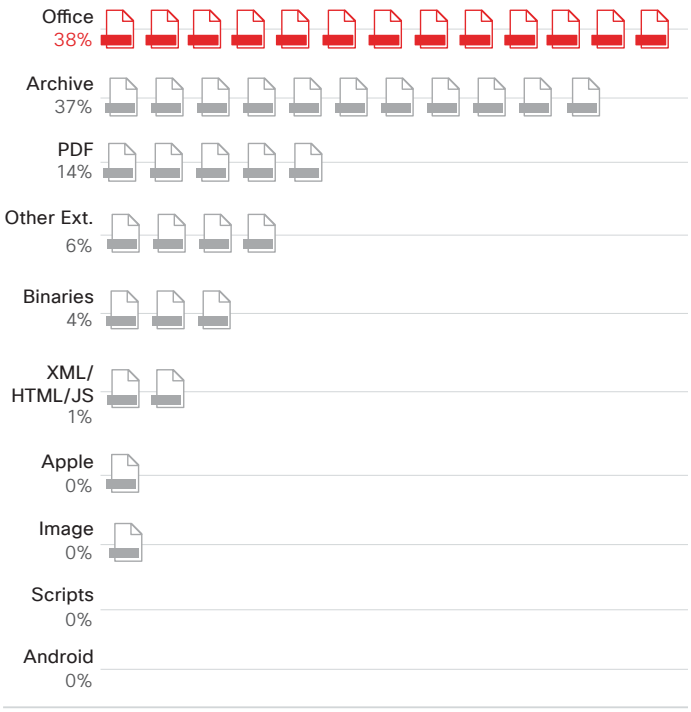
Malicious file extensions in email: common malware families' top 10 tools

Cisco threat researchers analyzed email telemetry from January through September 2017 to identify the types of malicious file extensions in email documents that common malware families employed most often. The analysis yielded a top 10 list that shows the most prevalent group of malicious file extensions (38 percent) was Microsoft Office formats such as Word, PowerPoint, and Excel (see Figure 10).

Archive files, such as .zip and .jar, accounted for about 37 percent of all the malicious file extensions observed in our study. That adversaries heavily employ archive files is not surprising, as they have long been favored hiding places for malware. Users must open archive files to see the contents—an important step in the infection chain for many threats. Malicious archive files also often find success in foiling automated analysis tools, especially when they contain threats that require user interaction for activation. Adversaries will also use obscure file types, such as .7z and .rar, to evade detection.

Malicious PDF file extensions rounded out the top three in our analysis, accounting for nearly 14 percent of malicious file extensions observed. (Note: The category of "Other Extensions" applies to extensions observed in our study that could not be mapped easily to known file types. Some malware types are known to use random file extensions.)

Figure 10 Top 10 malicious file extensions, January – September 2017

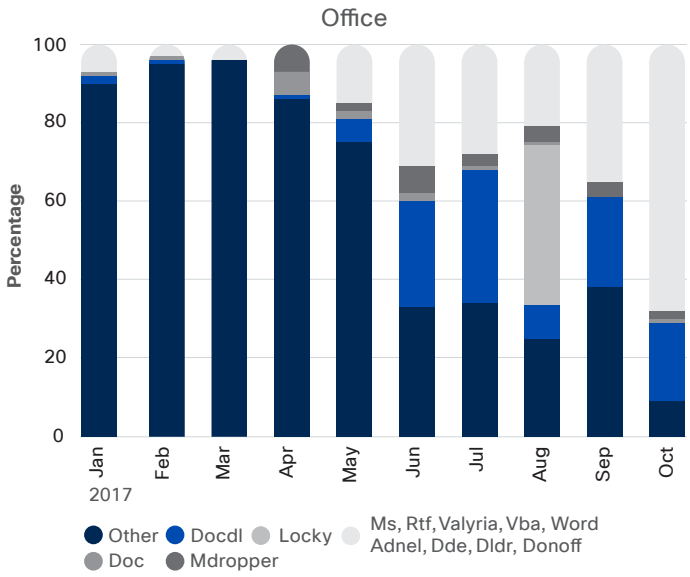


Source: Cisco Security Research

Figures 11a-c provide an overview of the malware families included in our investigation that were associated with the top three malicious file extension types: MS Office files, archives, and PDFs. Figure 12 shows the percentage of detections, by family, that included a malicious payload file extension. The spikes in activity align with spam campaigns observed during those months, according to Cisco threat researchers.

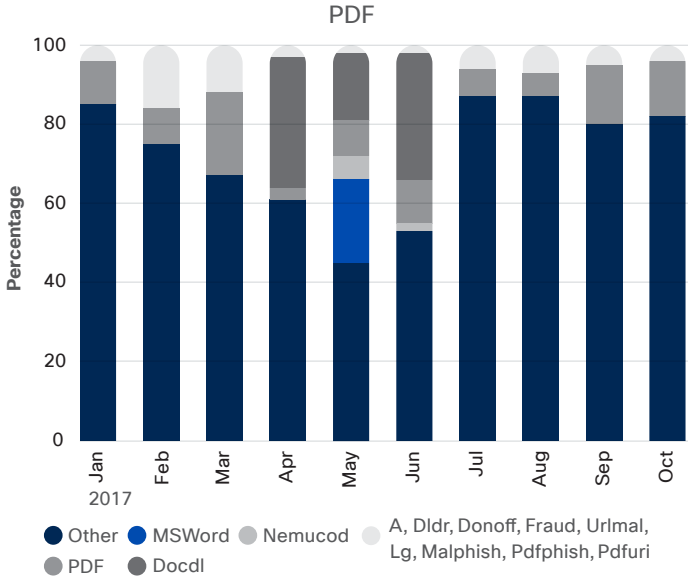
For example, in late summer, there were major campaigns underway distributing Nemucod and Locky—two threats that often work together. Nemucod is known to send malicious payloads in archive files like .zip that contain malicious script but look like normal .doc files. ("Dwnldr," also seen in Figure 12, is a likely variant of Nemucod.)

Figure 11a Top three malicious file extension types and malware family relationships



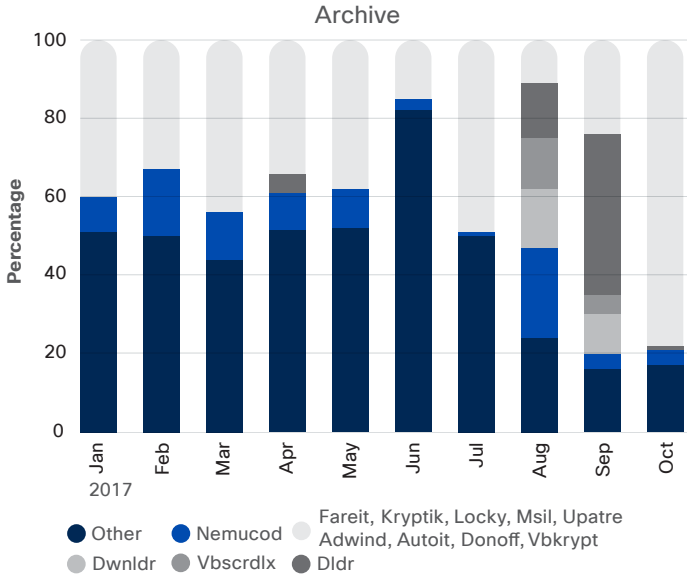
Source: Cisco Security Research

Figure 11b Top three malicious file extension types and malware family relationships



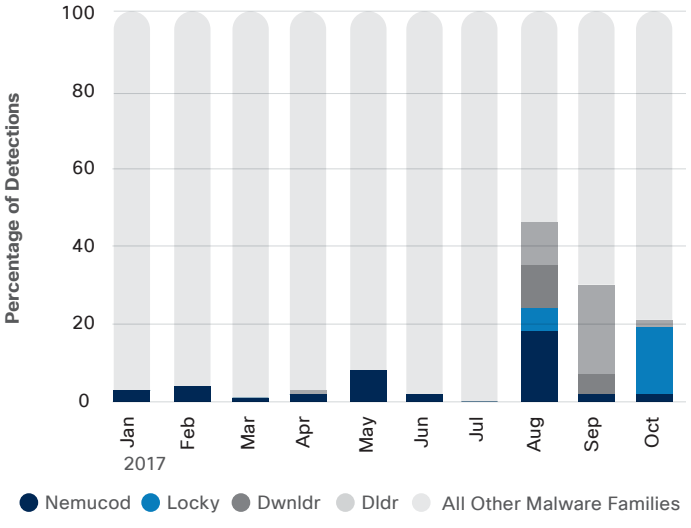
Source: Cisco Security Research

Figure 11c Top three malicious file extension types and malware family relationships



Source: Cisco Security Research

Figure 12 Patterns of top malware families, January - October 2017



Source: Cisco Security Research

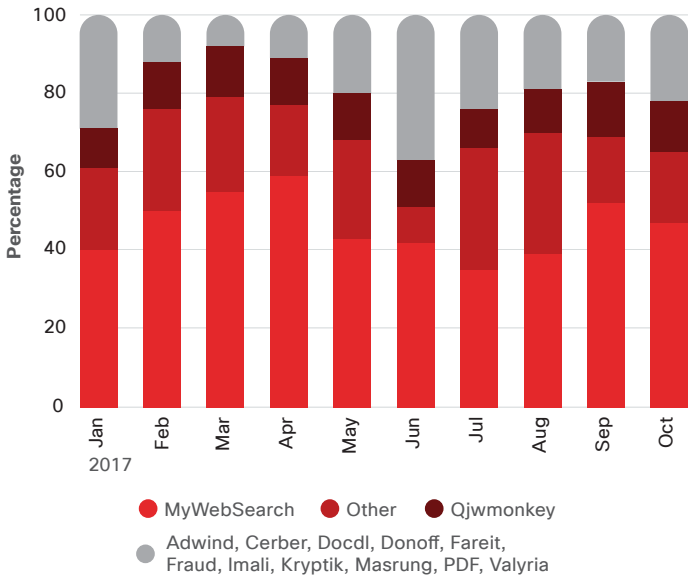
MyWebSearch spyware most active user of "other extensions"

The "other extensions" group in our study includes several well-known malware types. But MyWebSearch, a malicious adware software and browser hijacker that poses as a helpful toolbar, is the most active player (see Figure 13). It uses .exe file extensions exclusively, sometimes only one type per month. The potentially unwanted application (PUA) has been around for years and infects different browser types. It is often bundled with fraudulent software programs and can expose users to malvertising.

Our analysis of malicious file extension types shows that even in today's sophisticated and complex threat environment, email remains a vital channel for malware distribution. For enterprises, baseline defense strategies include:

- Implementing powerful and comprehensive email security defenses.
- Educating users about the threat of malicious attachments and links in phishing emails and spam.

Figure 13 MyWebSearch most active user of "other extensions"



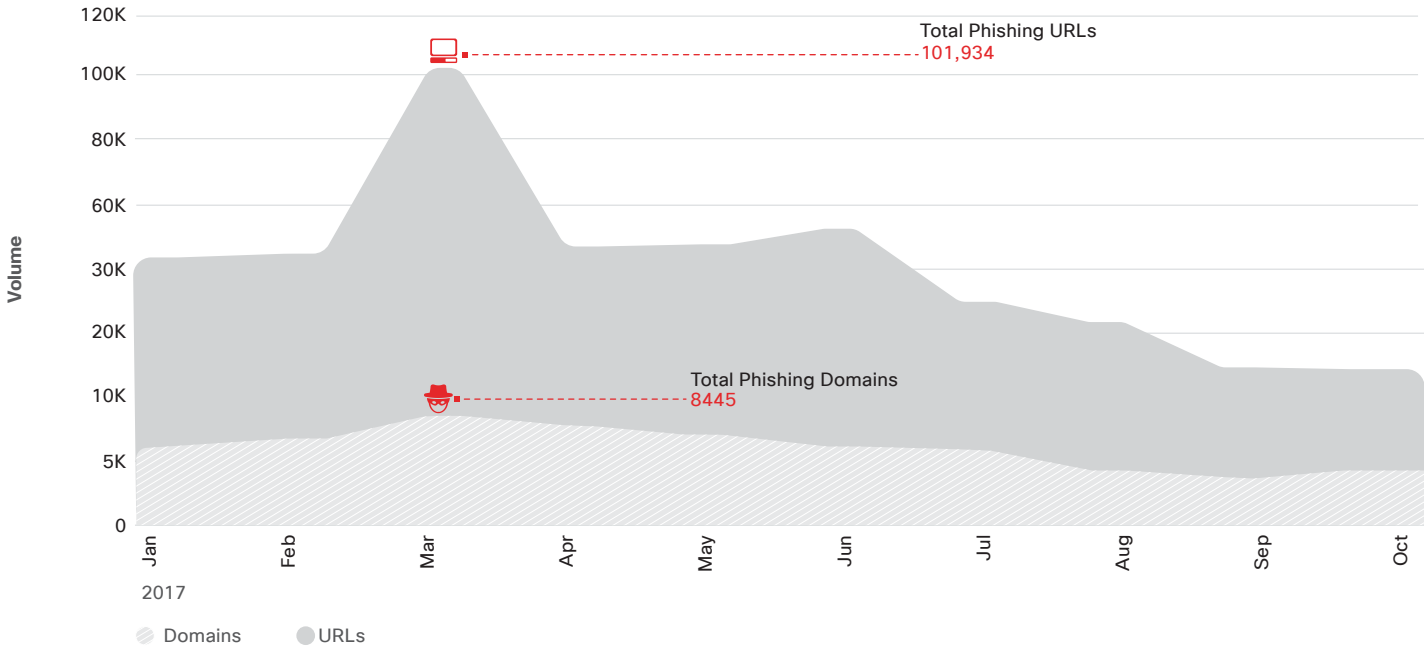
Source: Cisco Security Research

Social engineering still a critical launchpad for email attacks

Phishing and spear phishing are well-worn tactics for stealing users' credentials and other sensitive information, and that's because they are very effective. In fact, phishing and spear phishing emails were at the root of some of the biggest, headline-grabbing breaches in recent years. Two examples from 2017 include a widespread attack that targeted Gmail users[12] and a hack of Irish energy systems.[13]

To gauge how prevalent phishing URLs and domains are on today's Internet, Cisco threat researchers examined data from sources that investigate potentially "phishy" emails submitted by users through community-based, anti-phishing threat intelligence. Figure 14 shows the number of phishing URLs and phishing domains observed during the period from January to October 2017.

Figure 14 Number of observed phishing URLs and domains by month



Source: Cisco Security Research

The spikes seen in March and June can be attributed to two different campaigns. The first appeared to target users of a major telecom services provider. That campaign:

- Involved 59,651 URLs containing subdomains under aaaainfomation[dot]org.
- Had subdomains that contained random strings consisting of 50-62 letters.

Each subdomain length (50-62) contained about 3500 URLs, which allowed for programmatic use of the subdomains (example: Cewekonuxykysowegulukozapojygepuqybyteqe johofopefogu[dot]aaaainfomation[dot]org).

Adversaries used an inexpensive privacy service to register the domains observed in this campaign.

12 *Massive Phishing Attack Targets Gmail Users,* by Alex Johnson, NBC News, May 2017: nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501.

13 *Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure,* by Lizzie Deardon, *The Independent*, July 2017: independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html.

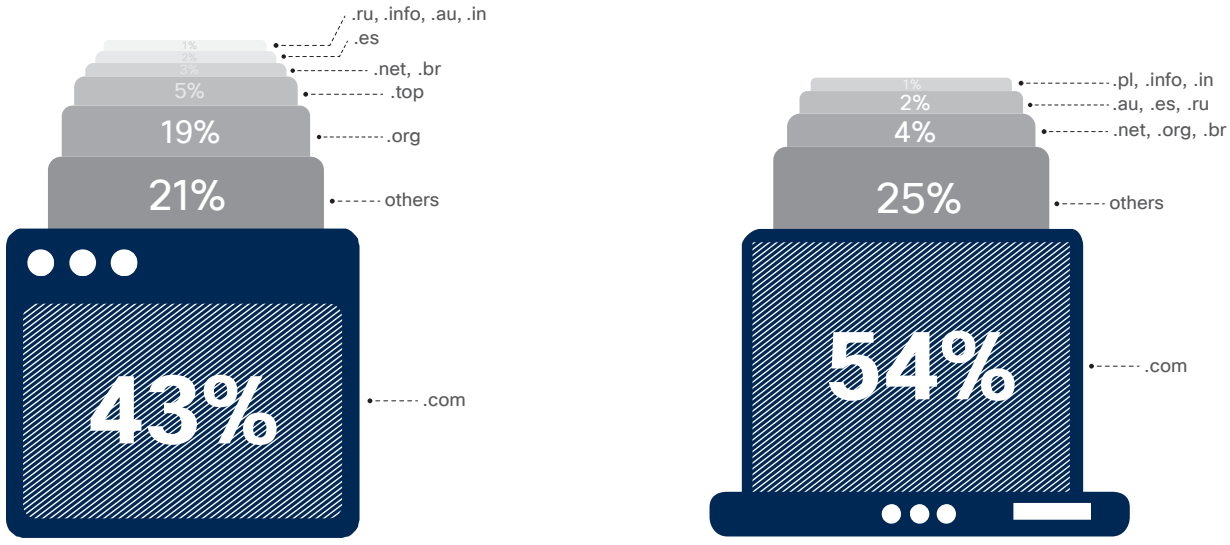
In the second campaign, which was most active in June, threat actors used the name of a legitimate tax agency in the United Kingdom to disguise their actions. They employed 12 top-level domains (TLDs). Eleven of the domains were URLs with six random six-character strings (example: jyzwyp[dot]top). And nine of the domains were associated with more than 1600 phishing sites each.

Like the March campaign, adversaries registered the domains using a privacy service to conceal domain registration information. They registered all the domains over a two-day period. On the second day, nearly 19,000 URLs connected to the campaign were observed, and all were discovered within a five-hour window (for more on how quickly threat actors put newly registered domains to use, see "Malicious use of legitimate resources for backdoor C2," on page 24).

TLD distribution across known phishing sites

Our analysis of phishing sites during the period from January to August 2017 found that threat actors were employing 326 unique TLDs for these activities, including .com, .org, .top (largely due to the United Kingdom taxing agency campaign), and country-specific TLDs (see Figure 15). Employing lesser-known TLDs can be advantageous for adversaries; these domains are typically inexpensive and often offer inexpensive privacy protection.

Figure 15 TLD distribution across known phishing sites



Source: Cisco Security Research

Defenders should be vigilant in monitoring this "old" threat

In 2017, tens of thousands of phishing attempts were reported monthly to the community-based, anti-phishing threat intelligence services included in our analysis. Some of the common tactics and tools adversaries use to execute phishing campaigns include:

- **Domain squatting:** Domains named to look like valid domains (example: cisc0[dot]com).
- **Domain shadowing:** Subdomains added under a valid domain without the owner's knowledge (example: badstuff[dot]cisco[dot]com).
- **Maliciously registered domains:** A domain created to serve malicious purposes (example: viqpbe[dot]top).
- **URL shorteners:** A malicious URL disguised with a URL shortener (example: bitly[dot]com/random-string).

  Note: In the data we examined, Bitly.com was the URL-shortening tool adversaries used most. Malicious shortened URLs represented 2 percent of the phishing sites in our study. That number peaked to 3.1 percent in August.
- **Subdomain services:** A site created under a subdomain server (example: mybadpage[dot]000webhost[dot]com).

Threat actors in the phishing and spear phishing game are continuously refining social engineering methods to trick users into clicking malicious links or visiting fraudulent web pages, and providing credentials or other types of high-value information. User training and accountability, and the application of email security technologies, remain crucial strategies for combatting these threats.

SANDBOX EVASION TACTICS

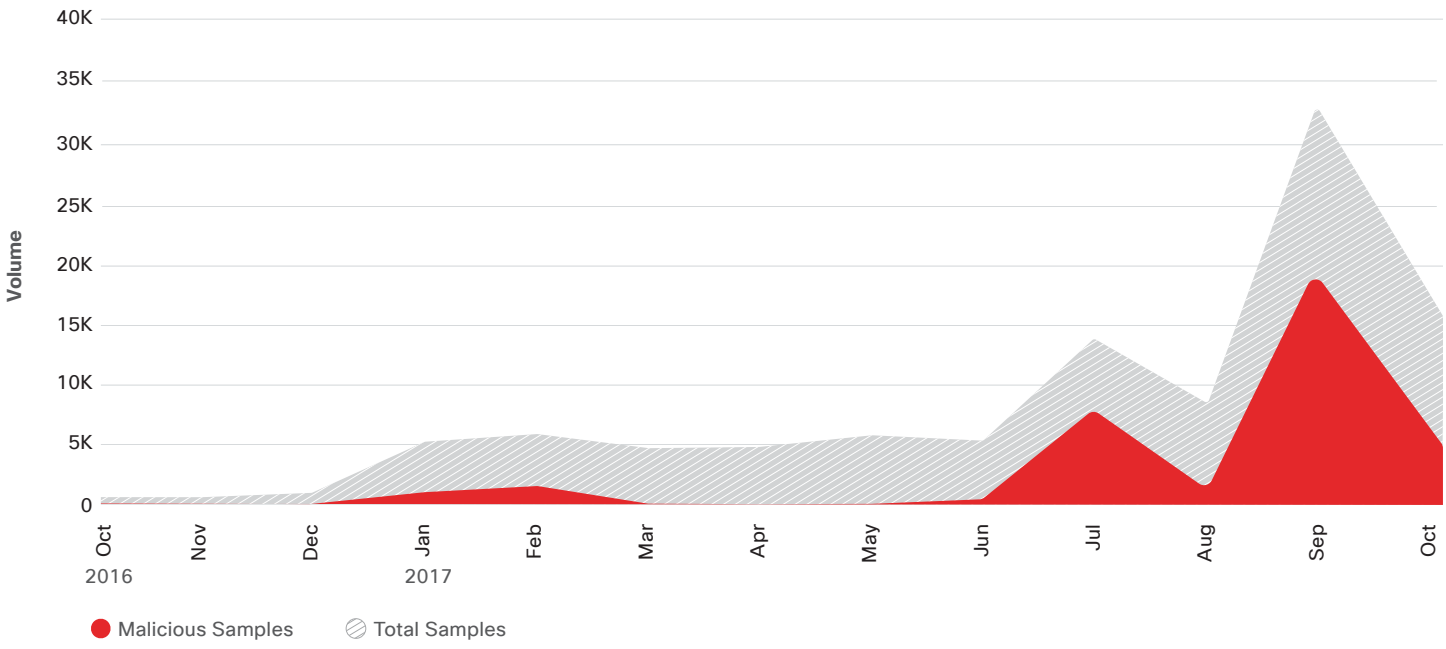
Adversaries are becoming adept at developing threats that can evade increasingly sophisticated sandboxing environments. When Cisco threat researchers analyzed malicious email attachments that were equipped with various sandbox evasion techniques, they discovered that the number of malicious samples using a particular sandbox evasion technique showed sharp peaks, and then quickly dropped. This is yet another example of how attackers are swift to ramp up the volume of attempts to break through defenses once they find an effective technique.

Malware authors playing dirty tricks in defenders' sandboxes

In September 2017, Cisco threat researchers noted high volumes of samples where a malicious payload is delivered after a document is closed (Figure 16). In this case, the malware is triggered using the "document_close" event. The technique works because, in many cases, documents are not closed after the document has been opened and analyzed in the sandbox. Because the sandbox doesn't explicitly close the document, the attachments are deemed safe by the sandbox, and will be delivered to the intended recipients. When a recipient opens the document attachment, and later closes the document, the malicious payload is delivered. Sandboxes that don't properly detect actions on document close can be evaded using this technique.

The use of the "document_close" event is a clever option for attackers. It takes advantage of the macro functionality built into Microsoft Office, as well as users' tendency to open attachments that they believe are relevant to them. Once users realize the attachment is not relevant to them, they close the document, triggering the macros in which the malware is hidden.

Figure 16 High volume of malicious Microsoft Word documents using "close function calls" observed in September 2017

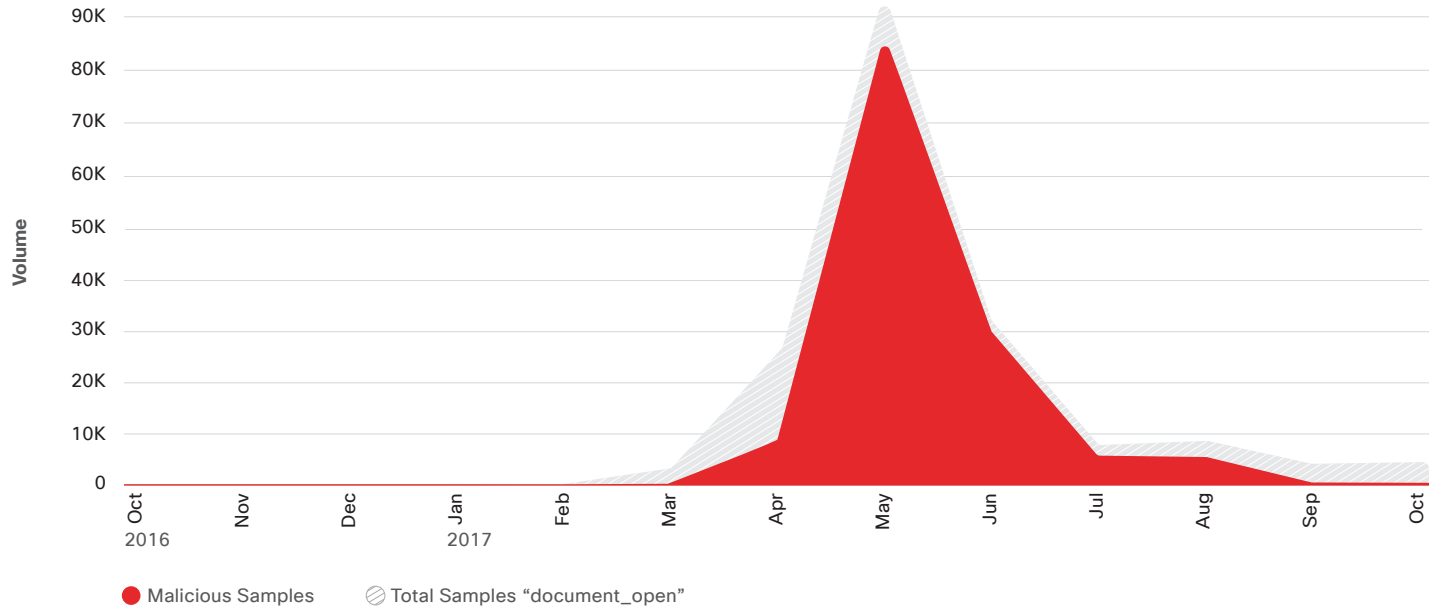


Source: Cisco Security Research

Some attackers evade sandboxing by disguising the type of document in which the malicious payload exists. As seen in Figure 17, we noted a significant attack in May 2017 that was built around malicious Word documents embedded within PDF documents. The documents might bypass sandboxes that simply detect and open the PDF, instead of also opening and analyzing the embedded Word document. The PDF document typically contained an enticement for the user to click and open the Word document, which would trigger the malicious behavior. Sandboxes that don't open and analyze embedded documents within PDFs can be bypassed using this technique.

After viewing the spike in malicious samples involving these PDFs, our threat researchers refined the sandbox environment to detect whether PDFs contained actions or enticements to open embedded Word documents.

Figure 17 Large attack in May 2017 involved PDFs with malicious embedded Word documents



Source: Cisco Security Research

The spikes in malicious samples using different sandbox evasion techniques point to malicious actors' desire to follow a method that seems to work for them—or for other attackers. Also, if adversaries go to the trouble of creating malware and associated infrastructure, they want a return on their investments. If they determine that malware can slip through sandbox testing, they will, in turn, increase the number of attack attempts and affected users.

Cisco researchers recommend using sandboxing that includes "content-aware" features to help ensure malware that uses the tactics described above does not evade sandbox analysis. For example, sandboxing technology should show awareness of the metadata features of the samples it is analyzing—such as determining whether the sample includes an action upon closing of the document.

ABUSE OF CLOUD SERVICES AND OTHER LEGITIMATE RESOURCES

As applications, data, and identities move to the cloud, security teams must manage the risk involved with losing control of the traditional network perimeter. Attackers are taking advantage of the fact that security teams are having difficulty defending evolving and expanding cloud and IoT environments. One reason is the lack of clarity around who exactly is responsible for protecting those environments.

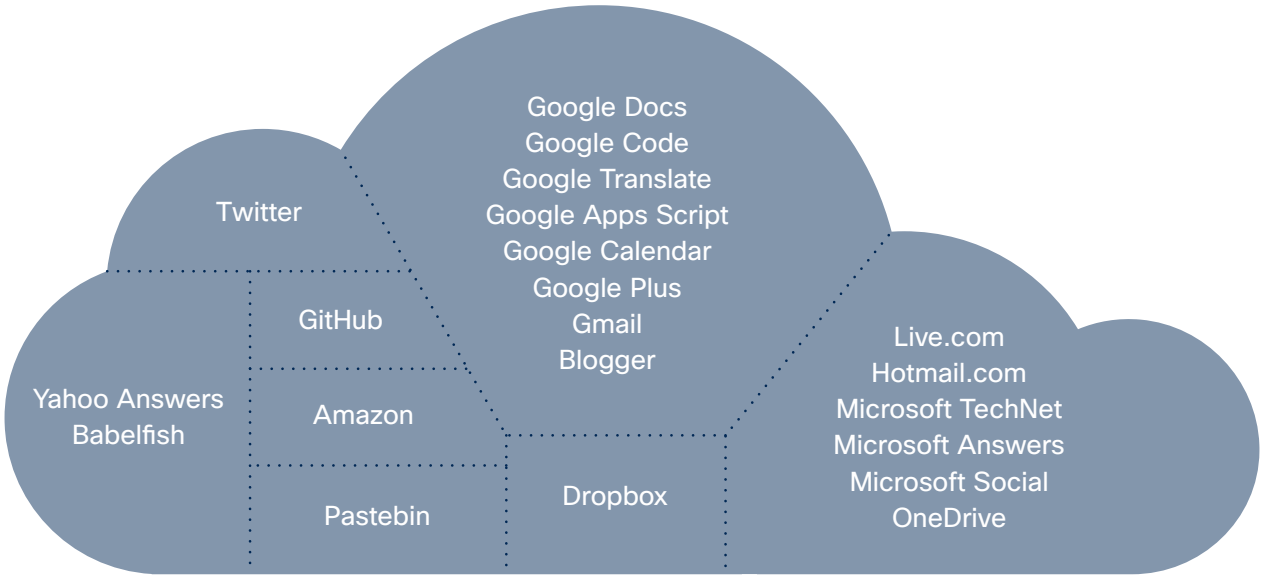
To meet this challenge, enterprises may need to apply a combination of best practices, advanced security technologies like machine learning, and even some experimental methodologies, depending on the services they use for their business and how threats in this space evolve.

Malicious use of legitimate resources for backdoor C2

When threat actors use legitimate services for command and control (C2), malware network traffic becomes nearly impossible for security teams to identify because it mimics the behavior of legitimate network traffic. Adversaries have a lot of Internet "noise" to use as cover because so many people today rely on services like Google Docs and Dropbox to do their work, regardless of whether these services are offered or systemically endorsed by their employers.

Figure 18 shows several of the well-known legitimate services that researchers with Anomali, a Cisco partner and threat intelligence provider, have observed being used in malware backdoor C2 schemas[14] in the last few years. (Note: These types of services face a dilemma in combatting abuse, as making it more difficult for users to set up accounts and use their services can adversely affect their ability to generate revenue.)

Figure 18 Examples of legitimate services abused by malware for C2



Source: Anomali

14 Anomali defines a C2 schema as "the totality of IP addresses, domains, legitimate services, and all the remote systems that are part of the … communications architecture" of malware.

According to Anomali's research, advanced persistent threat (APT) actors and state-sponsored groups were among the first adversaries to use legitimate services for C2; however, the technique is now embraced by a broader range of sophisticated adversaries in the shadow economy. Using legitimate services for C2 appeals to malicious actors because it's easy to:

- Register new accounts on these services.
- Set up a web page on the publicly accessible Internet.
- Usurp encryption for C2 protocols. (Instead of setting up C2 servers with encryption or building encryption into malware, attackers can simply adopt the SSL certificate of a legitimate service.)
- Adapt and transform resources on the fly. (Attackers can reuse implants across attacks without reusing DNS or IP addresses, for instance.)
- Reduce the likelihood of "burning" infrastructure. (Adversaries that use legitimate services for C2 don't need to hard-code malware with IP addresses or domains. When their operation is complete, they can simply take down their legitimate services pages—and no one will ever know the IP addresses.)
- Attackers benefit from this technique because it allows them to reduce overhead and improve their return on investment.

For defenders, adversaries' use of legitimate services for C2 presents some significant challenges:

Legitimate services are difficult to block
Can organizations, from a mere business perspective, even consider blocking parts of legitimate Internet services like Twitter or Google?

Legitimate services are often encrypted and innately difficult to inspect
SSL decrypting is expensive and not always possible at enterprise scale. So, malware hides its communication inside of encrypted traffic, making it difficult, if not impossible, for security teams to identify malicious traffic.

Use of legitimate services subverts domain and certificate intelligence, and complicates attribution
Adversaries don't need to register domains because the legitimate service account is considered the initial C2 address. Also, they're not likely to continue registering SSL certificates or using self-signed SSL certificates for C2 schemas. Both trends obviously will have a negative impact on indicator feeds for reputation filtering and indicator blacklisting, which are based on newly generated and newly registered domains and the certificates and IP addresses connected to them.

Detecting the use of legitimate services for C2 is difficult. However, Anomali's threat researchers recommend that defenders consider applying some experimental methodologies. For example, defenders may identify malware using legitimate services for C2 by looking for:

- Non-browser, non-app connections to legitimate services
- Unique or low page response sizes from legitimate services
- High certificate exchange frequencies to legitimate services
- Bulk sandboxing samples for suspicious DNS calls to legitimate services

All these unique behaviors merit further investigation of the source programs and processes.[15]

15 For details on these experimental methodologies, and more information about how adversaries use legitimate services for C2, download the Anomali research paper, *Rise of Legitimate Services for Backdoor Command and Control*, available at: anomali.cdn.rackfoundry.net/files/anomali-labs-reports/legit-services.pdf.

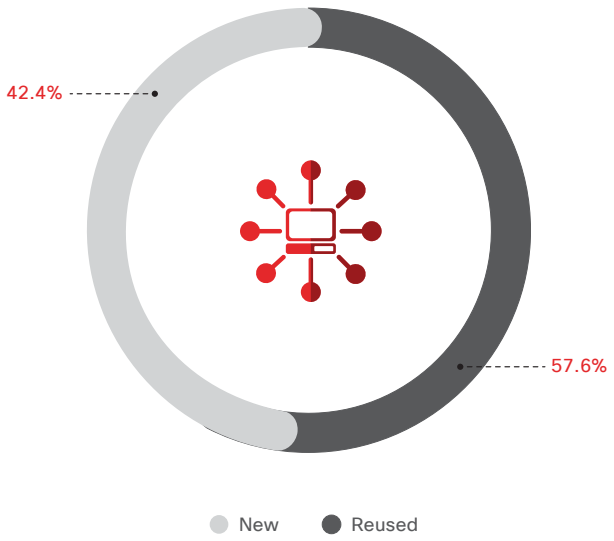
Extracting optimal value from resources

Cisco security researchers analyzed newly seen unique query names (domains) associated with DNS queries made over a seven-day period in August 2017. Note that "newly seen" in this discussion has no bearing on when a domain was created; it relates to when a domain was first "seen" by Cisco cloud security technology during the period of observation.

The purpose of this research was to gain more insight into how often adversaries use, and reuse, registered-level domains (RLDs) in their attacks. Understanding threat actor behavior at the domain level can help defenders identify malicious domains, and related subdomains, that should be blocked with first-line-of-defense tools like cloud security platforms.

So that our researchers could focus solely on the core group of unique RLDs—about 4 million in total—subdomains were stripped from the sample of newly seen domains. Only a small percentage of the RLDs in that sample was categorized as malicious. Of the RLDs that were malicious, more than half (about 58 percent) were reused, as Figure 19 shows.

Figure 19 Percent of new vs. reused domains



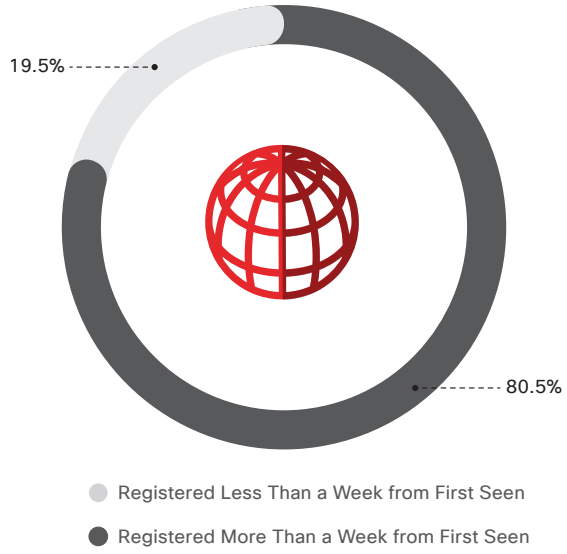
Source: Cisco Security Research

That finding suggests that, while most attackers build new domains for their campaigns, many are focused on trying to get the best return on their investments by launching multiple campaigns from a single domain. Domain registration can be costly, especially at the scale most attackers require to execute their campaigns and evade detection.

One-fifth of malicious domains quickly put into use

Adversaries may sit on domains for days, months, or even years after registering them, waiting for the right time to use them. However, Cisco threat researchers observed that a significant percentage of malicious domains—about 20 percent—were used in campaigns less than one week after they were registered (see Figure 20).

Figure 20 RLD registration times

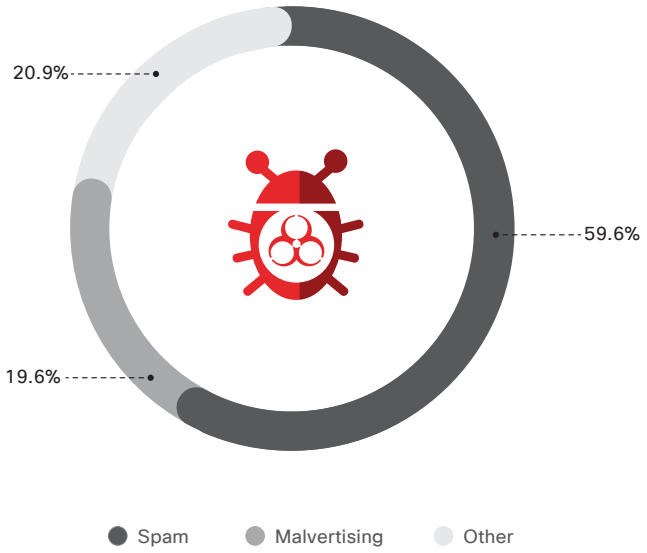


Source: Cisco Security Research

Many new domains tied to malvertising campaigns

Most malicious domains we analyzed were associated with spam campaigns—about 60 percent. Nearly one-fifth of the domains were connected to malvertising campaigns (see Figure 21). Malvertising has become an essential tool for directing users to exploit kits, including those that distribute ransomware.

Figure 21 Malicious categorizations



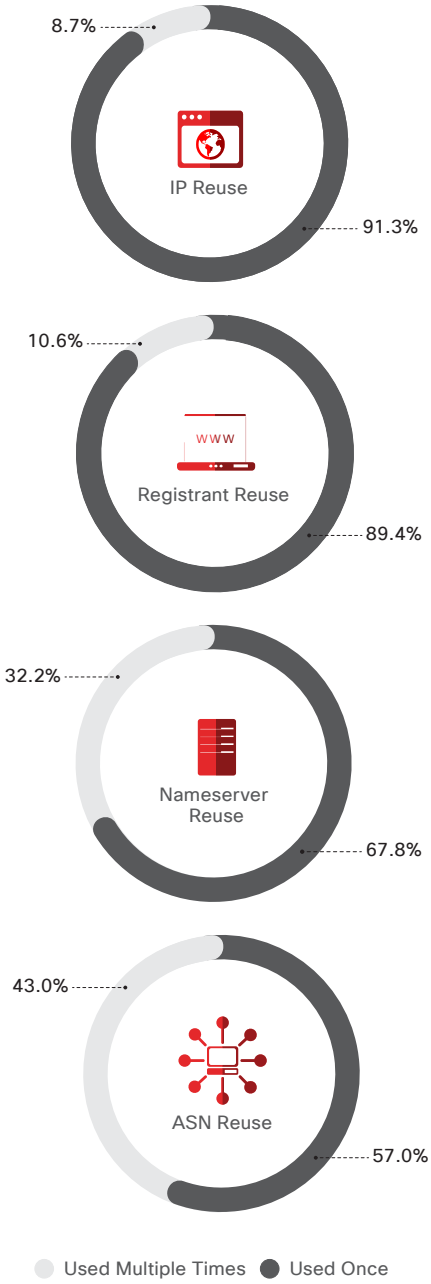
Source: Cisco Security Research

Well-worn, domain-related techniques for creating malvertising campaigns include domain shadowing. In this technique, attackers steal legitimate domain account credentials to create subdomains directed at malicious servers. Another tactic is the abuse of free, dynamic DNS services to generate malicious domains and subdomains. That allows threat actors to deliver malicious payloads from constantly changing hosting IPs, either infected users' computers or compromised public websites.

Domains reuse infrastructure resources

The malicious RLDs in our sample also appeared to reuse infrastructure resources, such as registrant email addresses, IP addresses, autonomous system numbers (ASNs), and nameservers (see Figure 22). This is further evidence of adversaries trying to get the most value from their investments in new domains and preserve resources, according to our researchers. For example, an IP address can be used by more than one domain. So, an attacker laying the groundwork for a campaign might decide to invest in a few IP addresses and an array of domain names instead of servers, which cost more.

Figure 22 Reuse of infrastructure by malicious RLDs



Source: Cisco Security Research

The resources that RLDs reuse give clues to whether the domain is likely to be malicious. For example, reuse of registrant emails or IP addresses occurs infrequently, so a pattern of reuse on either front suggests suspicious behavior. Defenders can have a high degree of confidence in blocking those domains, knowing that doing so probably will have no negative impact on business activity.

Static blocking of ASNs and nameservers is not likely to be feasible in most cases. However, patterns of reuse by RLDs are worthy of further investigation to determine whether certain domains should be blocked.

Using intelligent, first-line-of-defense cloud security tools to identify and analyze potentially malicious domains and subdomains can help security teams follow the trail of an attacker and answer questions, such as:

- What IP address does the domain resolve to?
- What ASN is associated with that IP address?
- Who registered the domain?
- What other domains are associated with that domain?

The answers can help defenders not only refine security policies and block attacks, but also prevent users from connecting to malicious destinations on the Internet while they're on the enterprise network.

DevOps technologies at risk for ransomware attacks

2017 saw the emergence of DevOps ransomware attacks, beginning with a campaign in January that targeted open-source database platform, MongoDB.[16] Attackers encrypted public MongoDB instances and demanded ransom payments for decryption keys and software. Soon after, they set their sights on compromising databases, such as CouchDB and Elasticsearch, with server-targeted ransomware.

Rapid7 is a Cisco partner and provider of security data and analytics solutions. As Rapid7 researchers explained in our *Cisco 2017 Midyear Cybersecurity Report*, DevOps services are often deployed improperly, or left open intentionally for convenient access by legitimate users—leaving these services open for attack.

Rapid7 performs regular Internet sweeps for DevOps technologies and catalogs both open instances and ransomed instances. Some of the DevOps services they encounter during their sweeps may contain personally identifiable information (PII), based on the names of the tables exposed to the Internet.

To reduce their risk of exposure to DevOps ransomware attacks, organizations that use public Internet instances of DevOps technologies should:

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

For more details on Rapid7's research, see "Don't let DevOps technologies leave the business exposed," in the *Cisco 2017 Midyear Cybersecurity Report.*

16 *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.**

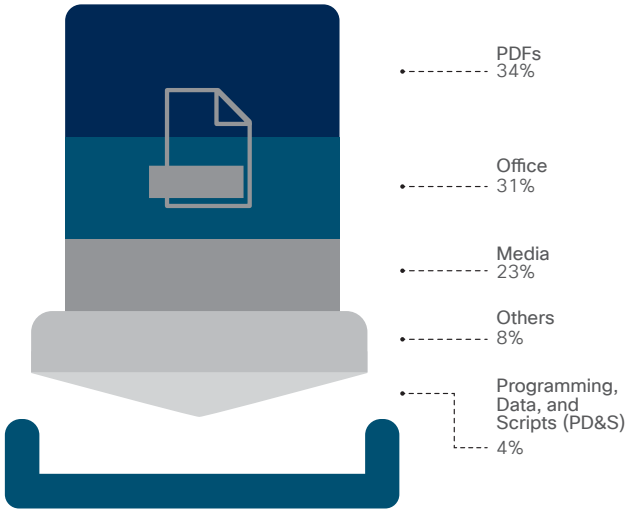
Insider threats: Taking advantage of the cloud

In previous security reports, we have discussed the value of OAuth permissions and super-user privileges to enforce who can enter networks, and how they can access data.[17] To further examine the impact of user activity on security, Cisco threat researchers recently examined data exfiltration trends. They employed a machine-learning algorithm to profile 150,000 users in 34 countries, all using cloud service providers, from January to June 2017. The algorithm accounted for not only the volume of documents being downloaded, but also variables such as the time of day of downloads, IP addresses, and locations.

After profiling users for six months, our researchers spent 1.5 months studying abnormalities. flagging 0.5 percent of users for suspicious downloads. That's a small amount, but these users downloaded, in total, more than 3.9 million documents from corporate cloud systems, or an average of 5200 documents per user during the 1.5-month period. Of the suspicious downloads, 62 percent occurred outside of normal work hours; 40 percent took place on weekends.

Cisco researchers also conducted a text-mining analysis on the titles of the 3.9 million suspiciously downloaded documents.

Figure 23 Most commonly downloaded documents



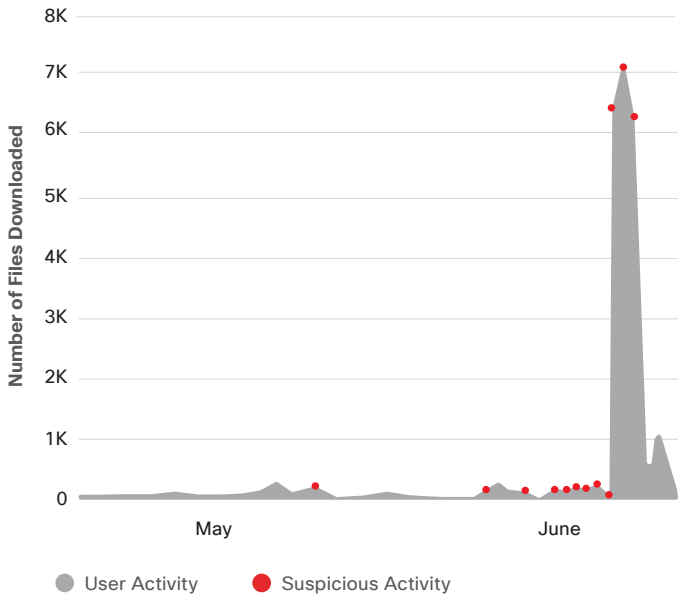
Source: Cisco Security Research

One of the most popular keywords in the documents' titles was "data." The keywords most commonly appearing with the word "data" were "employee" and "customer." Of the types of documents downloaded, 34 percent were PDFs and 31 percent were Microsoft Office documents (see Figure 23).

Applying machine-learning algorithms offers a more nuanced view of cloud user activity beyond just the number of downloads. In our analysis, 23 percent of the users we studied were flagged more than three times for suspicious downloads, usually starting with small numbers of documents. The volume slowly increased each time, and eventually, these users showed sudden and significant spikes in downloads (Figure 24).

Machine-learning algorithms hold the promise of providing greater visibility into the cloud and user behavior. If defenders can start predicting user behavior in terms of downloads, they can save the time it might take to investigate legitimate behavior. They can also step in to stop a potential attack or data-exfiltration incident before it happens.

Figure 24 Machine-learning algorithms capture suspicious user download behavior



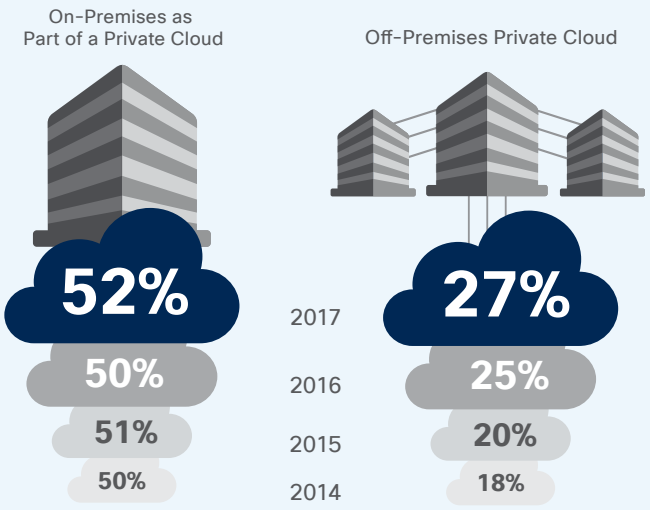
Source: Cisco Security Research

17 *Cisco 2017 Midyear Cybersecurity Report*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Cisco 2018 Security Capabilities Benchmark Study: Security viewed as a key benefit of hosting networks in the cloud

The use of on-premises and public cloud infrastructure is growing, according to the Cisco 2018 Security Capabilities Benchmark Study, although many organizations still host networks on-premises. In the 2017 study, 27 percent of security professionals said they are using off-premises private clouds, compared with 25 percent in 2016 and 20 percent in 2015 (Figure 25). Fifty-two percent said their networks are hosted on-premises as part of a private cloud.

Figure 25 More organizations are using private clouds



2014 (n=1727), 2015 (n=2417), 2016 (n=2887), 2017 (n=3625)

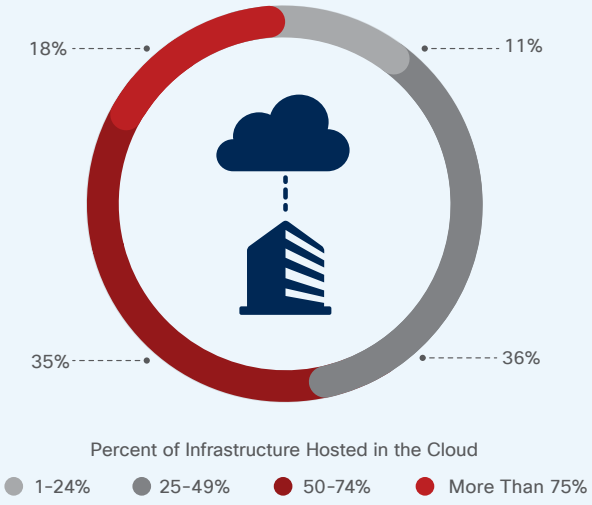
Source: Cisco 2018 Security Capabilities Benchmark Study

Of those organizations using the cloud, 36 percent host 25 to 49 percent of their infrastructure in the cloud, while 35 percent host 50 to 74 percent of their infrastructure in the cloud (Figure 26).

Security is the most common benefit of hosting networks in the cloud, according to the security personnel respondents. Among them, 57 percent said they host networks in the cloud because of better data security; 48 percent, because of scalability; and 46 percent, because of ease of use (see Figure 27).

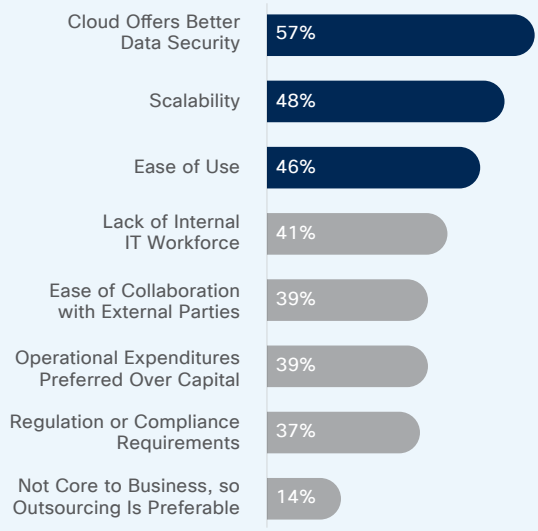
Respondents also said that, as more infrastructure is moved to the cloud, they may look to invest in cloud access security brokers (CASBs) to add extra security to cloud environments.

Figure 26 Fifty-three percent of organizations host at least half of infrastructure in the cloud



Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 27 Fifty-seven percent believe the cloud offers better data security



Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

IoT AND DDoS ATTACKS

The IoT is still evolving, but adversaries are already exploiting security weaknesses in IoT devices to gain access to systems—including industrial control systems that support critical infrastructure. IoT botnets are also growing in both size and power, and are increasingly capable of unleashing powerful attacks that could severely disrupt the Internet. Attackers' shift toward greater exploitation of the application layer indicates that this is their aim. But many security professionals aren't aware of, or they dismiss, the threat that IoT botnets pose. Organizations keep adding IoT devices to their IT environments with little or no thought about security, or worse, take no time to assess how many IoT devices are touching their networks. In these ways, they're making it easy for adversaries to take command of the IoT.

Few organizations see IoT botnets as an imminent threat—but they should

As the IoT expands and evolves, so too are IoT botnets. And as these botnets grow and mature, attackers are using them to launch DDoS attacks of increasing scope and intensity. Radware, a Cisco partner, offered an analysis of three of the largest IoT botnets—Mirai, Brickerbot, and Hajime—in the *Cisco 2017 Midyear Cybersecurity Report*, and revisits the IoT botnet topic in our latest report to underscore the severity of this threat.[18] Their research shows that only 13 percent of organizations believe that IoT botnets will be a major threat to their business in 2018.

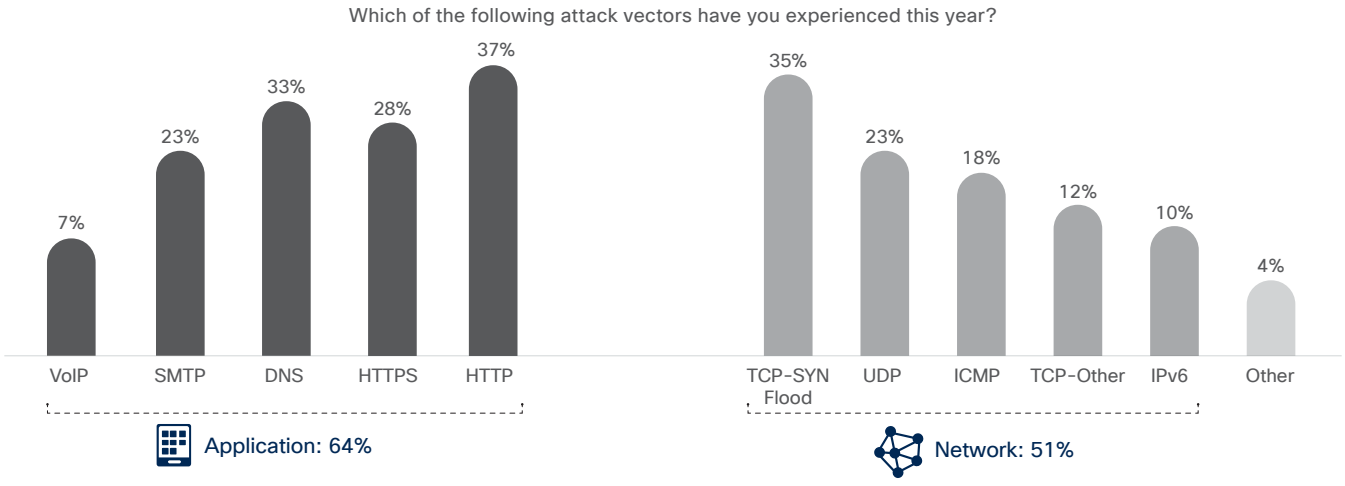
IoT botnets are thriving because organizations and users are deploying low-cost IoT devices rapidly and with little or no regard for security. IoT devices are Linux- and Unix-based systems, so they are often targets of executable and linkable format (ELF) binaries. They are also less challenging to take control of than a PC, which means it's easy for adversaries to quickly build a large army.

IoT devices operate on a 24-hour basis and can be called into action at a moment's notice. And as adversaries increase the size of their IoT botnets, they are investing in more sophisticated code and malware and shifting to more advanced DDoS attacks.

Application DDoS overtakes network DDoS

Application layer attacks are on the rise while network layer attacks are declining (see Figure 28). Radware researchers suspect this shift can be attributed to growth in IoT botnets. The trend is concerning because the application layer is so diverse, and has so many devices within it, which means attacks targeting this layer could potentially shut down large portions of the Internet.

Figure 28 Application DDoS attacks increased in 2017



Source: Radware

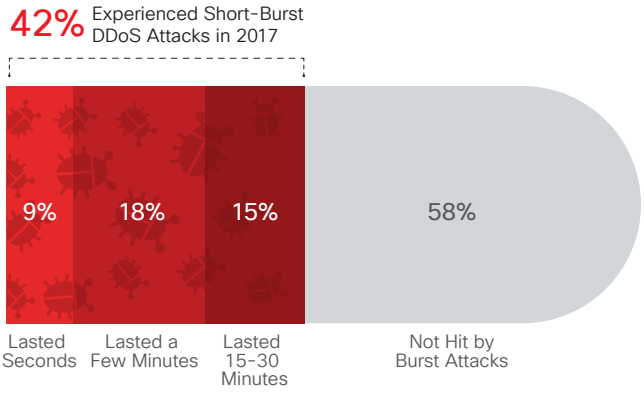
18 For more details on Radware's IoT botnet research, see "The IoT is only just emerging but the IoT botnets are already here," p. 39, *Cisco 2017 Midyear Cybersecurity Report*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

More attackers are turning to the application layer because there is little left to exploit in the network layer, according to Radware researchers. IoT botnets are also less resource-intensive than PC botnets to build. That means adversaries can invest more resources in developing advanced code and malware. The operators of the multivector botnet Mirai, which is known for advanced application attacks, are among those making that type of investment.

"Burst attacks" increasing in complexity, frequency, and duration

One of the most significant DDoS attack trends Radware observed in 2017 was an increase in short-burst attacks, which are becoming more complex, frequent, and persistent. Forty-two percent of organizations in Radware's investigation experienced this type of DDoS attack in 2017 (Figure 29). In most of the attacks, the recurring bursts lasted only a few minutes.

Figure 29 Experience with DDoS attacks in recurring bursts



Source: Radware

Burst tactics are typically aimed at gaming websites and service providers due to their targets' sensitivity to service availability and their inability to sustain such attack maneuvers. Timely or random bursts of high traffic rates over a period of days or even weeks can leave these organizations with no time to respond, causing severe service disruptions.

Radware researchers say that burst attacks:

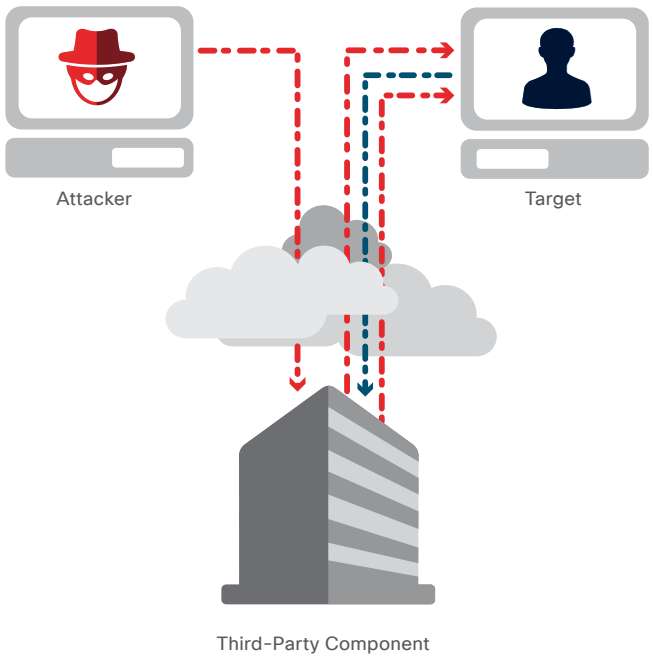
- Are composed of multiple changing vectors. The attacks are geographically distributed and manifest as a sustained series of precise and high-volume SYN floods, ACK floods, and User Datagram Protocol (UDP) floods on multiple ports.
- Combine high-volume attacks with varying durations—from two to 50 seconds of high burst-traffic with intervals of approximately five to 15 minutes.
- Are often combined with other long-duration DDoS attacks.

Growth in reflection amplification attacks

Another DDoS trend Radware observed during 2017 is growth in reflection amplification DDoS attacks as a major vector against a wide spectrum of services. According to Radware, two in five businesses experienced a reflection amplification attack in 2017. One-third of those organizations reported that they were unable to mitigate these attacks.

A reflection amplification attack uses a potentially legitimate third-party component to send attack traffic to a target, concealing the attacker's identity. Attackers send packets to the reflector servers with a source IP address set to the target user's IP. That makes it possible to indirectly overwhelm the target with response packets and exhaust the target's utilization of resources (see Figure 30).

Figure 30 Reflection amplification attack



Source: Radware

To successfully execute a reflection amplification attack, adversaries need to have a larger bandwidth capacity than their targets. Reflector servers make that possible: the attacker simply reflects the traffic from one or more third-party machines. Since these are ordinary servers, this type of attack is particularly difficult to mitigate. Common examples include:

DNS amplification reflective attacks
This sophisticated denial of service attack takes advantage of a DNS server's behavior to amplify the attack. A standard DNS request is smaller than the DNS reply. In a DNS amplification reflective attack, the attacker carefully selects a DNS query that results in a lengthy reply that's up to 80 times longer than the request (for example, "ANY"). The attacker sends this query using a botnet to third-party DNS servers while spoofing the source IP address with the target user's IP address. The third-party DNS servers send their responses to the target's IP address. With this attack technique, a relatively small botnet can channel a volumetric flood of large responses toward the target.

NTP reflection
This type of amplification attack exploits publicly accessible Network Time Protocol (NTP) servers to overwhelm and exhaust defenders with UDP traffic. NTP is an old networking protocol for clock synchronization between computer systems over packet-switched networks. It is still widely used across the Internet by desktops, servers, and even phones to keep their clocks in sync. Several old versions of NTP servers contain a command called monlist, which sends the requester a list of up to the last 600 hosts that connected to the queried server.

In a basic scenario, the attacker repeatedly sends the "get monlist" request to a random NTP server and spoofs the source IP address for the requesting server as the target server. NTP server responses are then directed to the target server to cause a significant increase in UDP traffic from source port 123.

SSDP reflection
This attack exploits the Simple Service Discovery Protocol (SSDP), which is used to allow Universal-Plug-and-Play (UPnP) devices to broadcast their existence. It also helps to enable discovery and control of networked devices and services, such as cameras, network-attached printers, and many other types of electronic equipment.

Once a UPnP device is connected to a network, and after it receives an IP address, the device is able to advertise its services to other computers in the network by sending a message in a multicast IP. When a computer gets the discovery message about the device, it makes a request for a complete description of the device services. The UPnP device then responds directly to that computer with a complete list of any services it has to offer.

As with NTP and DNS amplified DDoS attacks, the attacker can use a small botnet to query that final request for the services. The attacker then spoofs the source IP to the target user's IP address and aims the responses directly at the target.

Defenders must remediate "leak paths"

A "leak path," as defined by Cisco partner Lumeta, is a policy or segmentation violation or unauthorized or misconfigured connection created to the Internet on an enterprise network, including from the cloud, that allows traffic to be forwarded to a location on the Internet—such as a malicious website. These unexpected connections can also occur internally between two different network segments that should not be communicating with each other. For example, in critical infrastructure environments, an unexpected leak path between the manufacturing floor and business IT systems could indicate malicious activity. Leak paths can also stem from improperly configured routers and switches.

Devices that don't have permissions set up correctly, or are left open and unmanaged, are vulnerable to attackers. Devices and networks related to rogue or shadow IT are also fertile ground for adversaries to establish leak paths because they tend to be unmanaged and unpatched. Lumeta estimates that about 40 percent of the dynamic networks, endpoints, and cloud infrastructure in enterprises is leading to significant infrastructure blind spots and lack of real-time awareness for security teams.

Detection of existing leak paths are critical as they can be exploited at any time. However, newly created leak paths are important to detect in real time since they are immediate indicators of compromise and are associated with most advanced attacks, including ransomware.

Lumeta's recent analysis of IT infrastructure at more than 200 organizations across several industries underscores the endpoint visibility gap. It also shows that many companies significantly underestimate the number of endpoints in their IT environments (see Figure 31). Lack of awareness about the number of IP-enabled IoT devices connected to the network is often a key reason for underestimation of endpoints.

Figure 31 Overview of infrastructure blind spots across various industries

Lumeta Actual Customers	Government	Healthcare	Tech	Finance
Presumed endpoints	150,000	60,000	8000	600,000
Discovered endpoints	170,000	89,860	14,000	1,200,000
Endpoint visibility gap	12%	33%	43%	50%
Unmanaged networks	3278	24	5	771
Unauthorized or unsecured forwarding devices	520	75	2026	420
Known but unreachable networks	33,256	4	16,828	45
Leak paths to Internet identified on deployment	3000	120	9400	220

Source: Lumeta

Lumeta's researchers suggest that leak paths are on the rise, especially in cloud environments, where there is less network visibility and fewer security controls in place.

Malicious actors don't always immediately use the leak paths they create or find. When they do return to these channels, they use them to install malware or ransomware, steal information, and more. Researchers with Lumeta say one reason leak paths often remain undetected is because threat actors are adept at encrypting and obfuscating their activity—by using TOR, for example. They also are careful to use leak paths judiciously, so as not to alert security teams to their activity.

Lumeta researchers say security team skills gaps, namely the lack of fundamental knowledge about networks, can interfere with organizations' ability to investigate and remediate leak path issues in a timely manner. Better collaboration between security and network teams can help expedite investigations and remediation of leak paths.

Tools for automation that provide network context can also give security analysts insight into potential leak path issues. In addition, implementing appropriate segmentation policies can help security teams quickly determine whether unexpected communication between networks or devices is malicious.

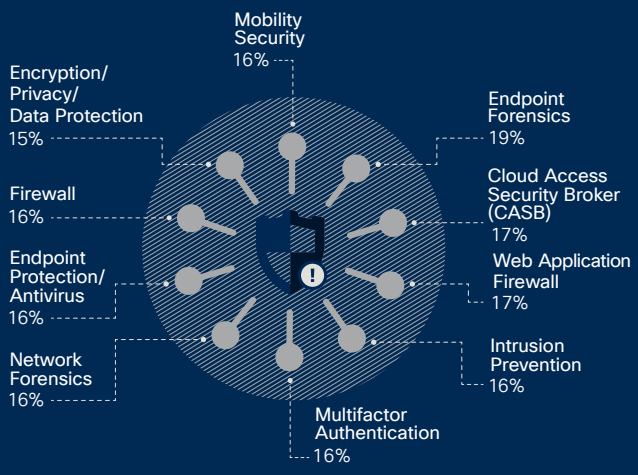
Cisco 2018 Security Capabilities Benchmark Study: Lack of security personnel prevents many organizations from implementing new cyber capabilities

Severe staff shortages remain a major issue for defenders. As noted above, skills gaps can interfere with an organization's ability to investigate and remediate certain types of threats.

Also, without the right talent in place, defenders can't deploy new technology and processes that could help to strengthen their security postures (Figure 32).

Many security professionals interviewed for the Cisco 2018 Security Capabilities Benchmark Study said that, ideally, they would automate or outsource more of their routine activities, so they could redirect staff to higher-value activities.

Figure 32 Key capabilities defenders would add, if staffing levels improved



Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

Industrial control systems vulnerabilities place critical infrastructure at risk

Industrial control systems (ICS) are at the heart of all manufacturing and process control systems. ICS connect to other electronic systems that are part of the control process, creating a highly connected ecosystem of vulnerable devices that a wide range of attackers is eager to compromise.

Threat actors who want to target ICS to cripple critical infrastructure are actively engaged in research and creating backdoor pivot points to facilitate future attacks, according to TrapX Security, a Cisco partner that develops deception-based cybersecurity defenses. Among the potential cyber attackers are experts with advanced knowledge of IT systems, ICS architectures, and the processes they support. Some also know how to program product lifecycle management (PLM) controllers and subsystems.

Threat researchers with TrapX recently conducted investigations into several cyber attacks that targeted customers' ICS to help highlight unexpected problems with ICS cyber defense. Two of the incidents, described below, took place in 2017 and remain under investigation.

Target: Large international water treatment and waste processing company

Attackers used the company's demilitarized zone (DMZ) server as a pivot point to compromise the internal network. The security operations team received alerts from deception security technology embedded in the network DMZ. This physical or logical subnetwork bridges internal networks from untrusted networks, such as the Internet, protecting other internal infrastructure. The investigation found that:

- The DMZ server was breached due to a misconfiguration that allowed RDP connections.
- The server was breached and controlled from several IPs, which were connected to political hacktivists hostile to the plant.
- The attackers were able to launch multiple major attacks against several of the company's other plants from the compromised internal network.

Target: Power plant

This power plant's critical assets include a very large ICS infrastructure and the necessary supervisory control and data acquisition (SCADA) components that manage and run their processes. The plant is considered critical national infrastructure and subject to scrutiny and oversight by the responsible national security agency. It is therefore considered a high-security installation.

The CISO involved decided to implement deception technology to protect the plant's standard IT resources from ransomware attacks. The technology was also distributed within the ICS infrastructure. Soon after, the security operations team received several alerts that indicated a breach to the systems within the critical infrastructure plant operations. Their immediate investigation concluded:

- A device in the process control network was attempting to interact with the deception traps, which were camouflaged as PLM controllers. This was an active attempt to map and understand the exact nature of each PLM controller within the network.
- The compromised device would normally have been closed, but a vendor performing maintenance failed to close the connection when finished. That oversight left the process control network vulnerable to attackers.
- The information adversaries were collecting is exactly the type needed to disrupt plant activity and potentially cause great damage to ongoing plant operations.

Recommendations

Many ICS breaches begin with the compromise of vulnerable servers and computing resources within the corporate IT network. Threat researchers with TrapX recommend that organizations take the following actions to reduce risk and help ensure the integrity of operations within their facilities:

- Review vendors and systems, and see that all patches and updates are applied promptly. (If patches are not available, consider migrating to new technology.)
- Reduce the use of USB memory sticks and DVD drives.
- Isolate ICS systems from IT networks. Don't allow any direct connections between the two. That includes network connections, laptops, and memory sticks.
- Implement policies that severely limit the use of the ICS networks for anything other than essential operations. Reduce accessibility to ICS workstations and monitors with external Internet browser access. Assume these policies will fail and plan accordingly.
- Research and eliminate all embedded passwords or default passwords in your production network. And wherever possible, implement two-factor authentication.
- Review plans for disaster recovery following a major cyber attack.

For additional case studies, see the TrapX Security research paper, *Anatomy of an Attack: Industrial Control Systems Under Siege.*

Cisco 2018 Security Capabilities Benchmark Study: More OT and IoT attacks on the horizon

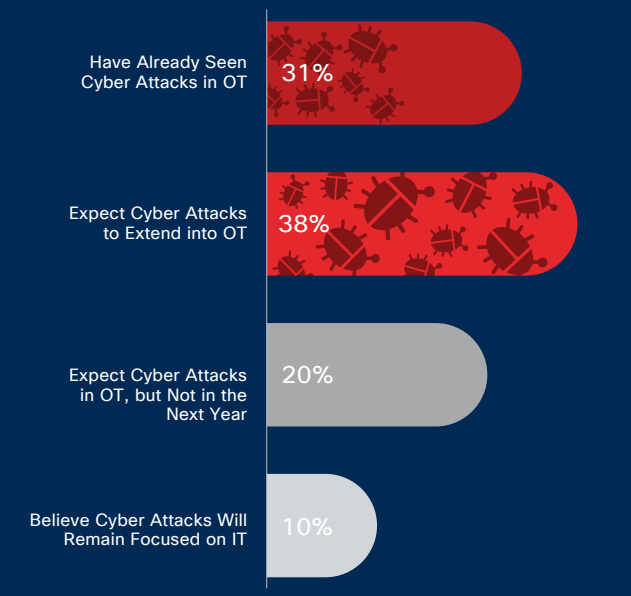
Attacks targeting operational technology (OT) such as ICS and IoT devices are still uncommon enough that many security professionals haven't experienced them firsthand. But according to research for the **Cisco 2018 Security Capabilities Benchmark Study**, security professionals fully expect such attacks to occur, and are trying to determine how they will respond to them.

Security professionals recognize that these systems often have few protections and unpatched and out-of-date software, making them vulnerable to attacks.

"We still have OT devices that are 25 years old, and compressors and machines that are 40 years old," said one respondent. "IT professionals are used to the schedule. [They say,] 'Tell me when Windows X is no longer supported,' or 'Hey, this Oracle version is going EOL [end of life].' There's no such thing in the OT environment."

Few security professionals can speak confidently on issues relating to securing OT in their organizations. That is either because they don't have or anticipate adding much OT, or because IoT implementations are new. Of these professionals, 31 percent said their organizations have already experienced cyber attacks on OT infrastructure, while 38 percent said they expect attacks to extend from IT to OT in the next year (Figure 33).

Figure 33 Thirty-one percent of organizations have experienced cyber attacks on OT infrastructure



Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

VULNERABILITIES AND PATCHING

Amid the chaos of security concerns, defenders may lose sight of vulnerabilities affecting their technology. But you can be sure attackers are paying attention, and calculating how to exploit these potential weaknesses to launch attacks.

There was a time when patching known vulnerabilities within 30 days was considered best practice. Now, waiting that long to remediate could increase an organization's risk of being targeted for attack because threat actors are moving faster to release and use active exploits of vulnerabilities. Organizations also must avoid neglecting small but significant security gaps that could benefit adversaries, especially during the reconnaissance phase of attacks when they are searching for pathways into systems.

Prevalent vulnerabilities in 2017 included buffer overflow errors, Apache Struts

Buffer overflow errors topped the list of Common Weakness Enumeration (CWE) vulnerabilities tracked by Cisco in 2017, although other categories showed movement up and down.

Input validation vulnerabilities increased, while buffer errors declined (Figure 34).

Figure 34 CWE threat category activity

Threat Category	Jan-Sep 2016	Jan-Sep 2017	Change
CWE-119: Buffer errors	493	403	(-22%)
CWE-20: Input validation	227	268	+15%
CWE-264: Permissions, privileges and access	137	163	+18%
CWE-200: Information leak/disclosure	125	250	+100%
CWE-310: Cryptographic issues	27	17	(-37%)
CWE-78: OS Command injections	7	15	+114%
CWE-59: Link following	5	0	

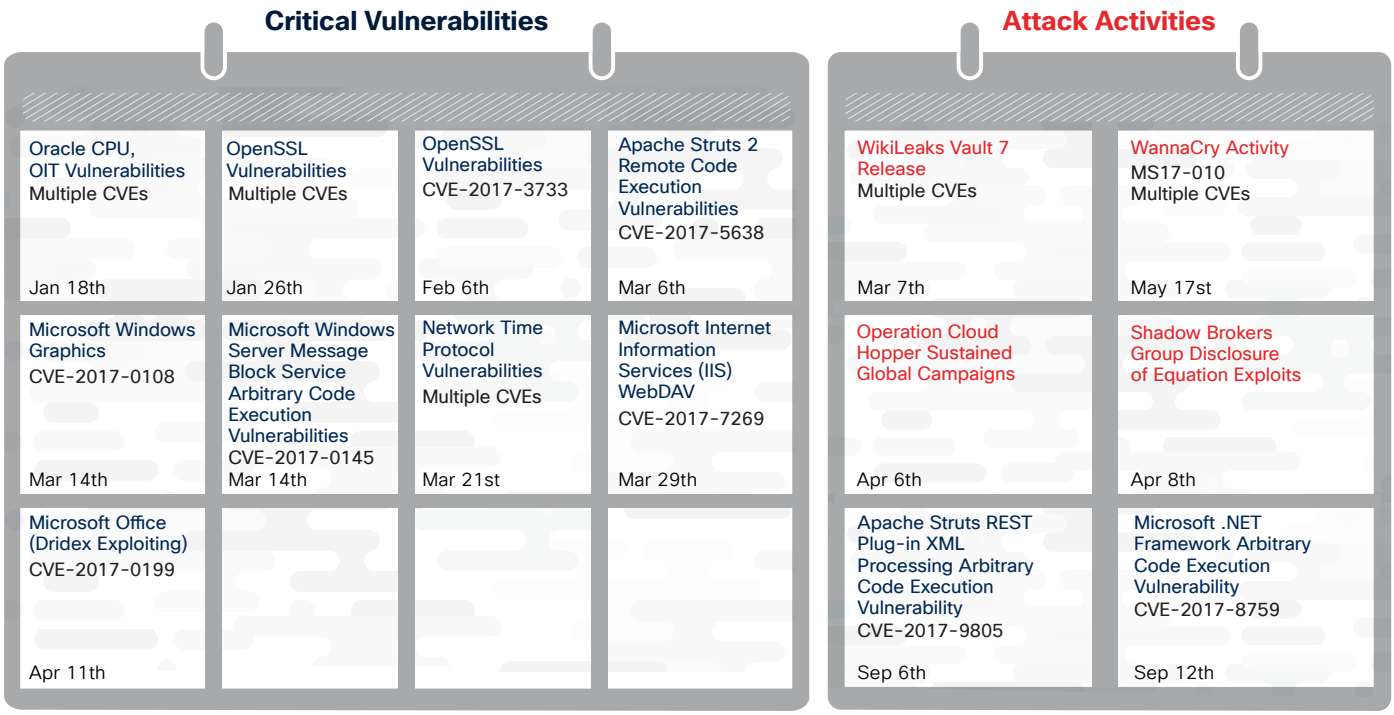
Source: Cisco Security Research

In examining critical advisories (Figure 35), Apache Struts vulnerabilities were still prominent in 2017. Apache Struts is an open-source framework for creating Java applications that is widely used. Apache Struts vulnerabilities were implicated in security breaches in 2017 that involved major data brokers.

While Apache tends to identify vulnerabilities and offer patches quickly, infrastructure solutions such as Apache Struts can be challenging to patch without disrupting network performance. As discussed in previous Cisco security reports,[19] third-party or open-source software vulnerabilities can require manual patching, which may not be done as frequently as automated patching from standard software vendors. That gives malicious actors a greater window of time to launch attacks.

Deep scanning of operating systems down to the library or individual file level can provide organizations with inventories of the components of open-source solutions.

Figure 35 Critical advisories and attack activities



Source: Cisco Security Research

Download the 2018 graphics at: cisco.com/go/acr2018graphics

19 *Cisco 2017 Midyear Cybersecurity Report*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

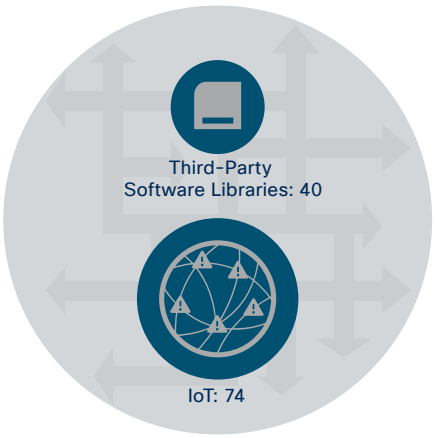
IoT and library vulnerabilities loomed larger in 2017

Between October 1, 2016, and September 30, 2017, Cisco threat researchers discovered 224 new vulnerabilities in non-Cisco products, of which 40 vulnerabilities were related to third-party software libraries included in these products, and 74 were related to IoT devices (Figure 36).

The relatively large number of vulnerabilities in libraries points to the need to delve deeper into third-party solutions that provide the framework for many enterprise networks. Defenders should assume that third-party software libraries can be targets for attackers; it's not enough to simply make sure the latest version of the software is running, or that no open CVEs (common vulnerabilities) have been reported. Security teams should check frequently for patches, and review the security practices of third-party vendors. Teams could, for example, request that vendors provide secure development lifecycle statements.

Another best practice for vetting third-party software is helping to ensure that auto-update or check-for-update features are running securely. For example, when an update is initiated, security professionals should be certain that the communication for that software occurs over a secure channel (such as SSL), and that the software is digitally signed. Both are needed: If only digital signatures are used, but not a secure channel, an attacker could intercept traffic and potentially replace an update with an older version of the software that is digitally signed, but may contain vulnerabilities. If only a secure channel is used, an attacker could potentially compromise the vendor's update server and replace the update with malware.

Figure 36 Third-party library and IoT vulnerabilities



Source: Cisco Security Research

Spectre and Meltdown vulnerabilities: proactive preparation can accelerate remediation

The January 2018 announcement of the Spectre and Meltdown vulnerabilities, which could allow attackers to compromise data on platforms running current-generation computer processors, raised concerns about security professionals' ability to protect data from attacks. The vulnerabilities could allow attackers to view application data in memory on the chipset, with potential for widespread damage, since affected microprocessors are found in everything from mobile phones to server hardware.

The threats posed by the Spectre and Meltdown vulnerabilities highlight the importance of communicating with security organizations about solutions such as patches—as well as ensuring that third-party providers, such as cloud and supply chain vendors, are adhering to best practices for remediating gaps in security posed by such vulnerabilities. Product security incident response teams, or PSIRTs (such as the Cisco PSIRT), are designed to respond quickly to vulnerability announcements, provide patches, and advise customers on how to avoid risks.

Organizations need to plan for vulnerabilities like Spectre and Meltdown to happen, instead of hoping they won't occur. The key is preparing for such announcements, and having systems in place to mitigate potential damage. For example, security teams should proactively inventory devices under their control, and document configurations in features in use, as some vulnerabilities are configuration-dependent and impact security only when certain features are activated.

Security teams should also ask third-party vendors, such as cloud providers, about their update and patching processes. Organizations need to ask for transparency from their cloud providers in terms of how they remediate such vulnerabilities, and how quickly they respond to alerts. But in the end, the responsibility for preparedness falls on the organizations themselves; they must communicate with PSIRT organizations, and establish processes for quickly responding to vulnerabilities.

For more information, read the Talos blog post on Spectre and Meltdown.

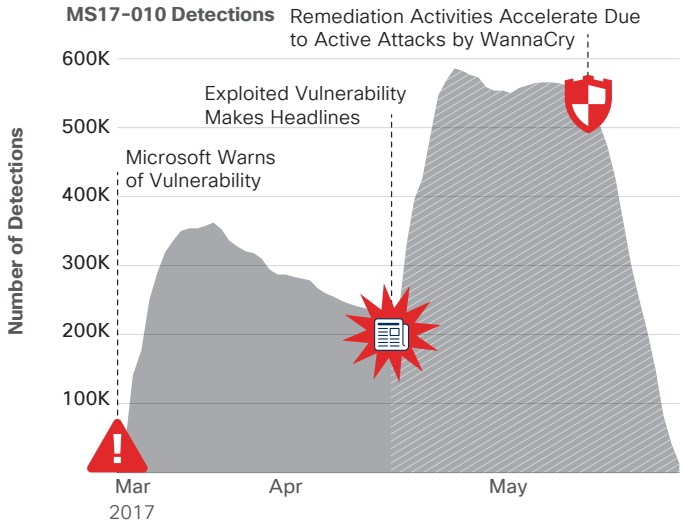
Active exploits fuel race to remediate, except for IoT devices

Qualys, Inc., a Cisco partner and provider of cloud-based security and compliance solutions, took a retrospective look at companies' patch management behavior before and after the WannaCry campaign that affected many organizations across the world in May 2017.

The ransomware cryptoworm WannaCry, which many security experts believe was designed to wipe data, took advantage of a Microsoft Windows security vulnerability called EternalBlue, which was leaked by the hacker group Shadow Brokers in mid-April 2017. (For more on this topic, see "They're out there: Defenders should prepare to face new, self-propagating, network-based threats in 2018," on page 6.)

On March 14, 2017, Microsoft issued a security update (MS17-010) alerting users to a critical vulnerability in its Microsoft Windows SMB Server. Figure 37 shows how the number of devices detected with the vulnerability spikes, and then gradually declines between mid-March and mid-April as organizations scan their systems and apply the patch.

Figure 37 Patching behavior before and after WannaCry campaign



Source: Qualys

Download the 2018 graphics at: cisco.com/go/acr2018graphics

However, a significant number of devices still remained unpatched as of mid-April. Then, on April 14, Shadow Brokers released the working exploit for targeting that known vulnerability in various versions of Microsoft Windows. Figure 37 shows that the number of devices detected with the vulnerability nearly doubled shortly thereafter. That happened as organizations learned of the exploit and its potential to impact both supported and unsupported versions of Windows through a remote check from Qualys that used a portion of the exploit code.

But even after the exploit was released, widespread patching didn't occur until mid-May, after the WannaCry attack made headlines around the world. Figure 37 shows the steep remediation curve after that campaign. By late May, few devices were left unpatched.

Qualys' research into its customers' patching behavior indicates that it takes a major event to motivate many organizations to patch critical vulnerabilites—even knowledge of an active exploit is not enough to accelerate remediation. And in the case of the WannaCry campaign, businesses had access to the patch for the Microsoft vulnerability for two months before the ransomware attacks occurred.

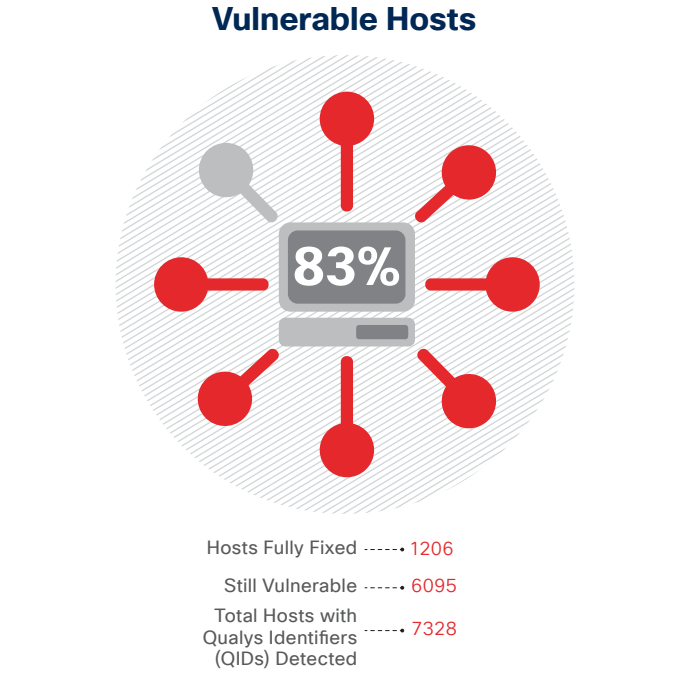
Another factor, as described by researchers with Cisco and Qualys partner Lumeta, was that unknown, unmanaged, rogue, and shadow IT endpoints were left unpatched. Attackers were able to leverage these blind spots. Without knowledge of these systems, vulnerabilty scanners were unable to evaluate and recommend patching of these systems, leaving them vulnerable to WannaCry.

Patching is even slower, or not happening at all, for IoT devices

Qualys also examined patching trends for IoT devices. The devices in the sample included IP-enabled HVAC systems, door locks, fire alarm panels, and card readers.

The researchers looked specifically for IoT devices vulnerable to several known threats, including Devil's Ivy malware that exploits a vulnerability in a piece of code called gSOAP that is widely used in physical security products, and Mirai, an IoT botnet that connects to targeted machines through brute-force attacks against Telnet servers.

Figure 38 IoT device patching trends



Source: Qualys

Qualys detected 7328 devices in total, but only 1206 had been fixed (see Figure 38). That means 83 percent of the IoT devices in the sample still have critical vulnerabilities. While Qualys did not find evidence of threat actors actively targeting those vulnerabilities, organizations were still susceptible to attack. However, they do not seem motivated to speed remediation.

There are several possible explanations for the patching inertia, according to Qualys. Some devices may not be updatable, for example. Others may require direct support from the vendor. Also, it is not always clear who inside the organization is responsible for maintenance of IoT devices. For example, an engineering team that takes care of the company's HVAC system may not be aware of IT risks that could affect that system, or even that the system is IP-enabled.

More concerning, though, is the low number of IoT devices that Qualys detected. The actual number is likely to be much higher because organizations simply do not know how many IoT devices are connected to their network. That lack of visibility puts them at serious risk of compromise (see page 34 for more on this topic).

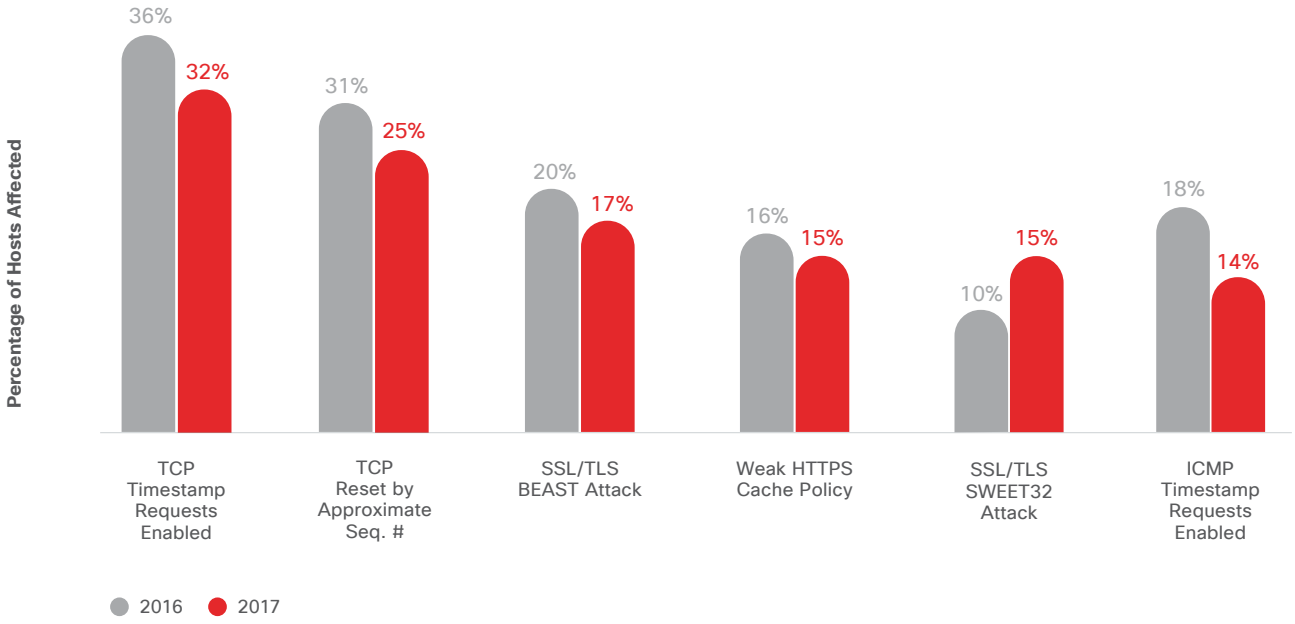
A first step to addressing this issue is inventorying all IoT devices on the network. Organizations can then determine whether the devices are scannable and still supported by vendors, and which employees in the company own and use them. Organizations can also improve IoT security by treating all IoT devices like other computing devices—helping to ensure they receive firmware updates and are patched regularly.

Most common vulnerabilities are low severity but high risk

Low-severity vulnerabilities are often left unremediated for years because companies either don't know they exist or don't consider them significant risks, according to security experts with SAINT Corporation, a security solutions company and Cisco partner. However, these small but significant security gaps could provide adversaries with pathways into systems.

SAINT researchers examined vulnerability exposure data collected from more than 10,000 hosts in 2016 and 2017. The company developed a list of the top vulnerabilities detected most often across all the organizations in the study, which indicated that low-severity vulnerabilities occur most often (see Figure 39). (Note: Some organizations included in the research had more than one host.)

Figure 39 Low-severity vulnerabilities most often detected, 2016-2017



Source: SAINT Corporation

Here's a closer look at the top three low-severity vulnerabilities in Figure 39 and why they might be valuable to threat actors:

TCP timestamp requests enabled
TCP timestamps offer information about how long a machine has been running, or when it was last rebooted, which could help adversaries learn what types of patchable vulnerabilities the machine might have to exploit. Also, software programs may use the system timestamp to seed a random number generator for creating encryption keys.

TCP reset by approximate sequence number
Remote attackers can guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as the Border Gateway Protocol.

"BEAST" attack
An attacker can use the Browser Exploit Against SSL/TLS (BEAST) vulnerability to launch a man-in-the-middle (MiTM) attack to essentially "read" protected content being exchanged between parties. (Note: This is a complicated attack to execute, as the threat actor also must have control of the client-side browser to read and inject data packets very quickly.)

Security researchers with SAINT did not detect adversaries actively exploiting these low-severity vulnerabilities during their analysis.

The vulnerabilities shown in Figure 39 are known to the security community, but some of them would not typically be flagged or lead to automatic failure during a routine compliance check, such as a Payment Card Industry Data Security Standard (PCI DSS) audit. They are not critical vulnerabilities as defined by standards relevant to that industry. Each industry triages the criticality of vulnerabilities differently.

Also, most of the commonly occurring vulnerabilities that are low-severity shown in Figure 39 cannot be remediated easily, or at all, through patch management because they stem from configuration problems or security certificate issues (for example, weak SSL ciphers or a self-signed SSL certificate).

Organizations should act promptly to address low-severity vulnerabilities that may present risk. They should evaluate and identify remediation priorities based on how they perceive the risk, rather than rely on third-party ratings, or partial use of a scoring system, such as a CVSS base score, or a certain compliance rating. Only the organizations know their unique environments and their risk management strategies.

Part II:
The defender landscape

Part II: The defender landscape

We know that attackers are evolving and adapting their techniques at a faster pace than defenders. They are also weaponizing and field testing their exploits, evasion strategies, and skills so they can launch attacks of increasing magnitude. When adversaries inevitably strike their organizations, will defenders be prepared, and how quickly can they recover? That depends largely on the steps they're taking today to strengthen their security posture.

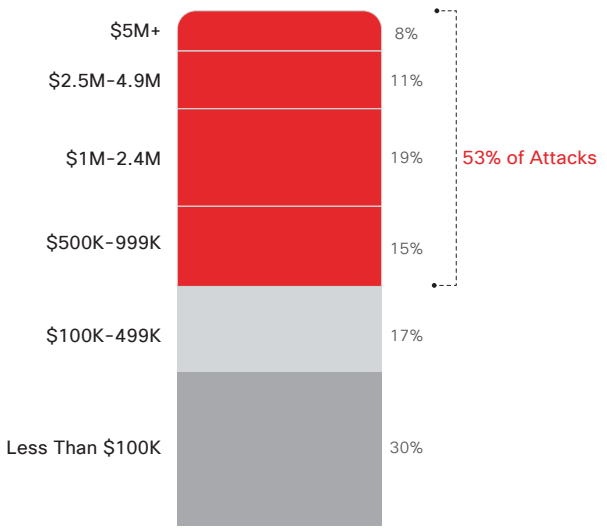
What we've learned through our research for the Cisco 2018 Security Capabilities Benchmark Study *is that defenders have a lot of work to do—and challenges to overcome. To gauge the perceptions of defenders on the state of security in their organizations, we asked chief information security officers (CISOs) and security operations (SecOps) managers in several countries and at organizations of various sizes about their security resources and procedures.*

The Cisco 2018 Security Capabilities Benchmark Study offers insights on security practices currently in use, and compares these results with those of the 2017, 2016, and 2015 studies. The research involved more than 3600 respondents across 26 countries.

The cost of attacks

The fear of breaches is founded in the financial cost of attacks, which is no longer a hypothetical number. Breaches cause real economic damage to organizations, damage that can take months or years to resolve. According to study respondents, more than half (53 percent) of all attacks resulted in financial damages of more than US$500,000, including, but not limited to, lost revenue, customers, opportunities, and out-of-pocket costs (Figure 40).

Figure 40 Fifty-three percent of attacks result in damages of $500,000 or more



Source: Cisco 2018 Security Capabilities Benchmark Study

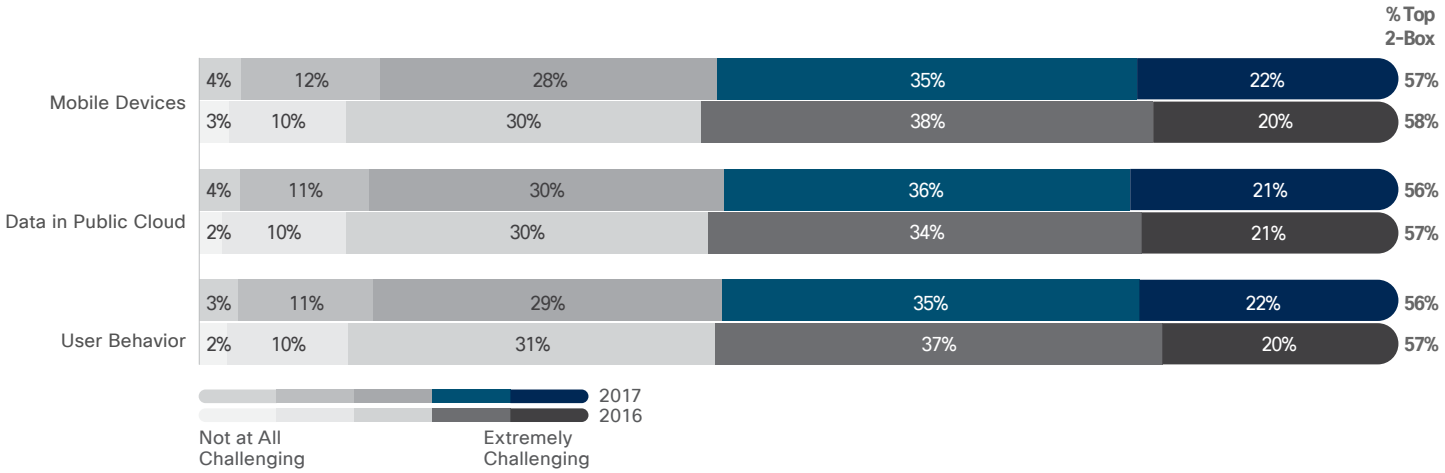
Download the 2018 graphics at: cisco.com/go/acr2018graphics

Challenges and obstacles

In their efforts to protect their organizations, security teams face many roadblocks. Organizations must defend several areas and functions, which adds to security challenges.

The most challenging areas and functions to defend are mobile devices, data in the public cloud, and user behavior (Figure 41).

Figure 41 Most challenging areas to defend: mobile devices and cloud data

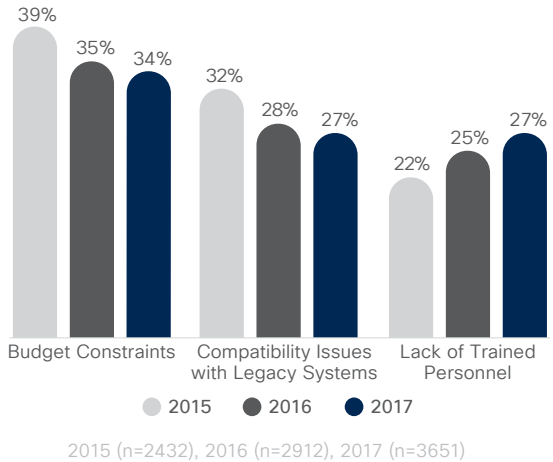


Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

Security professionals cite budget, interoperability, and personnel as their key constraints when managing security (Figure 42). The lack of trained personnel is also named as a challenge to adopting advanced security processes and technology. In 2017, 27 percent cited the lack of talent as an obstacle, compared with 25 percent in 2016 and 22 percent in 2015.

Figure 42 The greatest obstacle to security: budget constraints

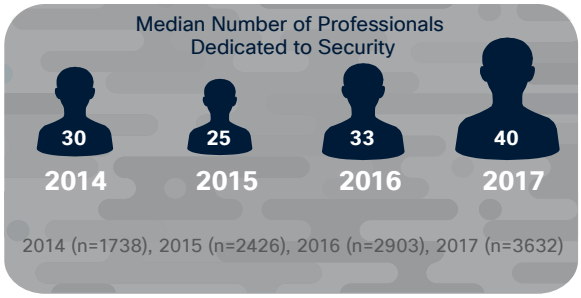


Source: Cisco 2018 Security Capabilities Benchmark Study

Lack of skilled talent tops the list of obstacles in all industries and across all regions. “If I could wave a magic wand and get 10 percent more people to take some of the burden off people who really feel the heat because of high demand for their particular service areas, I would be a very, very happy guy,” said a CISO for a large professional services firm.

While the skilled talent gap is an ongoing challenge, organizations report that they’re seeking out and hiring more resources for their security teams. In 2017, the median number of security professionals at organizations was 40, a significant increase from 2016’s median number of 33 (Figure 43).

Figure 43 Organizations hire more security professionals



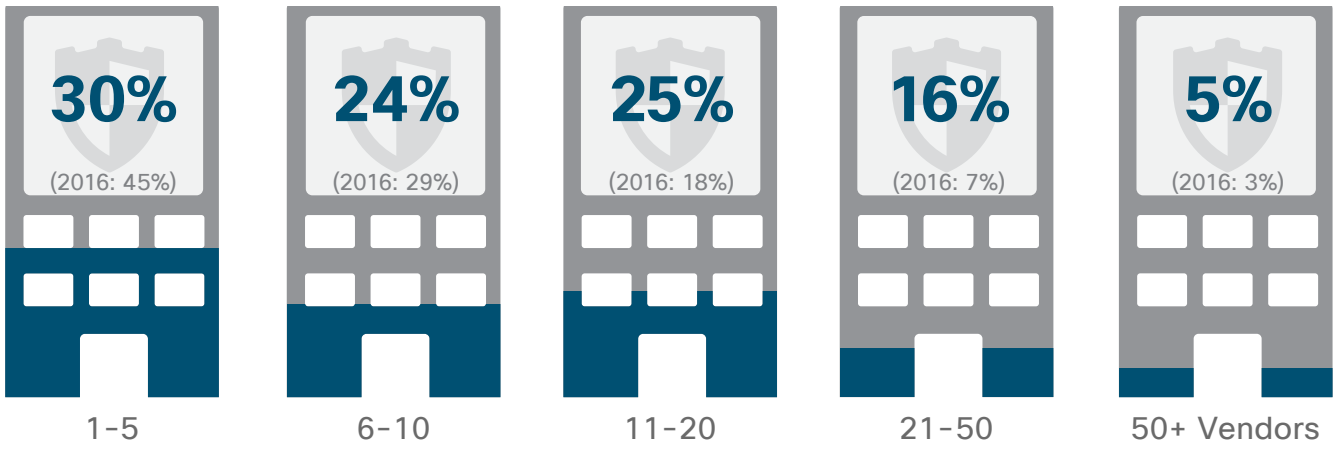
Source: Cisco 2018 Security Capabilities Benchmark Study

Complexity created by vendors in orchestration

Defenders are implementing a complex mix of products from a cross-section of vendors: an arsenal of tools that may obfuscate rather than clarify the security landscape. This complexity has many downstream effects on an organization's ability to defend against attacks, such as increased risk of losses.

In 2017, 25 percent of security professionals said they used products from 11 to 20 vendors, compared with 18 percent of security professionals in 2016. Also in 2017, 16 percent said they use anywhere from 21 to 50 vendors, compared to 7 percent of respondents in 2016 (Figure 44).

Figure 44 Organizations used more security vendors in 2017

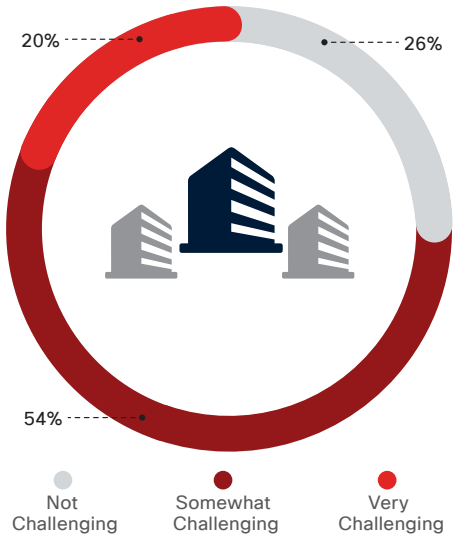


Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

As the number of vendors increases, so does the challenge of orchestrating alerts from these many vendor solutions. As seen in Figure 45, 54 percent of security professionals said that managing multiple vendor alerts is somewhat challenging, while 20 percent said it is very challenging.

Figure 45 The challenge of orchestrating alerts



Source: Cisco 2018 Security Capabilities Benchmark Study

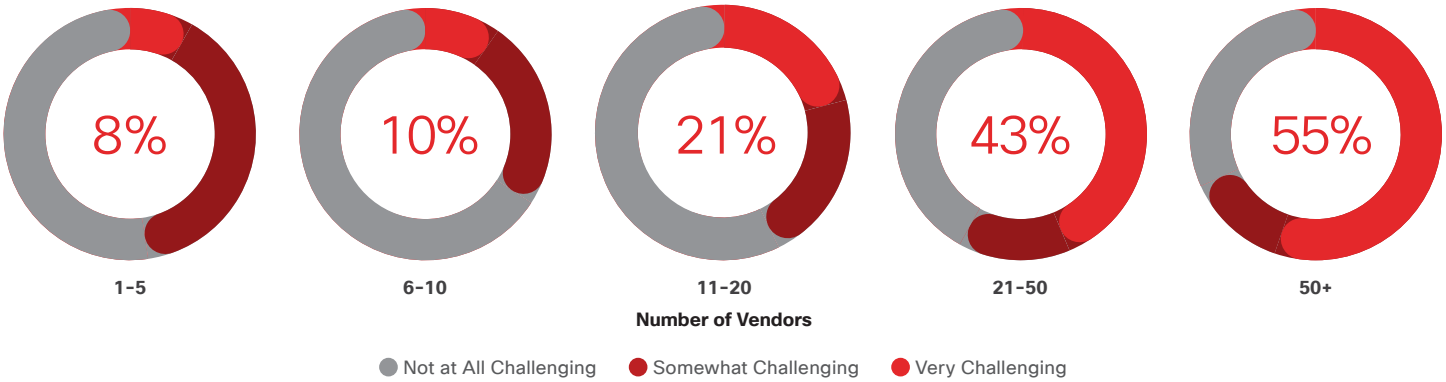
Security teams face challenges in orchestrating multiple vendor alerts

As seen in Figure 46, among organizations with just 1 to 5 vendors, 8 percent said orchestrating alerts is very challenging.

Among organizations using more than 50 vendors, 55 percent said such orchestration is very challenging.

When organizations can't orchestrate and understand the alerts they receive, legitimate threats can slip through the cracks.

Figure 46 As vendors increase, so does the challenge of orchestrating security alerts



	Education	Financial Services	Government	Healthcare	Manufacturing	Pharma	Retail	Telecom	Transportation	Utility/ Energy
Very Challenging	17%	24%	16%	42%	14%	25%	19%	14%	12%	27%

Source: Cisco 2018 Security Capabilities Benchmark Study

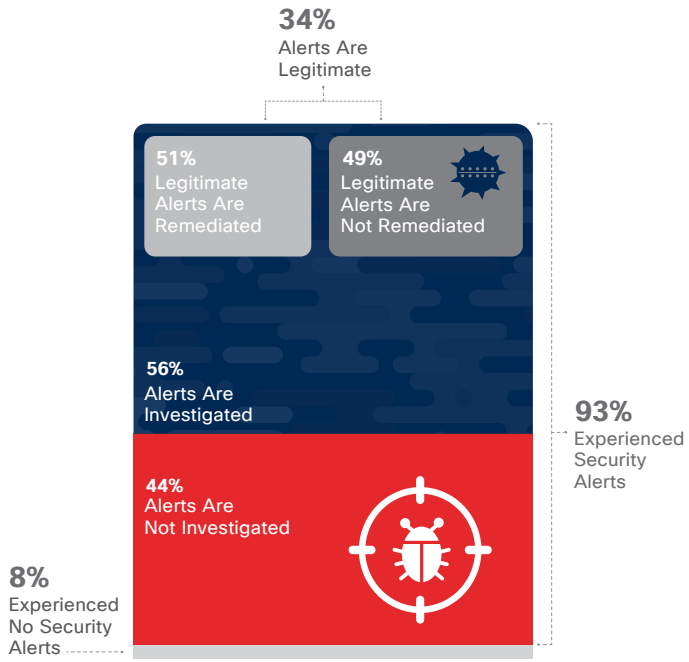
Download the 2018 graphics at: cisco.com/go/acr2018graphics

Respondent data indicates that gaps continue to exist between alerts generated, those that have been investigated, and those that are eventually remediated. As shown in Figure 47:

- Among organizations that receive daily security alerts, an average of 44 percent of those alerts are not investigated.
- Of those alerts investigated, 34 percent are deemed legitimate.
- Of those deemed legitimate, 51 percent of alerts are remediated.
- Nearly half (49 percent) of legitimate alerts are not remediated.

This process leaves many legitimate alerts unremediated. One reason appears to be the lack of headcount and trained personnel who can facilitate the demand to investigate all alerts.

Figure 47 Many threat alerts are not investigated or remediated

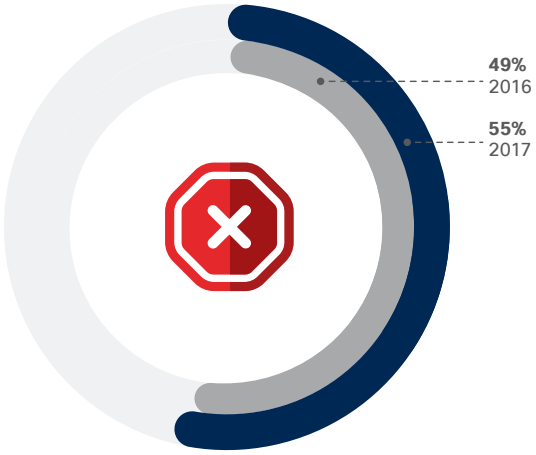


Source: Cisco 2018 Security Capabilities Benchmark Study

Impact: Public scrutiny from breaches, higher risk of losses

"There are two kinds of companies: those who have been breached and those who don't know they've been breached," said a benchmark study respondent. (The response echoes a well-known quote from former Cisco CEO John Chambers: "There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.") Even though organizations are trying to meet future security challenges with adequate preparation, security professionals expect they'll fall victim to a breach that receives public scrutiny. Fifty-five percent of respondents said their organizations had to manage public scrutiny of a breach in the last year (Figure 48).

Figure 48 Fifty-five percent of organizations have had to manage the public scrutiny of a breach



2016 (n=2824), 2017 (n=3548)

Source: Cisco 2018 Security Capabilities Benchmark Study

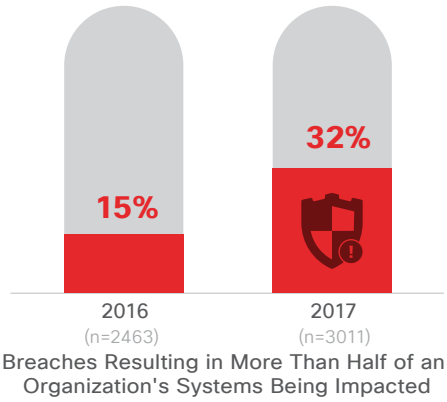
Download the 2018 graphics at: cisco.com/go/acr2018graphics

> *"The norm is going to be that almost every Fortune 500 company has been breached within the last 24 months. You have to be prepared for that, especially from a marketing perspective or a PR perspective."*
>
> *–Benchmark study respondent*

Organizations reported significantly more security breaches affecting over 50 percent of systems (Figure 49), than did the organizations responding last year. In 2017, 32 percent of security professionals said breaches affected more than half of their systems, compared with 15 percent in 2016. The business functions most commonly affected by breaches are operations, finance, intellectual property, and brand reputation (Figure 50).

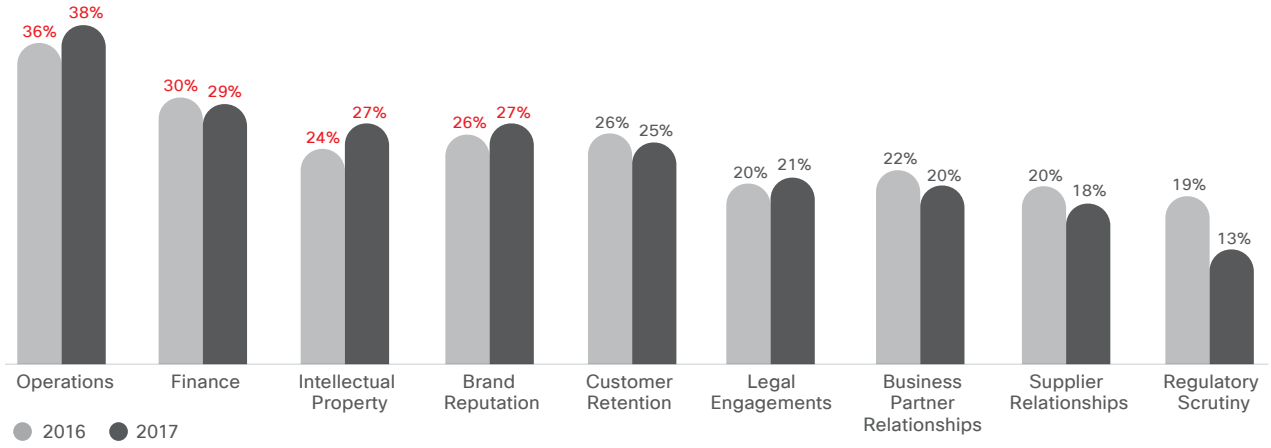
In complex security environments, organizations are more likely to deal with breaches. Of organizations using 1 to 5 vendors, 28 percent said they had to manage public scrutiny after a breach; that number rose to 80 percent for organizations using more than 50 vendors (Figure 51). That may be due to increased visibility into threats, which more products may allow.

Figure 49 Sharp increase in security breaches affecting more than 50 percent of systems



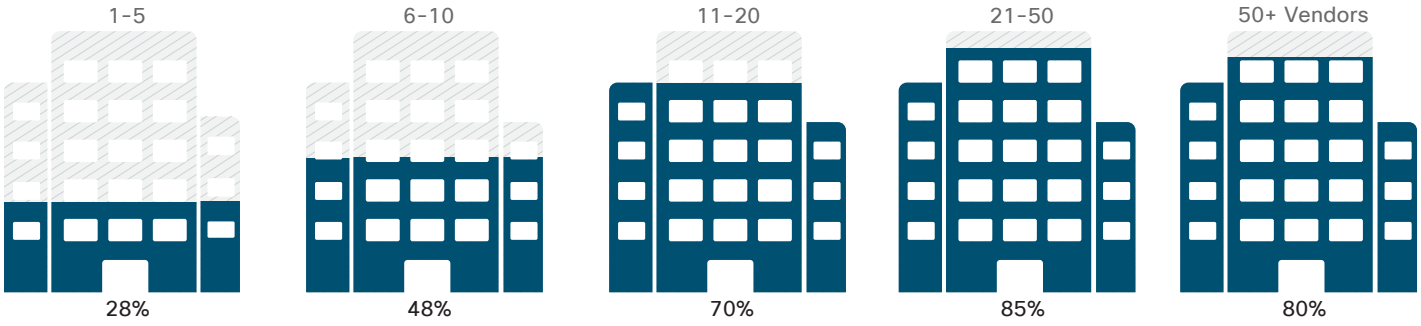
Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 50 Operations and finance are most likely to be affected by security breaches



Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 51 Eighty percent of organizations using more than 50 vendors had to manage scrutiny from public breaches



Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

The value of an integrated framework

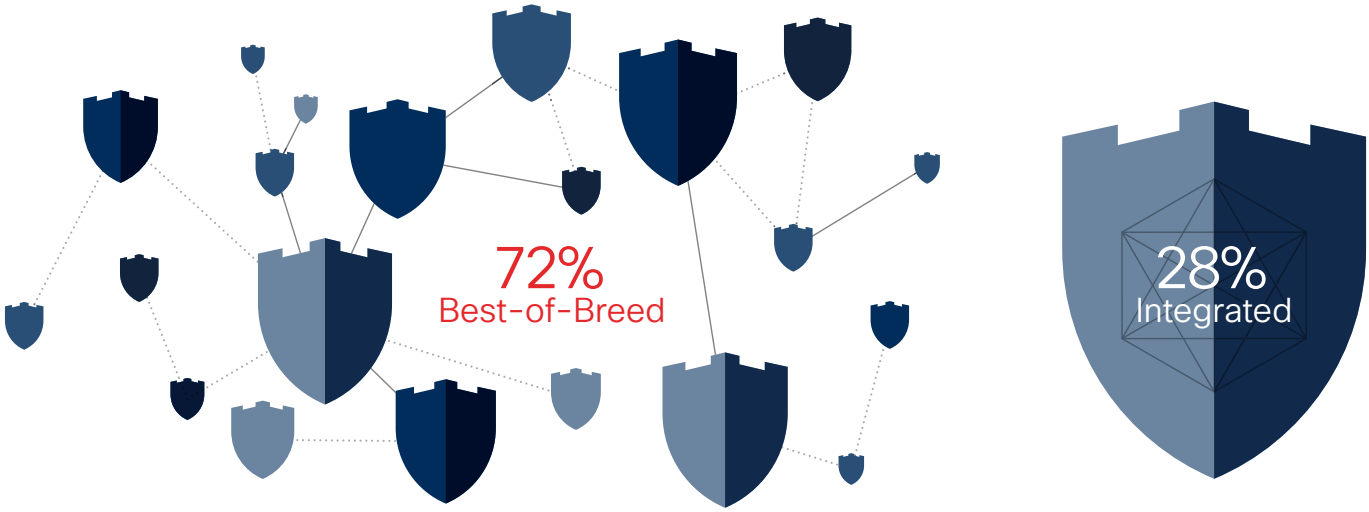
Why use a multitude of products from many vendors if the resulting environment is difficult to manage? The best-of-breed approach, in which security teams choose the best solution for each security need, is one key reason. Security professionals who practice the best-of-breed approach also believe it's more cost-effective, according to research for the benchmark study.

When comparing best-of-breed to integrated solutions, 72 percent of security professionals said they buy best-of-breed point solutions to meet specific needs, compared with 28 percent who buy products intended to work together as an integrated solution (see Figure 52). Of the organizations that adopt a best-of-breed approach, 57 percent cite cost-effectiveness, while 39 percent said the best-of-breed approach is easier to implement.

Interestingly, organizations that adopt an integrated approach to security cite similar reasons for their choice. Fifty-six percent said an integrated approach is more cost-effective. Forty-seven percent said it's easier to implement.

Ease of implementation is increasingly cited as a factor for using an integrated architecture approach: Only 33 percent of organizations said ease of implementation was a reason to choose an integrated approach in 2016, compared to 47 percent in 2017. While single-vendor solutions may not be practical for all organizations, buyers of security solutions must help ensure that solutions work together to reduce risk and increase efficacy.

Figure 52 Seventy-two percent buy best-of-breed solutions because they meet specific needs



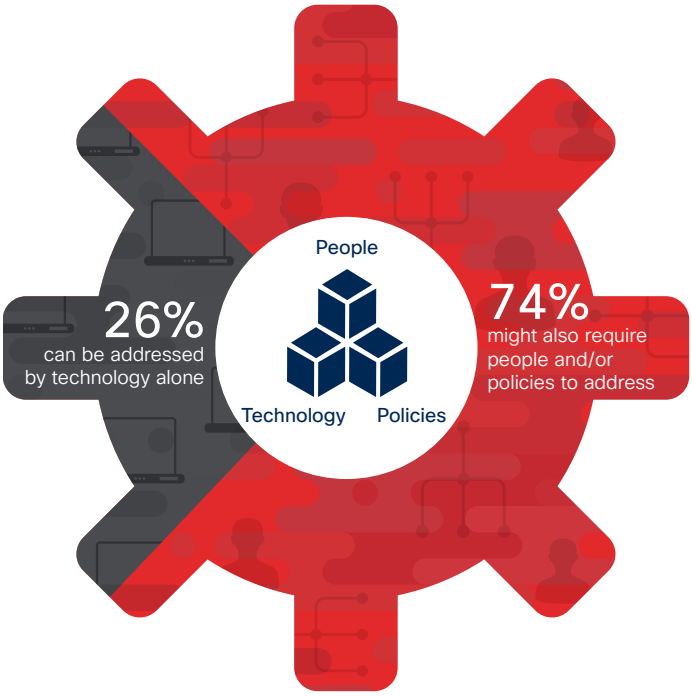
Source: Cisco 2018 Security Capabilities Benchmark Study

Services: Addressing people and policies, as well as technology

Faced with potential losses and adverse impact on systems, organizations need to move beyond relying solely on technology for defense. That means examining other opportunities to improve security, such as applying policies or training users. This holistic approach to security can be seen in the issues identified during an Intelligence Lead Security Assurance (known as a "Red Team" assessment) provided by the Cisco Advanced Services Security Advisory team.

In examining recommendation data from several Red Team assessments carried out in 2017, services team members identified three key defensive capabilities: people, policies, and technology. If an organization were to use technology alone to remediate security vulnerabilities, it would only solve 26 percent of issues that were identified during Red Team attack simulations. That would leave 74 percent of issues unresolved (see Figure 53). Likewise, if organizations use only policies to address security issues, they would resolve just 10 percent of issues; with user training for people, only 4 percent of issues. The three areas of defense need to be tackled in concert.

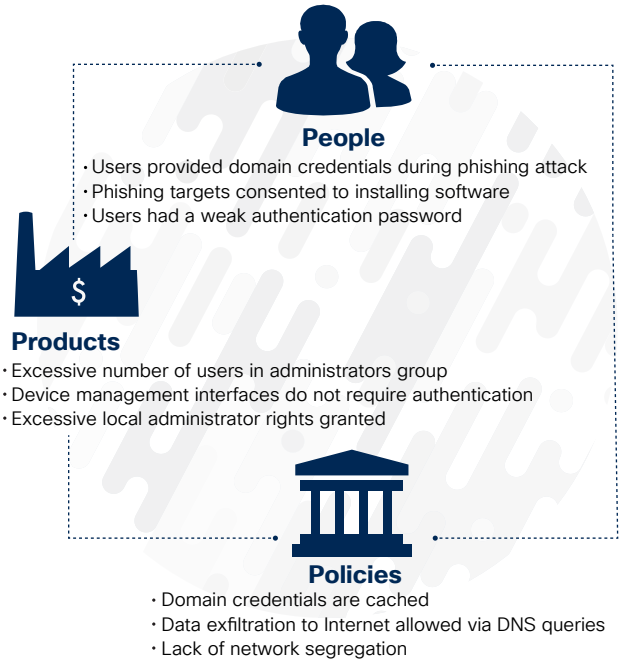
Figure 53 Only 26 percent of security issues can be addressed by products alone



Source: Cisco Security Research

Figure 54 offers examples of issues identified by category during the simulations. Some issues, such as weak passwords, cross over all three categories. Strengthening passwords can require improvements in people (user training), products (configuring servers for more complex passwords), and policies (setting stronger password requirements).

Figure 54 Types of issues uncovered during attack simulations categorized by remediation requirements



Source: Cisco Security Research

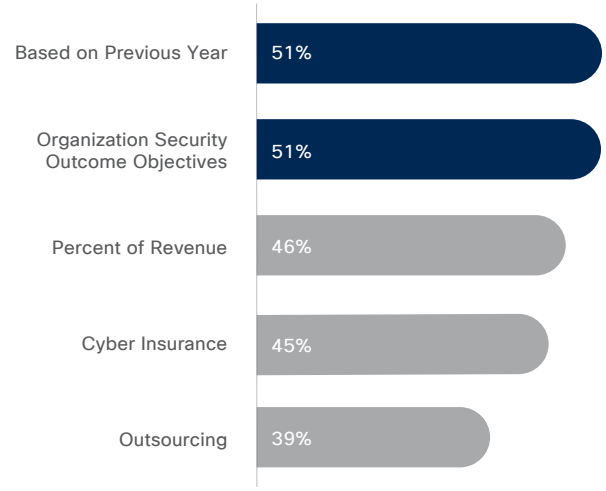
Organizations can increase their odds of successfully managing all three factors if they help ensure that security is embedded into every layer of the organization—not bolted on here and there. They should also avoid relying solely on products or technical improvements to fix security. For products to be successful, organizations need to understand and implement sensible policies and processes for the technology.

Expectations: Investing in technology and training

Security professionals fully anticipate that the threats facing their organizations will remain complex and challenging. They expect bad actors to develop more sophisticated and damaging ways to breach networks. They also know that the modern workplace creates conditions that favor the attackers: The mobility of employees and adoption of IoT devices provide attackers with fresh opportunities. Along with increased threats, many security professionals expect they'll be under additional scrutiny—from regulators, executives, stakeholders, partners, and clients.

To reduce the likelihood of risk and losses, defenders must determine where to invest finite resources. For the most part, security professionals said that security budgets remain relatively stable, unless a major public breach drives a rethink of, and new expenditures for, technology and processes. Fifty-one percent said security spending is based on previous years' budgets, while an equal percentage of respondents said outcome objectives drive budget (Figure 55). Most security leaders said they believe their companies are spending appropriately on security.

Figure 55 Fifty-one percent said security spending is driven by previous years' budgets

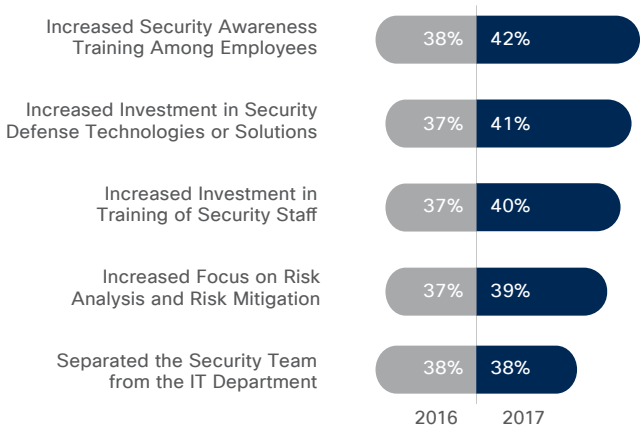


Source: Cisco 2018 Security Capabilities Benchmark Study

When planning budgets, many companies systematically work through wish lists developed as part of comprehensive security plans, prioritizing investments as resources become available. Investments may be reset if new vulnerabilities are exposed, whether by an internal incident, a highly publicized public breach, or a routine third-party risk assessment.

The most important factors driving future investment, and therefore improvements in technology and processes, appear to be breaches. In 2017, 41 percent of security professionals said that security breaches are driving increased investment in security technologies and solutions, up from 37 percent in 2016 (Figure 56). Forty percent said breaches are driving increased investment in the training of security staff, compared with 37 percent in 2016.

Figure 56 Security breaches are driving investment in technology and training



2016 (n=1375), 2017 (n=1933)

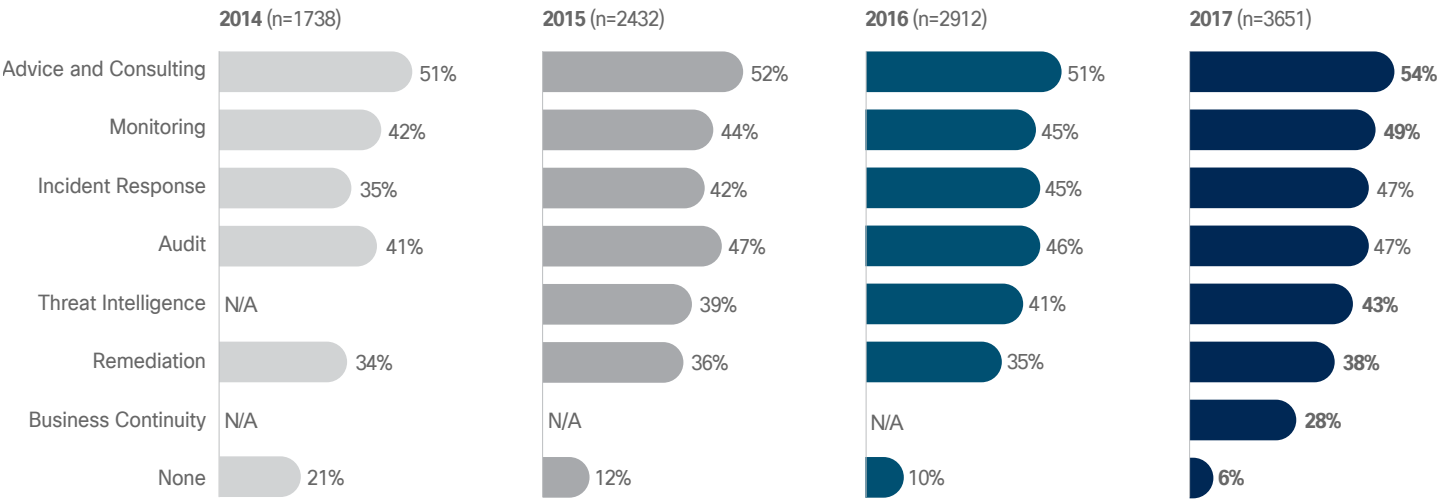
Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

Security professionals expect to spend more on tools that use artificial intelligence and machine learning in a bid to improve defenses and help shoulder the workload. In addition, they plan to invest in tools that will provide safeguards for critical systems, such as critical infrastructure services.

To stretch resources and strengthen defenses, organizations are stepping up their reliance on outsourcing. Among security professionals, 49 percent said they outsourced monitoring services in 2017, compared with 44 percent in 2015; 47 percent outsourced incident response in 2017, compared with 42 percent in 2015 (Figure 57).

Figure 57 Use of outsourcing for monitoring and incident response is growing year over year



Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

For more results from the Cisco 2018 Security Capabilities Benchmark Study, see the Appendix on **page 64**.

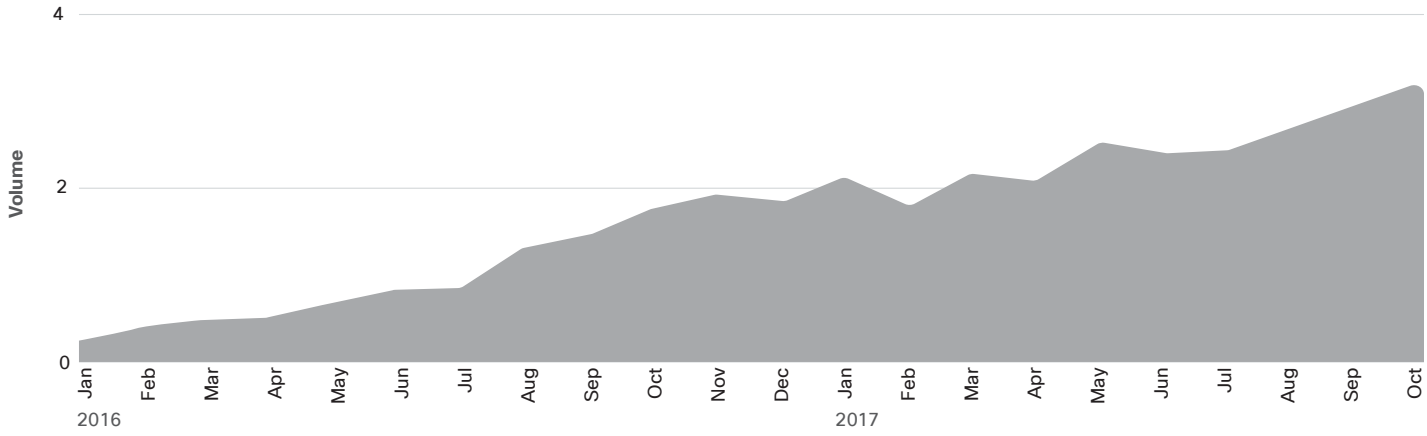
Conclusion

Conclusion

In the modern threat landscape, adversaries are adept at evading detection. They have more effective tools, like encryption, and more advanced and clever tactics, such as the abuse of legitimate Internet services, to conceal their activity and undermine traditional security technologies. And they are constantly evolving their tactics to keep their malware fresh and effective. Even threats known to the security community can take a long time to identify.

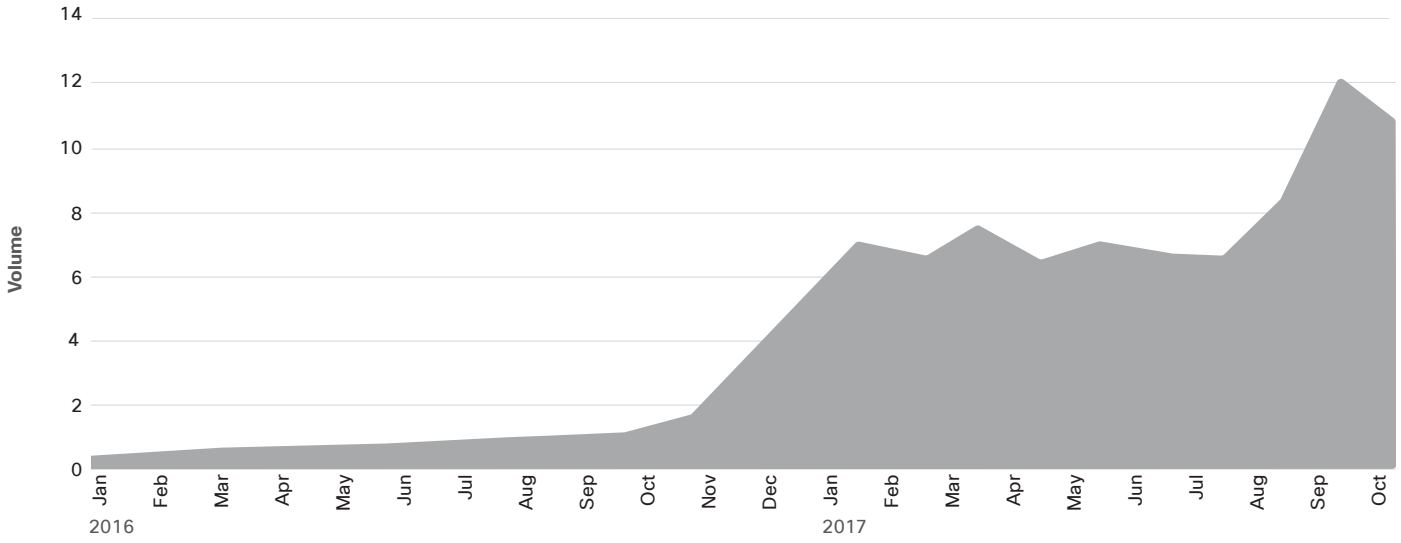
One reason defenders struggle to rise above the chaos of war with attackers, and truly see and understand what's happening in the threat landscape, is the sheer volume of potentially malicious traffic they face. Our research shows that the volume of total events seen by Cisco cloud-based endpoint security products increased fourfold from January 2016 through October 2017 (see Figure 58). "Total events" is the count of all events, benign or malicious, seen by our cloud-based endpoint security products during the period observed.

Figure 58 Total volume of events



Source: Cisco Security Research

Figure 59 Overall malware volume



Source: Cisco Security Research

Our security products also saw an elevenfold increase in overall malware volume during that same period, as Figure 59 shows.

Trends in malware volume have an impact on defenders' time to detection (TTD), which is an important metric for any organization to understand how well its security defenses are performing under pressure from the constant barrage of malware deployed by adversaries.

The Cisco median TTD of about 4.6 hours for the period from November 2016 to October 2017 helps to illustrate the ongoing challenge of identifying threats quickly in the chaotic threat landscape. Still, that figure is well below the 39-hour median TTD we reported in November 2015, after we first began tracking TTD, and the 14-hour median reported in the *Cisco 2017 Annual Cybersecurity Report* for the period from November 2015 to October 2016.[20]

The use of cloud-based security technology has been a key factor in helping Cisco to drive and keep its median TTD at a low level. The cloud helps to scale and maintain performance as both the volume of total events and malware targeting endpoints continues to increase. On-premises security solutions would struggle to offer the same flexibility. Designing one to scale that could handle more than 10 times the volume capacity of malicious events over a two-year period—and maintain or increase response times—would be a very difficult and costly undertaking for any organization.

Cisco defines "time to detection," or TTD, as the window of time between a compromise and the identification 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 are able to measure from the moment a malicious file is downloaded on an endpoint to the time it is determined to be a threat that was unclassified at the time of encounter.

"Median TTD" is the average of the monthly medians for the period observed.

20 *Cisco 2017 Annual Cybersecurity Report:* cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html.

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. Our 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 track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, and 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 our threat-centric approach to security, visit cisco.com/go/security.

CISCO 2018 ANNUAL CYBERSECURITY REPORT CONTRIBUTORS

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 2018 Annual 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 develop simple, open, and automated security that allows organizations to integrate the solutions they need to secure their environments.

Cisco Advanced Malware Protection (AMP) for Endpoints

Cisco AMP for Endpoints provides automated prevention, detection, and response capabilities in a single solution. It continuously monitors and analyzes for signs of malicious activity to uncover threats that bypass frontline security, and pose the greatest risk to organizations. It uses a variety of detection techniques including advanced sandboxing, exploit prevention, as well as machine learning to rapidly detect and mitigate threats. Cisco AMP for Endpoints is the only solution that provides retrospective security to quickly respond to threats and identify the scope, point of origin, and how to contain the threat so organizations stay protected.

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 Cognitive Threat Analytics

Cisco 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.

Cisco Product Security Incident Response Team (PSIRT)

The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global organization that manages the receipt, investigation, and public disclosure of information about security vulnerabilities and issues related to Cisco products and networks. PSIRT receives reports from independent researchers, industry organizations, vendors, customers, and other sources concerned with product or network security.

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 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.

Cisco Talos Intelligence Group

Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts, and engineers. These teams are supported by unrivaled telemetry and sophisticated systems to create accurate, rapid, and actionable threat intelligence for Cisco customers, products, and services. Talos Group defends Cisco customers against known and emerging threats, discovers new vulnerabilities in common software, and interdicts threats in the wild before they can further harm the Internet at large. Talos intelligence is at the core of Cisco products that detect, analyze, and protect against known and emerging threats. Talos maintains the official rule sets of Snort.org, ClamAV, and SpamCop in addition to releasing many open-source research and analysis tools.

Cisco Threat Grid

Cisco Threat Grid is a malware analysis and threat intelligence platform. Threat Grid performs static and dynamic analysis on suspected malware samples that are sourced from customers and product integrations located all over the world. Hundreds of thousands of samples, in a variety of file types, are submitted to the Threat Grid Cloud every day through the Threat Grid Cloud portal user interface, or by Threat Grid API. Threat Grid can also be deployed as an on-site appliance.

Cisco Umbrella

Cisco Umbrella is a secure Internet gateway that provides the first line of defense against threats on the Internet wherever users go. Because it is built into the foundation of the Internet, Umbrella delivers complete visibility into activity across all locations, devices, and users. By analyzing and learning from this activity, Umbrella automatically uncovers attacker infrastructure staged for current and emerging threats, and proactively blocks requests before a connection is established.

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 Cisco 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 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

The Cisco Security and Trust Organization underscores our 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 public and private customers, helping to enable and ensure Secure Development Lifecycle and Trustworthy Systems efforts across the Cisco 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.

Cisco 2018 Annual 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.

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 above any other solution on the market today, as well as real-time network and endpoint monitoring to detect unauthorized changes, prevent leak paths, ensure proper network segmentation, and detect suspicious network behaviors across dynamic network elements, endpoints, virtual machines, and cloud-based infrastructure. For more information, visit lumeta.com.

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.

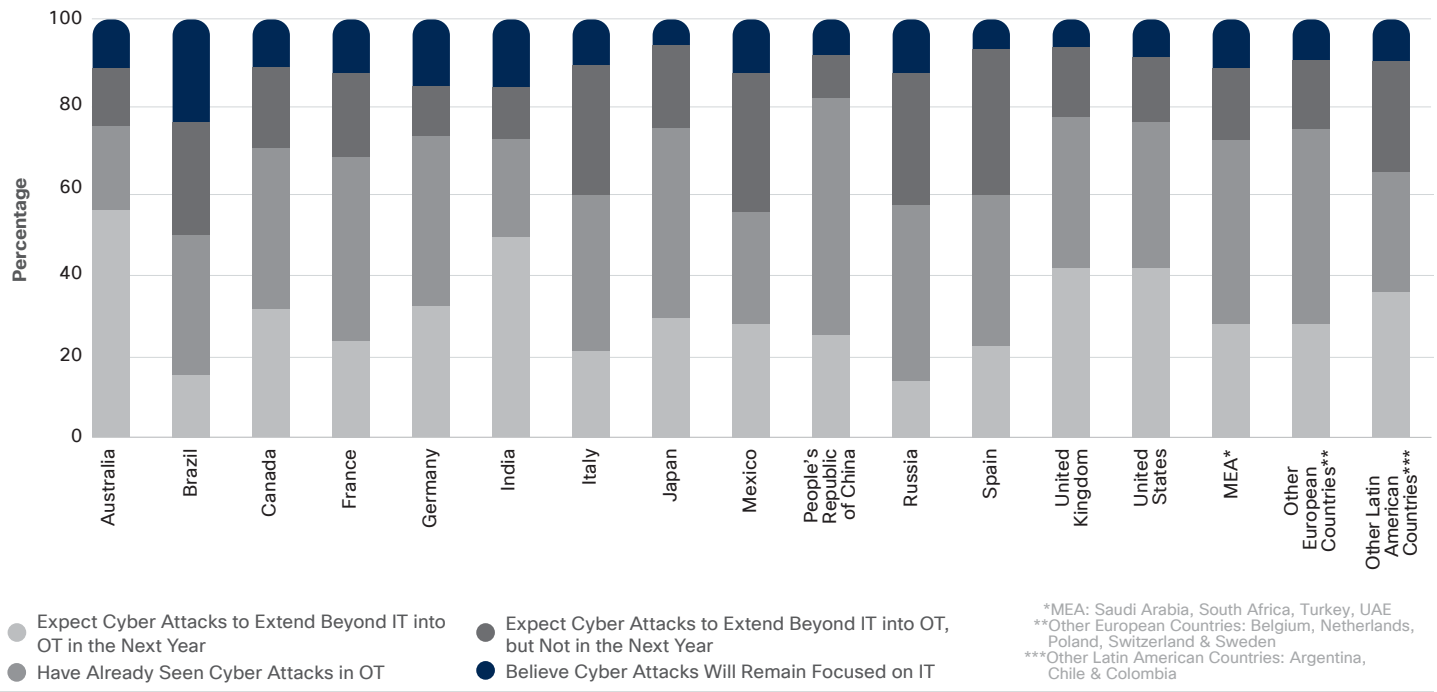
Radware (NASDAQ: RDWR) is a global leader of application delivery and cybersecurity solutions for virtual, cloud, and software-defined data centers. Its award-winning solutions portfolio delivers service-level assurance for more than 10,000 enterprises and carriers worldwide. For additional expert security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

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.

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.

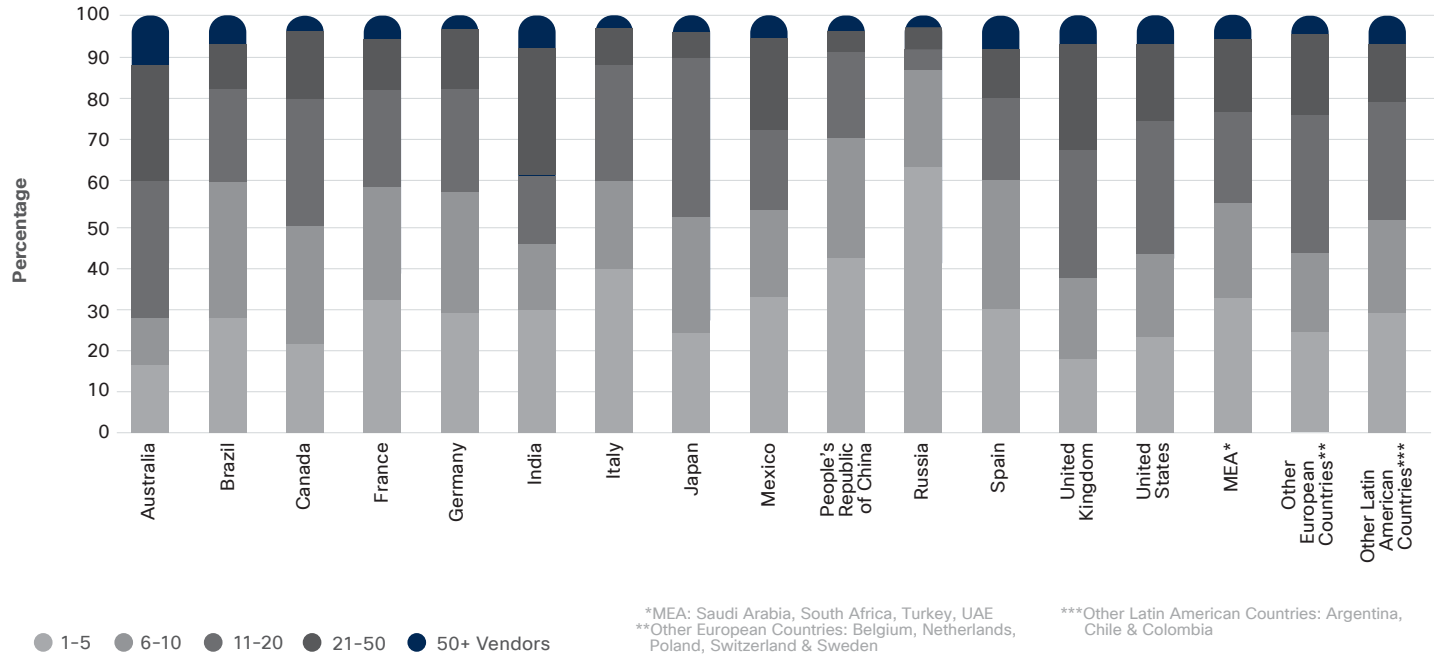
Appendix

Figure 60 Expectations for cyber attacks in OT and IT, by country or region



Source: Cisco 2018 Security Capabilities Benchmark Study

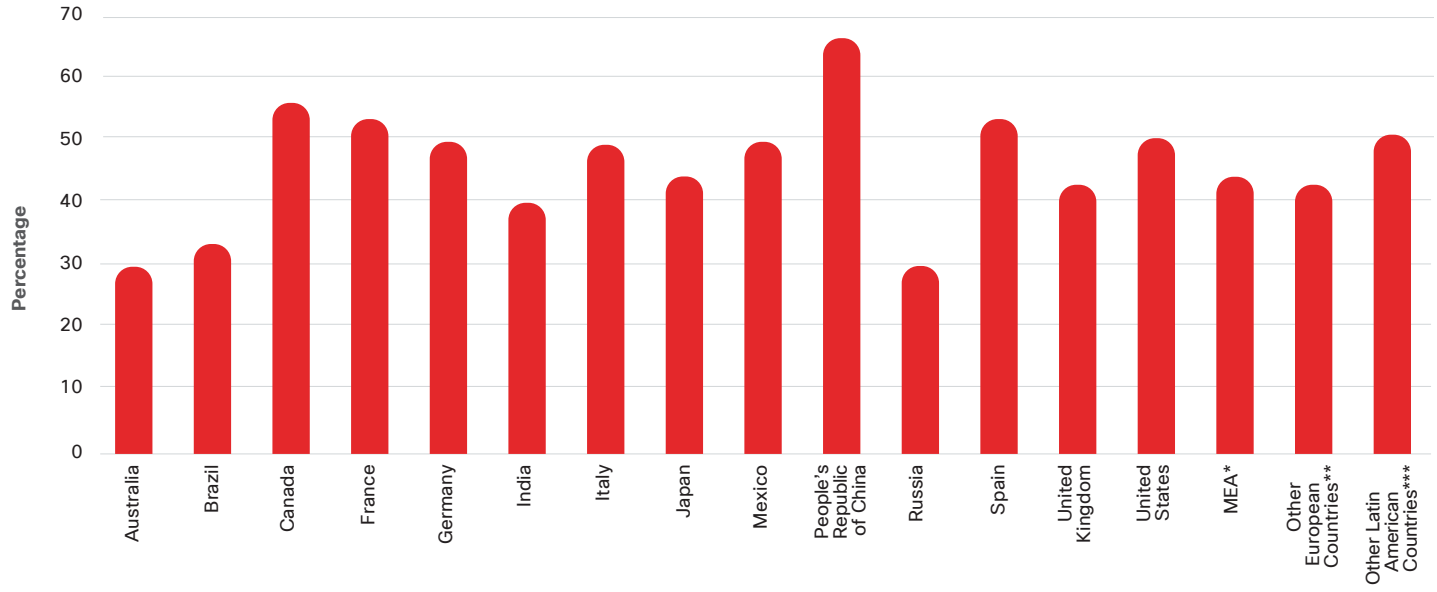
Figure 61 Number of security vendors in environment, by country or region



Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

Figure 62 Percent of alerts uninvestigated, by country or region



*MEA: Saudi Arabia, South Africa, Turkey, UAE **Other European Countries: Belgium, Netherlands, Poland, Switzerland & Sweden ***Other Latin American Countries: Argentina, Chile & Colombia

Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 63 Obstacles to adopting advanced security processes and technology, by country or region

Which of the following do you consider the biggest obstacles to adopting advanced security processes and technology?

	Australia	Brazil	Canada	France	Germany	India	Italy	Japan	Mexico	People's Republic of China	Russia	Spain	UK	US	MEA*	Other European Countries**	Other Latin American Countries***
Budget constraints	23%	35%	29%	33%	25%	36%	38%	31%	31%	38%	60%	33%	27%	34%	36%	37%	35%
Competing priorities	28%	11%	29%	27%	28%	26%	24%	27%	16%	27%	20%	18%	32%	32%	25%	18%	24%
Lack of trained personnel	25%	28%	19%	22%	24%	31%	24%	28%	30%	25%	35%	33%	31%	26%	25%	23%	26%
Lack of knowledge about advanced security processes and technology	26%	26%	24%	21%	22%	24%	21%	26%	23%	29%	18%	21%	27%	22%	22%	17%	21%
Compatibility issues with legal systems	27%	19%	30%	27%	30%	30%	22%	23%	32%	40%	25%	25%	24%	28%	30%	25%	28%
Certification requirements	33%	27%	29%	29%	24%	27%	27%	22%	27%	23%	22%	27%	27%	30%	24%	33%	21%
Organizational culture/ attitude about security	30%	23%	25%	20%	16%	26%	17%	21%	26%	17%	19%	24%	28%	25%	20%	20%	27%
Reluctant to purchase until they are proven in the market	19%	20%	23%	26%	25%	29%	20%	28%	15%	16%	17%	20%	21%	22%	22%	21%	25%
Current workload too heavy to take on new responsibilites	22%	16%	28%	18%	28%	28%	26%	27%	23%	21%	15%	28%	22%	22%	20%	17%	19%
Organization is not a high-value target for attacks	25%	18%	21%	22%	24%	17%	14%	20%	12%	16%	11%	13%	21%	21%	21%	20%	16%
Security is not an executive-level priority	22%	10%	17%	17%	20%	13%	13%	23%	15%	18%	11%	11%	19%	19%	17%	19%	21%

*MEA: Saudi Arabia, South Africa, Turkey, UAE **Other European Countries: Belgium, Netherlands, Poland, Switzerland & Sweden ***Other Latin American Countries: Argentina, Chile & Colombia

Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

Figure 64 Purchase of security threat solutions, by country or region

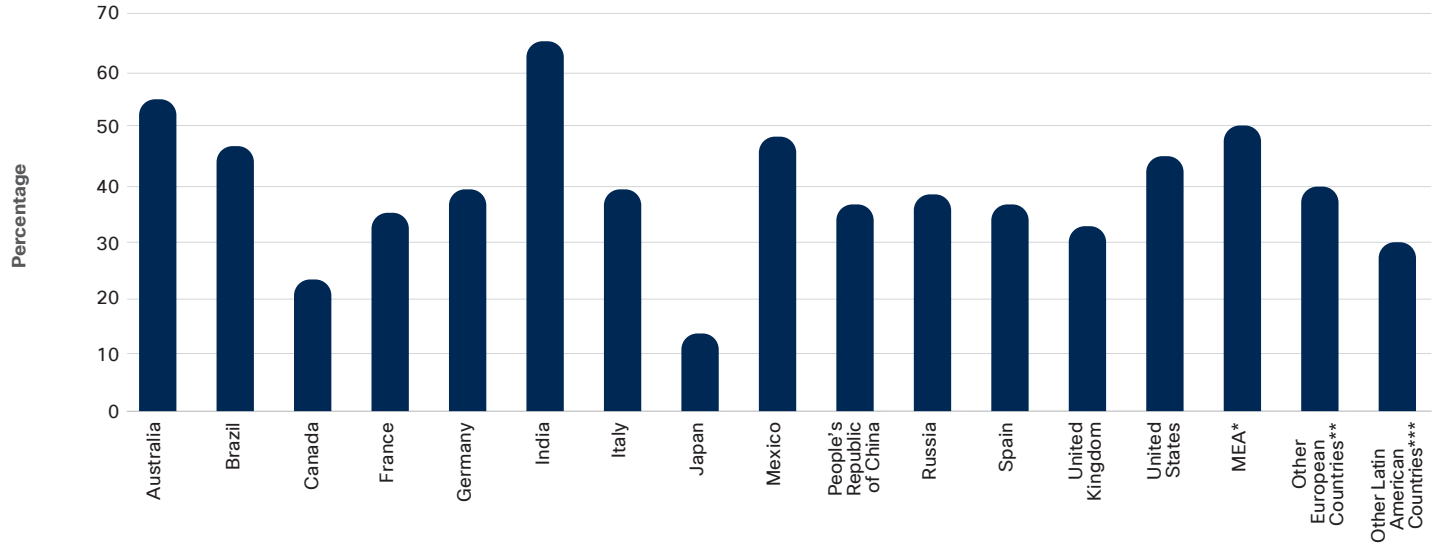
Which best describes how your organization purchases security threat defense solutions?

Country	N=	Typically Buy Best-of-Breed Point Products to Meet Specific Needs	Typically Buy Products That Are Designed to Work Together
Australia	203	86	14
Brazil	197	72	28
Canada	185	67	33
France	191	59	41
Germany	195	69	31
India	199	78	22
Italy	201	71	29
Japan	223	72	28
Mexico	198	77	23
People's Republic of China	205	63	37
Russia	196	58	42
Spain	148	70	30
United Kingdom	194	76	24
United States	393	81	19
MEA*	249	69	31
Other European Countries**	199	73	27
Other Latin American Countries***	196	71	29

*MEA: Saudi Arabia, South Africa, Turkey, UAE **Other European Countries: Belgium, Netherlands, Poland, Switzerland & Sweden ***Other Latin American Countries: Argentina, Chile & Colombia

Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 65 Percent of organizations perceiving they follow standardized infosec framework very well, by country or region



*MEA: Saudi Arabia, South Africa, Turkey, UAE **Other European Countries: Belgium, Netherlands, Poland, Switzerland & Sweden ***Other Latin American Countries: Argentina, Chile & Colombia

Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

Download the graphics

All the graphics in this report are downloadable at: cisco.com/go/mcr2018graphics.

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 February 2018