Cisco 2016
Midyear Cybersecurity Report

Table of Contents

EXECUTIVE SUMMARY AND MAJOR FINDINGS 2

INTRODUCTION 5

CYBERCRIME TREND SPOTLIGHT: RANSOMWARE ... 6

Ransomware: A Massive Revenue Generator with Undeniable Staying Power 7

The Evolution of Ransomware: Self-Propagation 9

Vulnerabilities 11

A False Sense of Security About Secure Connections 12

TIME TO OPERATE 13

Attack Vectors: Client Side 14

PDF and Java Attacks on the Decline 14

Leading Exploit Kits Continue to Rely on Flash 15

Exploit Kit Uses Tor to Hide Communication 16

Adversaries See Value in Server-Based Campaigns 16

JBoss: Vulnerabilities in Infrastructure Provide Attackers with Time to Operate 18

Spam Volume Remains Relatively Stable Worldwide 19

A Return to Blacklists? Attackers' Embrace of HTTPS Complicates Defenders' Investigations 21

Malvertising as a Service: High-Efficiency Infections Are the Name of the Game 23

Web Attack Methods: Setting Up Ransomware for Success 25

TIME TO SECURE 26

Time to Patch: Lag Times Between Patch and Upgrade Availability and Implementation Create Security Gaps 27

Aging Infrastructure: Ransomware's Rise Makes Patching Long-Standing Vulnerabilities an Urgent Imperative 30

Encryption: HTTPS Traffic Stable in 2016 ... So Far 35

TLS Encrypts Payloads but Doesn't Hide Malware Behavior 37

Time to Detection Trends Highlight a Heated "Arms Race" 40

Incident Response: Practices That Impair Organizational Security ... 44

Ransomware Attacks in Healthcare Offer Security Hygiene Lessons for All Organizations 45

GLOBAL PERSPECTIVE AND SECURITY RECOMMENDATIONS 46

Regional Overview of Web Block Activity 47

Vertical Risk of Malware Encounters: No Industry Is Safe 49

Geopolitical Update: Governments and Businesses Navigate the Data Protection Dilemma 50

Security Recommendations 52

Indicators of Compromise Are Not Threat Intelligence 53

CONCLUSION 54

ABOUT CISCO 55

Contributors to the Cisco 2016 Midyear Cybersecurity Report 55

Executive Summary and Major Findings

Defenders must reduce attackers' time to operate. It is the key to undermining their success.

Attackers currently enjoy unconstrained time to operate. Their campaigns, which often take advantage of known vulnerabilities that organizations and end users could have—and should have—known about and addressed, can remain active and undetected for days, months, or even longer. Defenders, meanwhile, struggle to gain visibility into threat activity and to reduce the time to detection (TTD) of both known and new threats. They are making clear strides but still have a long way to go to truly undermine adversaries' ability to lay the foundation for attacks—and strike with high and profitable impact.

The Cisco® 2016 Midyear Cybersecurity Report—which presents research, insights, and perspectives from Cisco Security Research—updates security professionals on the trends covered in our previous security report while also examining developments that may affect the security landscape later this year.

Our observation of recent developments within and from the shadow economy confirms that adversaries have become only more focused on generating revenue. Ransomware has become a particularly effective moneymaker, and enterprise users appear to be the preferred target of some operators. Many of the threat and security trends discussed in this report are related to ransomware—from techniques used to launch campaigns and conceal attackers' activity to our expectations for how the next generation of this potent threat will evolve.

In this report, we examine the many ways organizations can and should take action to start improving their defenses. Recommendations from Cisco researchers include:

- Instituting and testing an incident response plan that will enable a swift return to normal business operations following a ransomware attack
- Not blindly trusting HTTPS connections and SSL certificates
- Moving quickly to patch published vulnerabilities in software and systems, including routers and switches that are the components of critical Internet infrastructure
- Educating users about the threat of malicious browser infections
- Understanding what actionable threat intelligence really is

In this report, we cover four main topic areas:

I. CYBERCRIME TREND SPOTLIGHT: RANSOMWARE

Cisco security researchers have turned their spotlight on ransomware, examining innovations that may cause this particular type of malware attack to become far more prevalent. Predictions for the evolution of ransomware, based on previous trends observed, are also offered. In addition, we consider how vulnerabilities in unpatched systems and outdated devices provide time for bad actors to operate. Ransomware operators are now targeting enterprise users. This is why organizations should ensure they are backing up critical data at a protected location and establishing actionable plans that will allow them to return to normal business operations as quickly as possible after an attack.

II. TIME TO OPERATE

This section examines client-side attack vectors that provide adversaries with the time and opportunity to innovate threats and carry out their campaigns. The increase in vulnerabilities involving cryptography and authorization are signs that threat actors are now seeking to tamper with secure connections. Trends in exploit kits and attack vectors are discussed, such as the appeal of server exploits for online criminals seeking access to broader data sets. The emergence of "malvertising as a service" and the complications it creates for defenders, as well as the questions it raises about who should protect web users, are also examined.

III. TIME TO SECURE

In this section, Cisco security researchers explore the gap between attacker activity and security solutions. For example, while vendors have shortened the time between the announcement of public vulnerabilities and availability of patches, users have lagged in their implementation of such patches. This section also includes an update on Cisco's ongoing efforts to reduce its median time to detection (TTD)—and the impact of the ongoing "arms race" between attackers and defenders. Cisco researchers also detail the growing use of HTTPS in malicious campaigns, as well as bad actors' use of Transport Layer Security (TLS) to encrypt their communications.

IV. GLOBAL PERSPECTIVE AND SECURITY RECOMMENDATIONS

This section examines current geopolitical trends related to security, including increasing government concerns about the challenges of keeping pace with technological change in order to understand threats and to control or access data. Recommendations to defenders for reducing adversaries' time to operate are also presented. In addition, the important difference between indicators of compromise (IOCs) and threat intelligence is explained.

MAJOR FINDINGS

- Ransomware is dominating the malware market. Although it is not a new threat, it has evolved to become the most profitable malware type in history—and businesses are now becoming a target of choice for some ransomware operators. In the first half of 2016, ransomware campaigns targeting both individual and enterprise users became more widespread and potent. On the horizon: faster and more effective propagation methods that maximize the impact of ransomware campaigns and increase the probability that adversaries will generate significant revenue.
- Exploit kits, which have helped ransomware to become such a prominent threat, continue to take advantage of Adobe Flash vulnerabilities. In Cisco researchers' recent examination of the popular Nuclear exploit kit, for example, Flash accounted for 80 percent of successful exploit attempts.
- Vulnerabilities in the enterprise application software JBoss are providing attackers with a new vector that they can use to launch campaigns such as ransomware. Cisco research shows that JBoss-related compromises have made significant inroads within servers, leaving them vulnerable to attack.
- From September 2015 to March 2016, Cisco security researchers observed a fivefold increase in HTTPS traffic related to malicious activity. The rise in this type of web traffic can be attributed largely to malicious ad injectors and adware. Threat actors are increasing their use of HTTPS encrypted traffic to conceal their activity on the web and expand their time to operate.
- Even though patches are available from major software vendors almost at the same time vulnerabilities are announced, many users still do not download and install these patches in a timely manner, according to Cisco research. The gap between the availability and the actual implementation of such patches is giving attackers ample time to launch exploits.
- To help draw attention to the security risks that organizations create by not properly maintaining aging infrastructure or patching vulnerable operating systems, Cisco researchers examined a sample set of Cisco devices to determine the ages of known vulnerabilities running on fundamental infrastructure. We learned that 23 percent of those devices had vulnerabilities dating back to 2011; nearly 16 percent had vulnerabilities that were first published in 2009.
- A small but growing number of malware samples show that bad actors are using Transport Layer Security (TLS), the protocol used to provide encryption for network traffic, to hide their activities. This is a cause for concern among security professionals, since it makes deep-packet inspection ineffective as a security tool. The combination of machine-learning methods and novel data views provide higher-quality information on this trend.
- For the period from December 2015 through April 2016, Cisco reduced its median TTD to about 13 hours—well below the current and unacceptable industry estimate of 100 to 200 days. Increases and decreases in TTD observed during this period help to highlight an ongoing and heated "arms race" between attackers and defenders, with adversaries unleashing a constant barrage of new threats that security vendors must move swiftly to identify.

Introduction

Defenders are not protecting systems in a way that matches how attackers do their work. Although defenders have evolved their strategies and tools for fighting online criminals, attackers are still permitted far too much unconstrained time to operate.

Lack of visibility is the problem, leaving users open to attacks. Security professionals' reliance on point solutions and a "triage" approach—trying to stop attacks here and there, instead of looking holistically at security challenges—is playing to attackers' strengths.

With time on their side, attackers can identify and use vulnerabilities in infrastructure, systems, and devices deployed but unmaintained or simply long forgotten. They can gain a foothold in networks and move laterally. And they can launch server-based campaigns that give them more operational space in which to work, and provide a greater return on investment.

"If defenders improve the tools at their disposal, by reducing the time needed to patch vulnerabilities and upgrade their infrastructure, attackers become known—and therefore, defenders can constrain and even close adversaries' operational spaces."

In spite of the time advantage, attackers are limited in how they can operate. They have only so many ways to gain entry into networks. If defenders improve the tools at their disposal, by reducing the time needed to patch vulnerabilities and upgrade their infrastructure, attackers become known—and therefore, defenders can constrain and even close adversaries' operational spaces. Defenders can also obtain the full picture of the security landscape: whether adversaries are present, how they gained entry, and which systems succeeded (or failed) in identifying the malicious activity.

Unfortunately, defenders seem overwhelmed by the responsibilities of securing networks on so many levels, which is why they default to the triage approach. This mindset allows attackers to pull together all their advantages—time to operate, and the failure of defenders to block the easiest paths to attacks—and strengthen their campaigns. This is why ransomware is the "perfect storm" result of attackers' ability to breach defenses and make money—and it's on the rise and becoming harder to defeat (see "Ransomware: A Massive Revenue Generator with Undeniable Staying Power," **page 7**).

Cybercrime Trend Spotlight: Ransomware

Cybercrime Trend Spotlight: Ransomware

Ransomware is dominating the malware market. Although it is not a new threat, it has evolved to become the most profitable malware type in history. In the first half of 2016, ransomware campaigns targeting both individual and enterprise users became more widespread and potent.

The success of recent ransomware attacks against businesses, including several organizations in the healthcare industry, has likely prompted many adversaries to plan similar campaigns in the future. Network and server-side vulnerabilities provide an opportunity for attackers to quietly carry out ransomware campaigns that could potentially affect entire industries.

Ransomware: A Massive Revenue Generator with Undeniable Staying Power

There are dozens of ransomware variants, many language-specific, and all of them resilient. Innovators in the space—namely, the authors responsible for well-known ransomware brands such as CryptoLocker and CryptoWall—took their malware to an entirely new level of effectiveness when they began using cryptographically sound file encryption. Currently, the majority of known ransomware cannot be easily decrypted, leaving victims with little option but to pay the asking price in most cases.

Adversaries are typically paid in Bitcoin. The cryptocurrency has inadvertently helped the ransomware industry to flourish because users of bitcoin addresses can remain anonymous. Another complication for security researchers is that nearly all ransomware exchanges are conducted through Tor, an Internet anonymizer. Bitcoins also can be broken down into fractions, enabling adversaries to pay their entire team from just one bitcoin in a convenient and essentially untraceable way.

A NEW VECTOR FOR RANSOMWARE

Email and malicious advertising (malvertising) are the primary vectors for ransomware campaigns. However, some threat actors are now using network and server-side vulnerabilities.

One widespread campaign that appeared to target the healthcare industry earlier this year employed the Samas/Samsam/MSIL.B/C ("SamSam") ransomware variant, which was distributed through compromised servers. The threat actors used the servers to move laterally through the network and compromise additional machines, which were then held for ransom.

Adversaries used JexBoss, an open-source tool for testing and exploiting JBoss application servers, to gain a foothold in organizations' networks. Once they had access to the network, they proceeded to encrypt multiple Microsoft Windows systems using the SamSam ransomware family.

"We expect the next wave of ransomware to be even more pervasive and resilient. Organizations and end users should prepare now by backing up their critical data and confirming that those backups will not be susceptible to compromise."

In many respects, the SamSam attack was inevitable because many organizations were operating JBoss servers with unpatched vulnerabilities. (See "JBoss: Vulnerabilities in Infrastructure Provide Attackers Time to Operate," **page 18**.) In an April 2016 investigation, Cisco identified at least 2100 JBoss servers that were already compromised and waiting for a malicious actor to abuse them. All organizations were informed that they should take the servers offline and upgrade them immediately.

Vulnerable Internet infrastructure is a pervasive problem, and we fully expect to see more threat actors explore this channel as a way to quietly conduct malware campaigns that target not only enterprises but also entire industries. (See "Aging Infrastructure: Ransomware's Rise Makes Patching Long-Standing Vulnerabilities an Urgent Imperative," **page 30**.)

ANOTHER NEW CONCERN: DATA INTEGRITY

Users and businesses targeted by ransomware are in the unenviable position of having to trust their attackers. While it may seem that paying the ransom is the easiest (and only) thing to do, it is important for users in a ransomware situation to understand that their files may not be decrypted and could even be lost. Bugs in early versions of some ransomware variants resulted in file loss, even when the ransom was paid.

There is also a risk that adversaries may intentionally tamper with the files while they are in their control. Depending on the types of files encrypted—for example, medical records or engineering designs—the fallout from data tampering or theft could be dire.

The chance of reinfection is another concern, as we have seen instances of ransomware striking the same users twice on the same machine. In some cases, the ransom amount was reduced in the second attack, essentially providing the user an offer akin to a preferred customer discount. Attackers have also taken the opposite approach: asking for a higher ransom when users were indecisive about paying the first asking price.

Ransomware has become extremely effective as well as very profitable, leaving no doubt that more attackers will come to rely on it as a main source of easy revenue. Businesses, of course, offer an opportunity for adversaries to demand payments that far exceed amounts an individual end user would be expected to pay. The potential disruption and cost for an organization or industry targeted by ransomware is also obviously much greater.

We expect the next wave of ransomware to be even more pervasive and resilient. (See "The Evolution of Ransomware: Self-Propagation," **page 9**.) Organizations and end users should prepare now by backing up critical data and confirming that those backups will not be susceptible to compromise. They must also ensure that their backup data can, in fact, be restored quickly following an attack. For enterprises, restoration can be a major undertaking; therefore, being proactive about identifying potential bottlenecks is essential. Organizations should also confirm that known vulnerabilities in their Internet infrastructure and systems have been patched.

For more information on the SamSam campaign and JBoss vulnerabilities, see the following Cisco Talos blog posts:

"SamSam: The Doctor Will See You, After He Pays the Ransom"

"Widespread JBoss Backdoors a Major Threat"

The Evolution of Ransomware: Self-Propagation

The SamSam attack represents a change in focus for ransomware operators from targeting individual end users to infecting entire networks (see **page 16**). Its propagation method, while simple, is highly effective. Given SamSam's success, it's only a matter of time before adversaries introduce faster and more effective propagation methods to maximize its impact and increase the probability of receiving payment.

Cisco security researchers anticipate, based on trends and advances observed to date, that self-propagating ransomware is the next step for innovators in this space—and urge users to take steps now to prepare. Attackers' use of JBoss back doors earlier this year to launch ransomware campaigns against organizations in the healthcare industry is a strong reminder that adversaries, when given time to operate, will find new ways to compromise networks and users—including exploiting old vulnerabilities that should have been patched long ago.

Self-propagating malware is not new—in fact, it has been around for decades in the form of worms and botnets. Many of these threats are still pervasive and continue to be effective. The traits of self-propagating malware can include:

- **Utilization of a vulnerability in a widely deployed product.** Most successful worms of the past used vulnerabilities in products deployed across the Internet.
- **Replication to all available drives.** Some strains of malware will enumerate local and remote drives, including network drives and USB drives, and copy itself to those drives as a way to spread or persist. This enables the infection of offline systems as well as systems not reachable through the public Internet.
- **File infections.** File-infecting malware will either append or prepend itself to files. Specifically, the malware attaches to executables not protected by Windows SFC or SFP (System File Checker or System File Protector). Some worms can attach themselves to and spread through nonexecutable files.
- **Limited brute-force activity.** Few worms have attempted this method in the past.
- **Resilient command and control.** Some worms take into account actions normally used to disrupt command-and-control infrastructure and will implement preemptive measures to circumvent those disruptions. Many worms have no command-and-control infrastructure. They exhibit only a simplistic default action to spread as quickly as possible.
- **Use of other back doors.** Some malware authors, aware that other infections may have already made an impression on a system, will piggyback on those back doors to spread their malware.

"Cisco security researchers anticipate, based on trends and advances observed to date, that self-propagating ransomware is the next step for innovators in this space—and urge users to take steps now to prepare."

THE KING'S RANSOM FRAMEWORK

Our observation of the techniques of ransomware innovators suggests that the adversaries who develop the next generation of ransomware are likely to prefer to use software with a modular design—the type of architecture found in many popular open-source penetration-testing suites. This approach allows them to use certain functions as needed. It increases efficiency and provides threat actors with the ability to switch tactics in the event one method is discovered or is found to be ineffective.

We hypothesize that the next-generation ransomware framework—what we have dubbed the King's Ransom Framework—will include core functionality such as:

- Encrypting standard locations for user files as well as the provision for customizing directories and file types, allowing for per-target customization
- Marking which systems and files have already been encrypted
- Providing instructions for payment using bitcoin
- Allowing the attacker to set the ransom amount, and specify dual deadlines: one before a cost increase, and one where the key encrypting the data will be deleted

The framework will also support different modules, so the attacker can customize the ransomware for use in different environments and change techniques to propagate more aggressively when openings are available. Examples of such modules include:

AUTORUN.INF/USB MASS STORAGE PROPAGATION

This module would search the infected system to find mapped drives, both local and remote. It would then copy itself to specific locations on those drives and set the file attributes to make those copies harder to find and delete. Then, it would write an "autorun.inf" file into those drives to request any computer that the drives are connected to in the future to run these infecting programs.

AUTHENTICATION INFRASTRUCTURE EXPLOITS

This module would take advantage of known weaknesses in popular authentication infrastructures that are components of many corporate networks. Credentials could then be exploited to provide access to other systems, sometimes at an administrative level.

COMMAND-AND-CONTROL AND REPORTING INFECTIONS

To reduce the risk of discovery, next-generation ransomware could be configured to have no command-and-control functionality. This module would transmit a beacon with a GUID (globally unique identifier) to a command-and-control domain, trying to reach this domain through common protocols and services such as HTTP, HTTPS, or DNS, to transmit this data. The domain could then collect these GUIDs for statistics on the number of infected and encrypted systems in a targeted network. Attackers could use this information to determine the effectiveness of their campaigns.

RATE LIMITER

This module would ensure that ransomware would be "polite" to system resources, making it less likely that the user will notice it running. It would limit the amount of CPU usage, throttle its network usage down to a trickle, and ensure that it performs as subtly as possible.

RFC 1918 TARGET ADDRESS LIMITER

The implant would be designed to attack and implant only target hosts if the host has an RFC 1918 address; these addresses are used by internal networks.

Carefully constructed architecture and vigilant password management can make lateral movement much more difficult for the self-propagating ransomware of the future. For more on defenses to meet the challenge of next-generation ransomware, see "Security Recommendations," **page 52**.

For more details on the evolution of ransomware, and what enterprises can do to prepare for next-generation threats in this space, see the Cisco Talos blog post:

"Ransomware: Past, Present, and Future"

Vulnerabilities

Vulnerabilities buy time for bad actors to operate—and they use this advantage to launch campaigns before the weak points can be patched by defenders. Through exploit kits, ransomware, and even socially engineered spam, attackers rely on unpatched systems and outdated devices to achieve their goals.

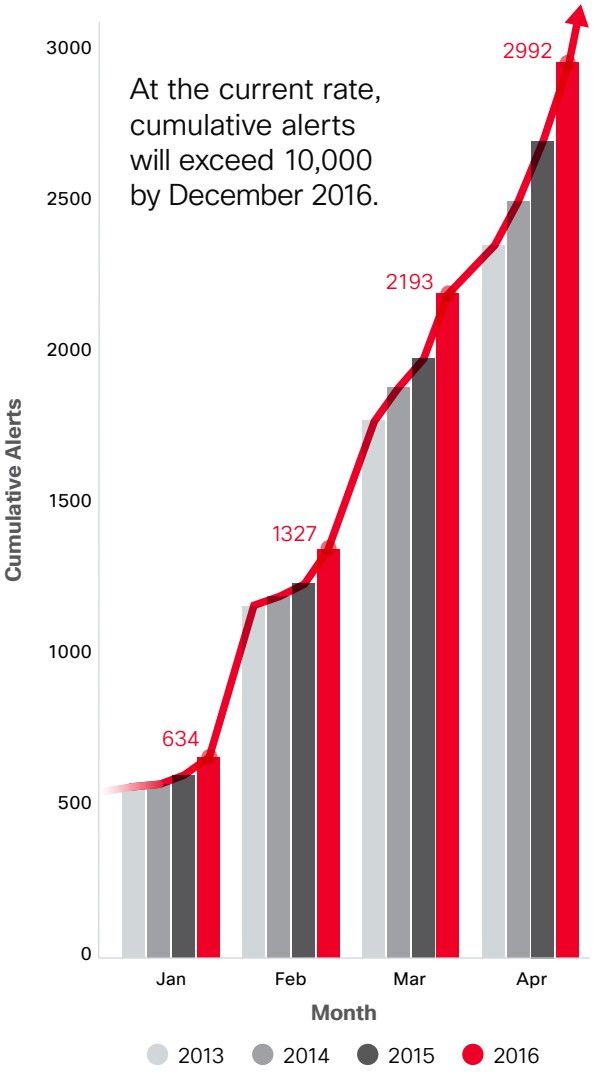
Vulnerabilities sit at the intersection of attacker opportunity and defenders' ability to protect their organizations. If defenders can close the window of opportunity for attackers by patching vulnerabilities, they reduce the threat. If defenders leave vulnerabilities open and unpatched, attackers use them as a stepping-stone to launch their campaigns.

Vendors have become more attentive to identifying and disclosing vulnerabilities, thanks to secure development lifecycle (SDL) practices. But as explained on **page 15**, attackers pay close attention to patches as well, reverse-engineering them to determine what was fixed and developing new approaches based on what they've learned.

The first four months of 2016 showed a slight increase in cumulative annual alerts over the previous years' totals during the same period, most likely due to major software updates from vendors such as Microsoft and Apple; increased code reviews; improved code review tools; and the aforementioned SDL practices (Figure 1). All of these trends are leading to an increase in the identification of vulnerabilities in products.

Defenders refine and innovate their processes to close gaps through vulnerability disclosure and patching, but attackers use their skills to open these gaps yet again—creating attacks that are more numerous and more complex and that undermine defenders' ability to respond. Defenders must identify and close the operational space of the attackers. Addressing disclosed vulnerabilities and implementing robust patch-management systems are core to meeting this objective.

Figure 1. Cumulative Annual Alert Totals



Source: Cisco Security Research

SHARE

"Defenders refine and innovate their processes to close gaps through vulnerability disclosure and patching, but attackers use their skills to open these gaps yet again—creating attacks that are more numerous and more complex and that undermine defenders' ability to respond."

A FALSE SENSE OF SECURITY ABOUT SECURE CONNECTIONS

Secure connections, such as those created by HTTPS connections and SSL certificates, are supposed to give users a sense of security about their online activities. However, a recent increase in vulnerability alerts involving encryption and authentication raises concerns that adversaries can more easily compromise secure connections. The result: connections of questionable security.

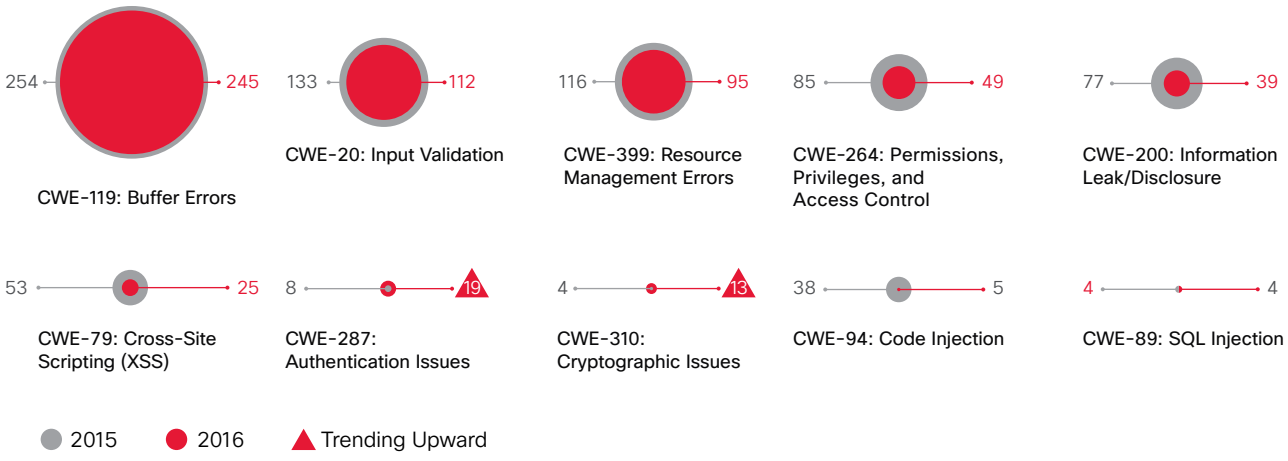
As shown in the Common Weakness Enumeration (CWE) chart below (Figure 2), authentication issues and cryptographic issues have been on the rise since 2014 and 2015. From December 2015 to March 2016 alone, 19 authentication issues and 13 cryptographic issues were identified, approaching the previous years' totals.

The growing use of encryption is a positive development, as it serves to help keep information safe from prying eyes. But there is an inherent risk: Encryption creates more complexity, and with it comes new vulnerabilities both in the tools used for encryption and in the associated expectation of privacy it cannot guarantee. If encryption isn't done properly, it's not providing protection.

Establishing secure connections requires a complex chain of processes and tools. Beyond certificates, that chain may be questionable. There are devices in-between the connections, such as VPN gateways, that may or may not be secure. In addition, websites that indicate secure connections may have been compromised. The bottom line is that URLs with the "lock" icon, which casual observers believe is an indication of safe activity, can't ever be assumed to be safe or secure.

SHARE

Figure 2. Rise of Authentication and Cryptographic Issues, December–March



Source: Cisco Security Research

Time to Operate

Time to Operate

The rise in ransomware activity, and the breadth of recent campaigns, underscore how adversaries benefit from having unconstrained time to operate. It allows them to quietly lay the groundwork for their campaigns, strike when they are ready, and ultimately succeed in generating revenue from their efforts.

To conceal their activity, they are using cryptocurrency, Tor, HTTPS encrypted traffic, and Transport Layer Security (TLS). Meanwhile, exploit kit authors further enable their success by moving fast to reverse-engineer patches and exploit unmanageable vulnerability disclosures. And a new twist to malvertising is providing adversaries with a high-efficiency and hard-to-track method to increase traffic to compromised sites, so they can infect users' machines and eventually launch ransomware attacks.

Attack Vectors: Client Side

Attackers have traditionally favored the client side because it offers greater user engagement, and users are a perennial weak link. In addition, the client side offers many ways for attackers to gain operational space in which to work. The choices are vast.

Nevertheless, attacks using such vectors as PDFs appear to have stabilized after years of growth. At the same time, there are signs that adversaries are finding new opportunities on the server side, where they can move laterally across networks and amass more strength.

PDF AND JAVA ATTACKS ON THE DECLINE

The popularity of PDF and Java as attack vectors continues to slide. In January 2016, Oracle announced that it would extinguish its Java browser plugin, since browser vendors are proceeding with plans to end support for such plugins.[1] Oracle is instead focusing on its plugin-free Java Web Start technology.

The end of the Java browser plugin means its use as an attack vector will continue to fade—but security researchers will watch closely to see if attackers evolve older threats to take advantage of Java's new incarnation. Security professionals and enterprises should consider blocking Java except on sites where it is required.

[1] "Moving to a Plugin-Free Web," Java Platform Group, January 2016: **https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free**.

Although PDF exploits are also declining, they are still a presence in email—for example, persuading email recipients to click compromised attachments. Spam creators use such tactics in tandem with subject lines that play to current news or seasonal events (see more on spam on **page 19**).

Exploit kit developers still rely on Flash, but Flash content elsewhere online has been slowly but steadily decreasing. However, many online applications, such as those using rich media content or interactive advertising, still rely heavily on Flash to function.

Alternative applications such as HTML5 are slowly being adopted, but the transition is gradual, hence the ongoing reliance on Flash. As long as Flash exists, it will remain an attack vector.

LEADING EXPLOIT KITS CONTINUE TO RELY ON FLASH

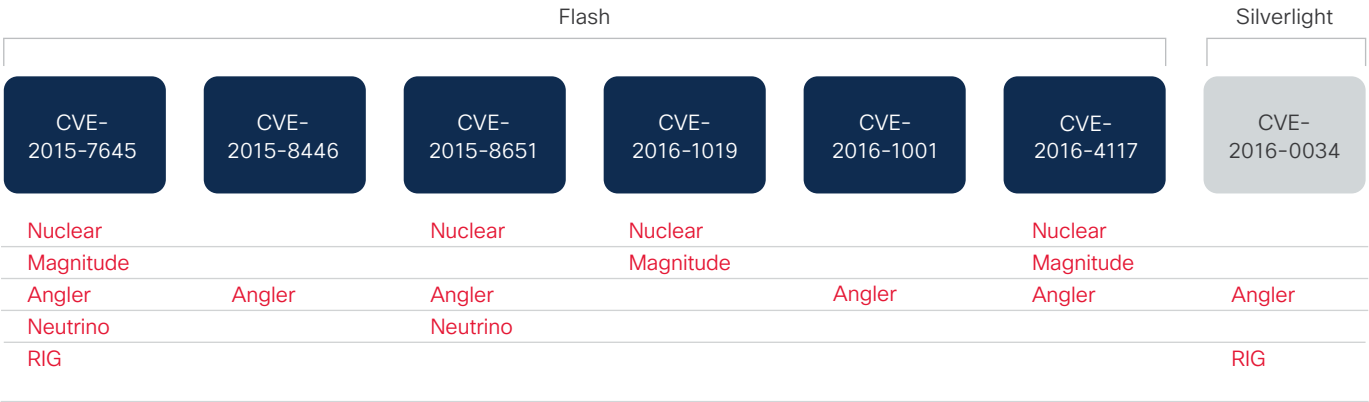
Exploit kits, which have helped ransomware to become such a prominent threat, continue to make use of Adobe Flash vulnerabilities. In Cisco researchers' recent examination of the popular Nuclear exploit kit, for example, Flash accounted for 80 percent of successful exploit attempts.[2]

Adobe is responding to the frequent exposure of vulnerabilities with patches; however, attackers move just as fast. As soon as Adobe releases a Flash update to patch vulnerabilities, exploit kit authors begin reverse-engineering the patches to discover what was fixed. Within a week, exploit authors identify and weaponize Flash vulnerabilities that they use for remote code implementation.

We recommend that users and administrators disable or remove unnecessary browser plugins to reduce their exposure to threats—or at minimum, upgrade Flash as soon as updates are released.

To help emphasize the positive impact of installing patches, Figure 3 shows the various exploit kits that have incorporated recent Flash and Microsoft Silverlight vulnerabilities. By installing available patches for all these vulnerabilities, users can significantly blunt the impact of ransomware delivered by exploit kits.

Figure 3. Vulnerabilities Used by Exploit Kits



Source: Cisco Security Research

SHARE

[2] "Threat Spotlight: Exploit Kit Goes International, Hits 150+ Countries," Cisco Talos blog, April 20, 2016: **http://blog.talosintel.com/2016/04/nuclear-exposed.html**.

Exploit Kit Uses Tor to Hide Communication

Exploit kit authors are always seeking ways to evade security defenses, and they can be very creative in their efforts. One example we recently observed involved the Nuclear exploit kit. The kit, which typically drops variants of ransomware, was observed delivering a variant of Tor, the software used for anonymous communication. This tactic appears to be a method for anonymizing the eventual malicious payload, therefore making the activity more difficult for defenders to track.

Typically, when an exploit kit drops a malicious file, it can be detected by monitoring the resulting command-and-control traffic—that is, when the malware "calls home." However, in the Nuclear exploit kit payload drop observed by Cisco, a Tor executable file was dropped first and was followed by communication requests through Tor. Because Tor is an end-to-exit encrypted routing protocol, security professionals can't see what the malware is doing within it.

Ransomware, delivered by exploit kits, has become a tremendous moneymaker for its creators. (See "Ransomware: A Massive Revenue Generator with Undeniable Staying Power," **page 7**.) It is therefore logical that ransomware developers seek new ways to make their malware more effective—and to compete with other exploit kits. The observation of the Nuclear exploit kit's use of Tor suggests yet another clever evolution by malware developers.

Read more about the Nuclear exploit kit's use of Tor in this Cisco **Talos blog post**.

ADVERSARIES SEE VALUE IN SERVER-BASED CAMPAIGNS

Attackers seek high value for their campaigns—bang for the buck, in other words. Delivering malware or exploit kits to clients or end users is effective, but it also blunts the impact of an attack: Bad actors are limited in how much bandwidth and how many capabilities they can amass during client-side attacks.

However, attackers are seeing greater payoff for their efforts by expanding to campaigns that utilize the server side. JBoss is an enterprise application platform that was recently used to gain access to networks in order to spread SamSam, a ransomware variant (see **page 7**). Attackers used JexBoss, an open-source tool for testing and exploiting JBoss application servers, to gain a foothold in networks for healthcare organizations in the cases observed by Cisco researchers. Once attackers were in the network, they were able to encrypt Windows files using SamSam.

Targeting vulnerabilities in servers to spread ransomware adds a new dimension to a prolific threat. Cisco researchers scanned machines on the Internet and found machines that were already compromised and waiting for a ransomware payload. In addition, Cisco found that 2000 back doors had been installed across 1600 IP addresses. Many of the back doors were present in systems using a common library management system for schools. When contacted by Cisco, the software developer quickly took action to release the necessary patch.

By relying on vulnerabilities in server-side systems, attackers gain a far wider playing field, and their activities require much more time and effort to contain the damage. Client-side applications such as web browsers are increasingly patched by auto-updates, making them less prone to vulnerabilities.

On the other hand, server-side applications are chronically out of date, since patching and upgrades depend on the often limited work hours of the IT staff—and these systems are difficult to upgrade without having an impact on operations. In addition, the porousness of the network perimeter is giving attackers access to servers that previously relied on that perimeter for defense.

As seen in Figure 4, many major infrastructure vendors' products show vulnerabilities for both client and server applications.

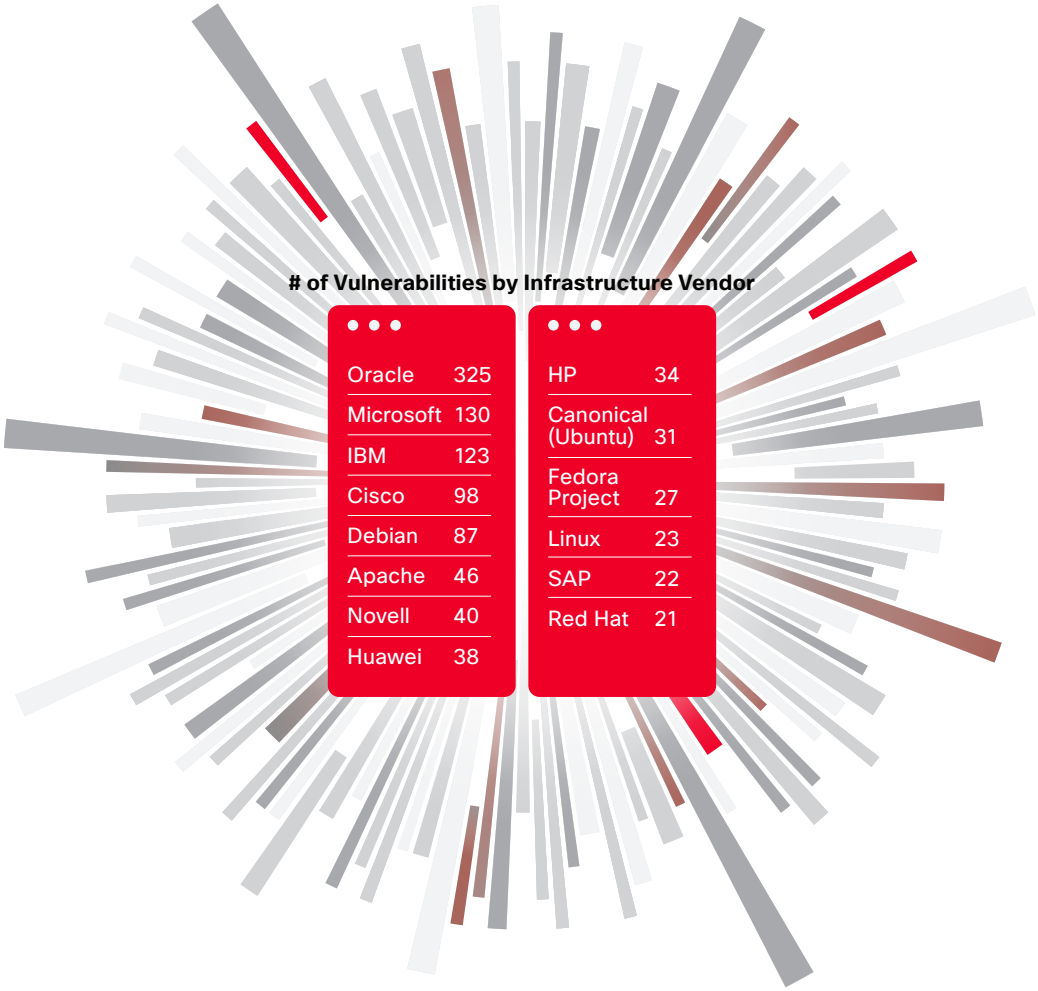
To learn more about the dangers of vulnerabilities in server solutions, read the Cisco Talos blog posts:

"Widespread JBoss Backdoors a Major Threat"

"SamSam: The Doctor Will See You, After He Pays the Ransom"

SHARE

Figure 4. Vulnerabilities by Infrastructure Vendor, January 1–March 30, 2016



Source: Cisco Security Research

JBOSS: VULNERABILITIES IN INFRASTRUCTURE PROVIDE ATTACKERS WITH TIME TO OPERATE

Ransomware creators have gained an advantage in their campaigns from JBoss, the enterprise application software. As seen in a recent ransomware campaign involving healthcare organizations (**page 7**), vulnerabilities in JBoss are allowing bad actors to gain entry into networks—and gain time to gather data or launch malware. The JBoss-enabled compromises offer more evidence that poor maintenance of networks provides criminals with access to them—access that can be blocked.

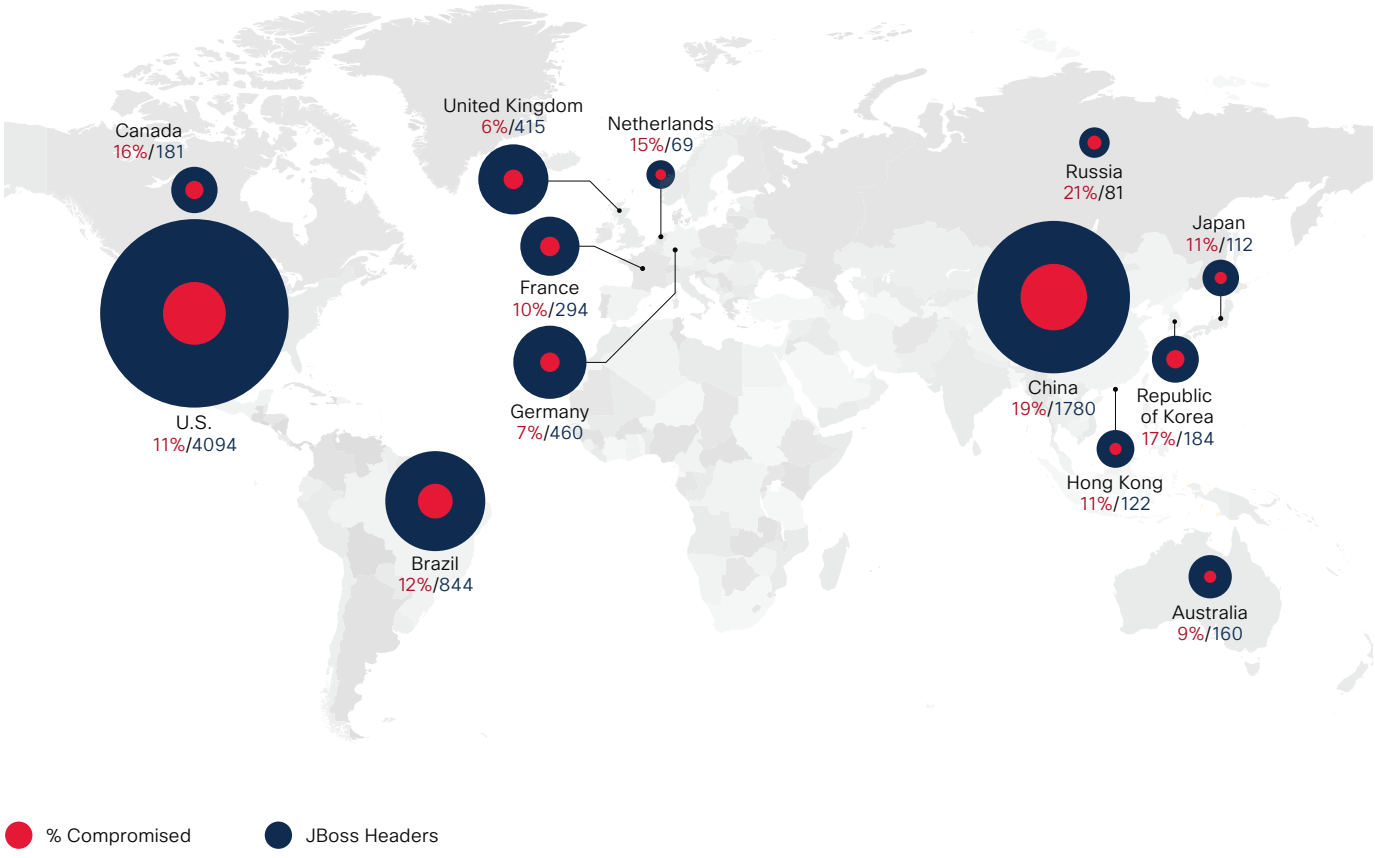
SHARE

Cisco researchers have found that JBoss-related compromises have made significant inroads within servers, leaving them vulnerable to attack. In our scan of the Internet:

- We looked for servers reporting a JBoss installation in the HTTP headers or page content.
- We then searched for the presence of a number of different back doors, web shells, or other .jsp compromises on the hosts.

Figure 5 shows the percentage of servers that appear to have been compromised compared with the number of servers showing a JBoss installation. In the United States, for example, 11 percent of the observed web shells show signs of compromise.

Figure 5. Presence of Web Shells Indicates JBoss Compromises



Source: Cisco Security Research

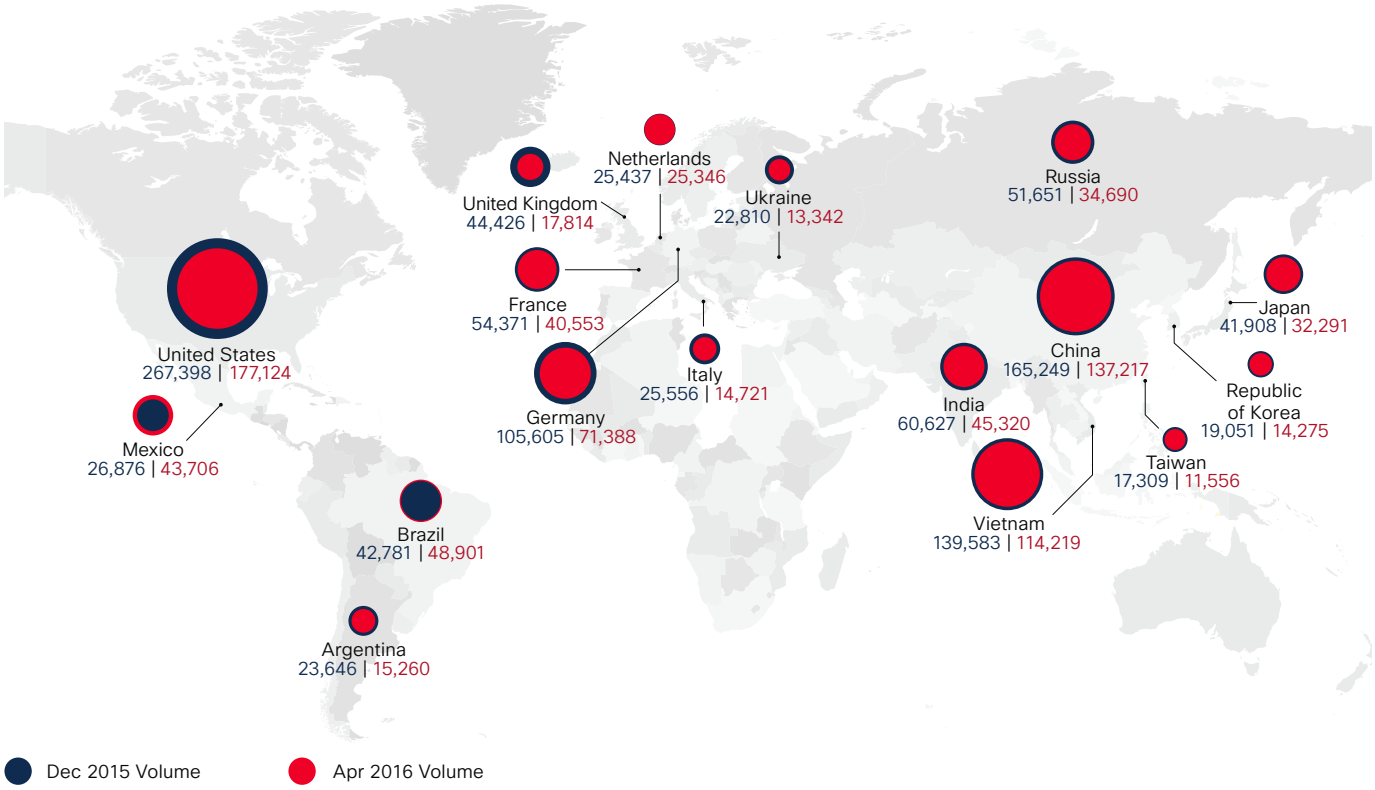
SPAM VOLUME REMAINS RELATIVELY STABLE WORLDWIDE

To gauge spam traffic worldwide, Cisco collects samples from its email appliances, indicating the impact of policy decisions coded into email appliances and gateways—for example, emails that are blocked or marked as unknown. Spam email is frequently used as an attack vector, especially for ransomware.

According to Cisco's examination of email traffic, spam volume remained steady from December 2015 to May 2016 (Figure 6). Spam traffic from Brazil showed spikes in spam in January and March 2016. These increases may be due to activity of a spam botnet at that time.

As explained in the section on regional web block activity (see **page 47**), attackers will often shift their operations from country to country, and from host provider to host provider, as they find hospitable environments for launching their campaigns. Spammers use botnet machines that are owned and collocated within reliable hosts. They employ them until detection systems catch up—and then they move to another botnet.

Figure 6. Spam Volume by Country, December 2015–May 2016



Source: Cisco Security Research

SHARE

Figure 7. Popular Social Engineering Topics Used in Spam

# of Versions	URL	Message Summary	Language	Last Publication Date (GMT)
95	RuleID4626	Invoice, Payment	German, English	3.18.16
82	RuleID4400KVR	Purchase Order	English	2.1.16
64	RuleID4626(cont)	Invoice, Payment, Shipping Confirmation	English, German, Spanish	1.28.16
62	RuleID4961KVR	Payment, Transfer, Order, Shipping	English	3.25.16
58	RuleID4961KVR	Quote Request, Product Order	English, German, Multiple Languages	1.25.16
52	RuleID5118KVR	Product Order, Payment	German, English	3.17.16
49	RuleID858KVR	Shipping Quote, Payment	English	3.14.16
47	RuleID4961	Transfer, Shipping, Invoice	English, German, Spanish	2.22.16
44	RuleID4627 and RuleID4627KVR	Air Travel E-ticket	English	3.29.16
30	RuleID8337KVR	Order, Payment, Quote	English	1.21.16

Source: Cisco Security Research

SHARE

Spam creators continue to persuade users to click attachments (such as PDFs carrying malware—see **page 15**) or links within messages through clever social engineering. As Figure 7 shows, spam authors create attachments or links that purport to contain vital information about bills and invoices, travel arrangements, or business quotes. Spammers also create versions of their messages in other languages to snare more victims.

A RETURN TO BLACKLISTS? ATTACKERS' EMBRACE OF HTTPS COMPLICATES DEFENDERS' INVESTIGATIONS

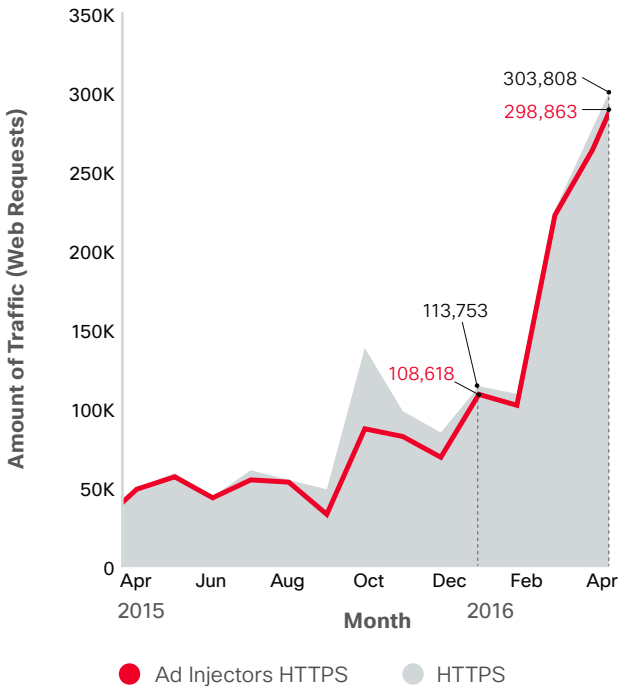
When ad injectors deliver malicious advertising through HTTPS encrypted traffic, users and security teams can't rely on the information sent through the URL to identify the potential threat. Knowing this, adversaries are increasing their use of HTTPS encrypted traffic—by leaps and bounds—to conceal their activity on the web and expand their time to operate.

From September 2015 to March 2016, Cisco security researchers observed a fivefold increase in HTTPS traffic related to malicious activity. To identify this trend in the use of HTTPS, we tracked 80 malicious campaigns distributed across eight threat categories over a 16-month period. The rise in HTTPS traffic can be attributed largely to ad injectors and adware, according to our research (Figure 8).

We also found that HTTPS traffic related to ad injectors increased 300 percent from December 2015 through April 2016 (Figure 9).

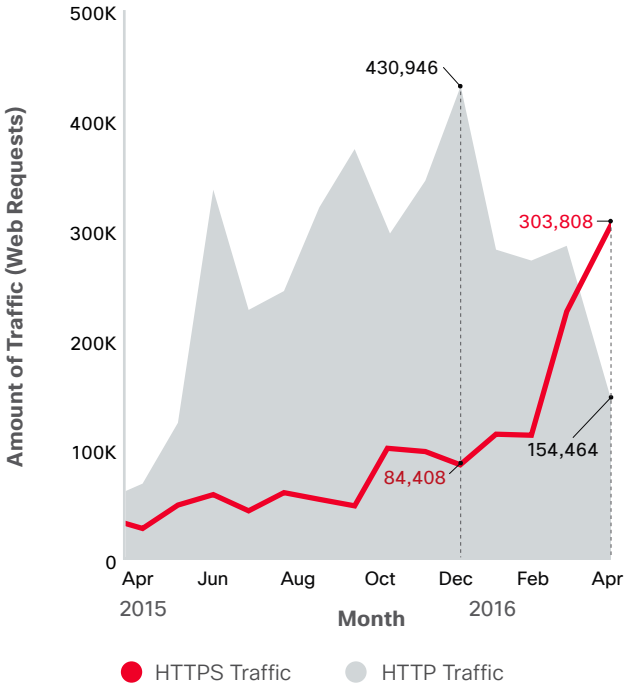
SHARE

Figure 8. Ad Injectors Are Major Source of HTTPS Increase



Source: Cisco Security Research

Figure 9. HTTPS Traffic Increased 300 Percent for Ad Injectors in 4-Month Period



Source: Cisco Security Research

Malicious ad injectors are a primary component of adware infections (Figure 10). Cybercriminals rely on these browser extensions to inject malvertising onto webpages, and expose users to display ads and pop-ups that facilitate ransomware and other malware campaigns. Malvertising and malicious ad injectors inhabit a part of the advertising ecosystem where it can be difficult to distinguish legitimate behavior from malicious activity.

Ad injector and adware infections are not to be ignored. This year Cisco security researchers found a new version of a DNSChanger Trojan delivered through adware. This development represents an increase in the danger that ad injector and adware infections pose to users and companies.[3]

We also found evidence of adversaries transitioning malware to HTTPS. This move is happening at a slower pace than what we have observed with ad injectors. This is likely because adversaries are always looking to maximize revenue and therefore will make changes to infrastructure only when necessary.

Ironically, cybercriminals' delay of these infrastructure updates echoes a trend in the legitimate business world. Many organizations have postponed patching known vulnerabilities in their Internet infrastructure—often for years—due to concerns about losing revenue while they take devices and software offline to perform upgrades. (See "Aging Infrastructure: Ransomware's Rise Makes Patching Long-Standing Vulnerabilities an Urgent Imperative," **page 30**). The challenge of patching a large number of infected hosts no doubt also incentivizes attackers to keep their legacy technology operational.

During our 16-month analysis, we observed the following malware families increasing their use of HTTPS:

- Gamarue/Andromeda, a multipurpose botnet
- Necurs, an information-stealing botnet
- Miuref/Boaxxe, a click-fraud botnet
- Ramdo/Redyms, a click-fraud botnet
- Data-exfiltration Trojans

The growth in HTTPS encrypted traffic related to malicious activity is troubling, as it creates significant challenges for security researchers tracking and investigating malware campaigns. The techniques defenders use to identify threats in HTTP traffic, such as signature-based IDS detection based on URL patterns, cannot be applied to HTTPS traffic without adding SSL inspection capabilities. In many cases, security researchers have only a domain name or IP address as a starting point for investigation.

Threat categorization also becomes difficult, as threats often share infrastructure. One fallback strategy for defenders is to use blacklists (lists of all known malware), but this method is prone to error and not granular enough to be effective. It is also time-intensive, as analysts need to manually investigate and categorize threats.

SHARE

Figure 10. Ad Injectors a Main Component Observed in Adware Infections

Source: Cisco Security Research

[3] "DNSChanger Outbreak Linked to Adware Install Base," Cisco Security Blog, February 2016: **http://blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base**.

MALVERTISING AS A SERVICE: HIGH-EFFICIENCY INFECTIONS ARE THE NAME OF THE GAME

Ad agencies, knowingly or not, are serving as a conduit for malicious ads on the web—essentially enabling a new business model for adversaries: "malvertising as a service." Threat actors are buying ad space on popular legitimate websites as a way to serve up malvertising. This is creating new challenges for defenders and raising questions about who is responsible for protecting users from malvertising.

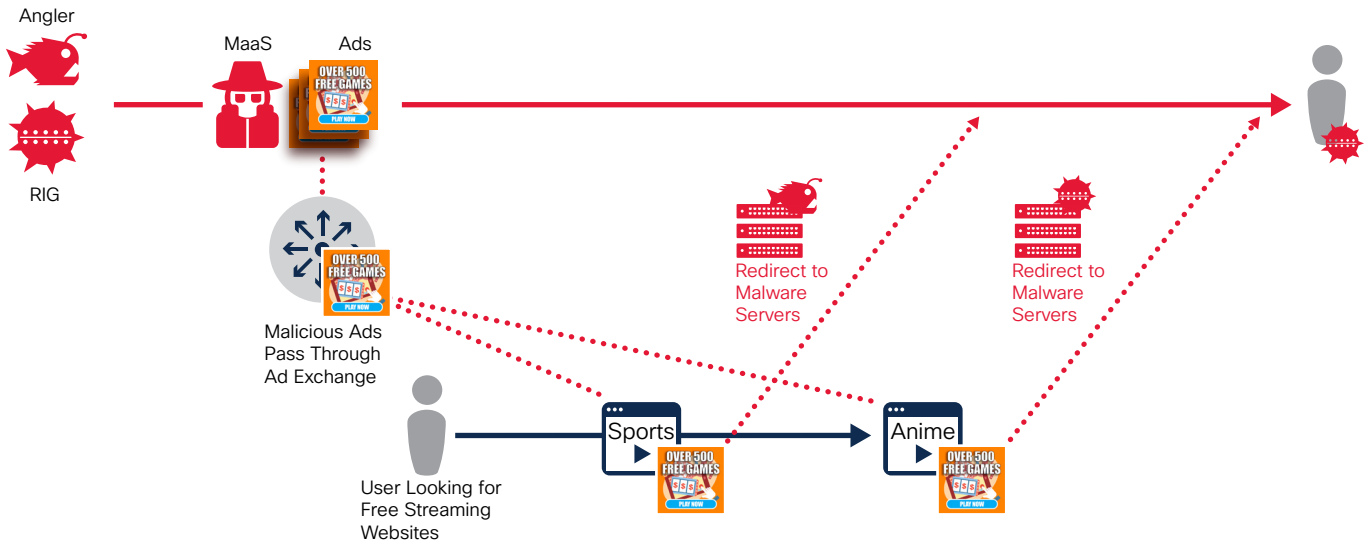
By purchasing legitimate ad space, adversaries can easily spread threats across unrelated sites. Ads pop up for only a short time, leaving defenders little or no time to identify the presence of a threat. And because ad agencies use information such as browser types and versions to target users, it's easier for adversaries to exploit specific groups of users at a granular level, including language.

The malvertising-as-a-service trend is similar to domain squatting. Domain squatters profit from selling or using domain names that users would be likely to associate with legitimate businesses and well-known brands. By directing traffic from those domains, they facilitate malware distribution without playing a direct role in delivering threats.

Turning on ad blockers is a logical strategy for avoiding exposure to malvertising—especially the emerging variety we have seen that does not require user interaction to infect machines and deliver a payload. But some leading providers of online content—which rely heavily on digital advertising for revenue—are mandating that users disable ad blockers if they want to view other content on the site. This obviously creates risk for users, as well as a dilemma for security teams, which must now consider deciding whether to block sites that serve up ads from ad exchanges.

SHARE

Figure 11. How Malvertising as a Service (MaaS) Works



Source: Cisco Security Research

Multiple Tiers of Redirection

Cisco researchers have observed threat actors buying ad space to deliver malicious ads that either infect users' computers directly or redirect users to another location to deliver the malware payload. In many cases, there are multiple tiers of redirection. In others, users do not even have to interact with the malicious ad for their machine to be infected; everything happens in the background, far off-screen.

One malvertising-as-a-service campaign that first appeared in October 2015 redirected users to several different exploit kits, including Angler and RIG, which delivered different payloads. Many of the payloads were variants of ransomware such as TeslaCrypt and CryptoWall. Users were duped by a malicious ad that spoofed a gambling site. A link to JavaScript was buried in the code behind the ad. That link took users to an Angler landing page, but there were other redirections as well, including iFrames.

The emergence of this new approach to distributing malvertising is another indicator that the shadow economy is becoming more industrialized. Cisco researchers expect the malvertising-as-a-service trend to grow as more cybercriminals look for efficient ways to infect large numbers of web users through legitimate sites and to evade detection. Malvertising plays a central role in helping adversaries to run ransomware campaigns, which are fast becoming a preferred attack method because they can be highly profitable ventures for adversaries. (See "Ransomware: A Massive Revenue Generator with Undeniable Staying Power," **page 7**.)

For more details on the malvertising-as-a-service trend, see the Cisco Talos blog post:

"Threat Spotlight: Spin to Win ... Malware"

"Cisco researchers expect the malvertising-as-a-service trend to grow as more cybercriminals look for efficient ways to infect large numbers of web users through legitimate sites and to evade detection."

WEB ATTACK METHODS: SETTING UP RANSOMWARE FOR SUCCESS

Certain trends in web attack methods in the first half of 2016 are connected to the explosive growth in ransomware. Suspicious Windows binaries, for example, which top the list in Figure 12, are used by adversaries to deliver threats such as spyware and adware. These tools allow them to gain a foothold in network infrastructure so they can launch attacks like ransomware.

Facebook scams (social engineering), Trojans, and iFrames also remain popular tools for gaining initial access to users' computers and organizational networks.

Facebook scams were the number one web attack method we observed in the latter half of 2015, as noted in our last cybersecurity report. Windows binaries were fourth on that list. JavaScript malware, which held three spots in our previous top 10, doesn't even rank among the current top 10.

JavaScript malware has by no means disappeared, however. In fact, this type of malware has been an essential component in facilitating many ransomware campaigns this year.

The list in Figure 13 is a collection of malware that is less frequently encountered and more likely to be deeper in an infection chain.

The long tail of the spectrum illustrated in Figure 13 shows a sample where ransomware signatures, Trojans, and droppers are present. With adversaries' growing embrace of ransomware, we are seeing infrastructure components for ransomware more frequently than information-stealing malware.

SHARE

Figure 12. Most Commonly Observed Malware

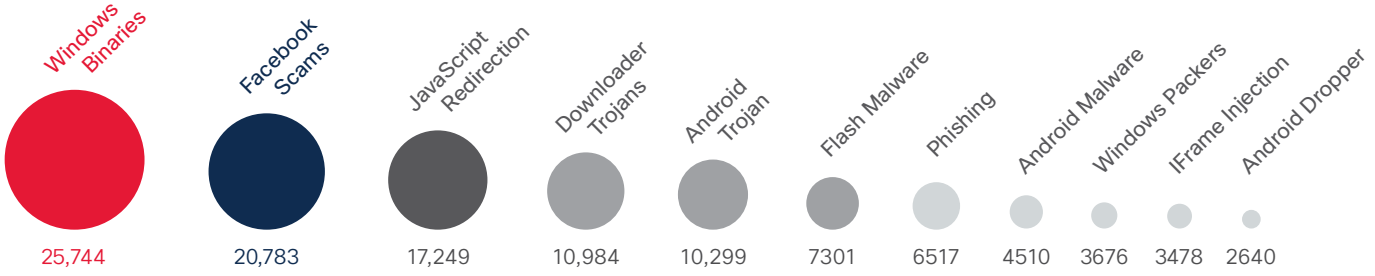
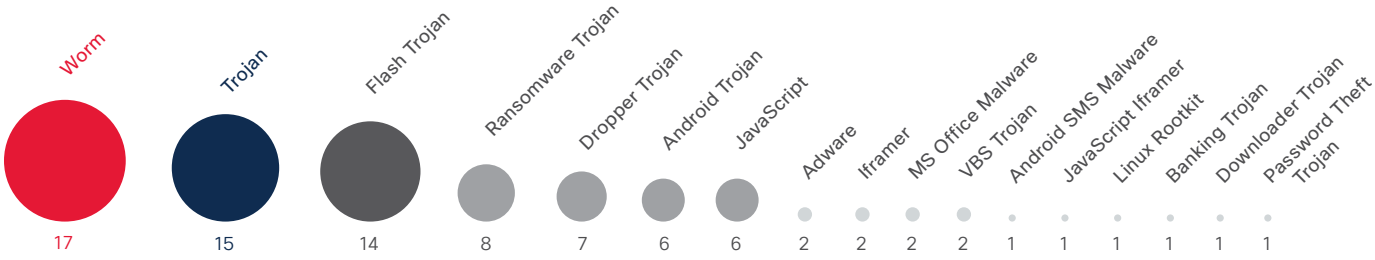


Figure 13. Sample of Observed Lower-Volume Malware



Source: Cisco Security Research

Time to Secure

Time to Secure

Even though defenders are always innovating, the infrastructure on which the digital economy depends remains fragile—and reliant on inadequate security practices. Today, there are many entryways for attackers, thanks to the hodgepodge of web browsers, applications, and infrastructure in place at most organizations.

These poorly protected devices and software open up operational space to attackers—and security professionals must close the space. Reducing the unconstrained operational space of adversaries, and making attackers' presence known, are the top jobs for security.

Time to Patch: Lag Times Between Patch and Upgrade Availability and Implementation Create Security Gaps

In recent years, major vendors have become more proactive in delivering patches in less and less time after vulnerabilities and exploits are exposed, as well as cooperating with the security researchers who find those vulnerabilities. In fact, according to Cisco research involving the examination of thousands of common vulnerabilities and exposures (CVEs), the median time between public disclosure of vulnerabilities and patch availability is zero days for major endpoint software vendors. In other words, at the same time a vulnerability is generally publicly disclosed, there is a patch available—so vendors are practicing coordinated disclosure practices.

However, despite the swift availability of patches, many users still do not download and install these patches in a timely manner, according to Cisco research. The gap between the availability and the actual implementation of such patches is giving attackers an opportunity to launch exploits—that is, time to operate within a network that could have blocked their entry with a simple software patch. The bad actors could start their path to exploitation even before a vulnerability has been publicly disclosed. Therefore, closing the window between patch availability and installation is critical for defense.

To help close that window, vendors have adopted various forms of an auto-update capability for their products. These range from periodic checks with user notifications, to opt-in and opt-out background updates that are increasingly difficult to disable.

Depending on the auto-update policy, users can opt to delay an update until a more convenient time in the future or, sometimes, skip the update completely. In studying the installations of browser software on endpoints used by Cisco customers, we can see the value of automatic updates. An examination of installation of the Google Chrome web browser, which has instituted a strong opt-out policy, shows that most users (60 percent to 85 percent of the user base as the strength of the auto-update policy increases) are running the latest version of the software, demonstrating the value of auto-update.

At worst, 75 percent to 80 percent of users are using the newest version of the browser, or are one version behind (Figure 14). Google increasingly makes it harder to run old versions of its browser: turning off auto-updates requires administrative access, and the vendor does not allow old versions to be downloaded from its own site or other sites.

Auto-update policy is a big influencer of which versions users are running—not simply the existence of auto-updates. All software examined by Cisco has some type of system for auto-updates, ranging from user notification pop-ups to silent and automatic operation, unless the user has gone to great lengths to actively disable the process. The stricter the policy, the more the desired behavior becomes visible.

Figure 14. Chrome Installations by Version (Top 50 Percent of Users)

Note: The time-to-patch charts in this section show results for the top 50 percent of the populations studied. By highlighting a simple majority of the population, it is easier to see whether updating is working as intended, or whether there are more pervasive barriers to securing the customer base.

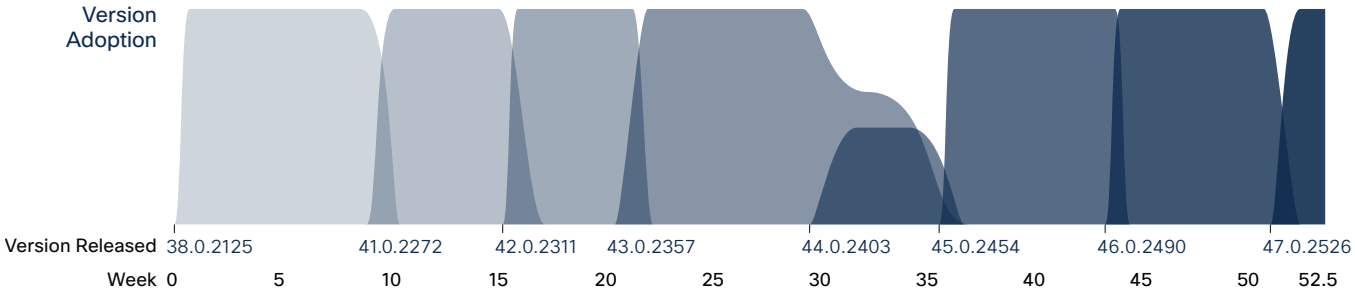


Figure 15. Java Installations by Version (Top 50 Percent of Users)

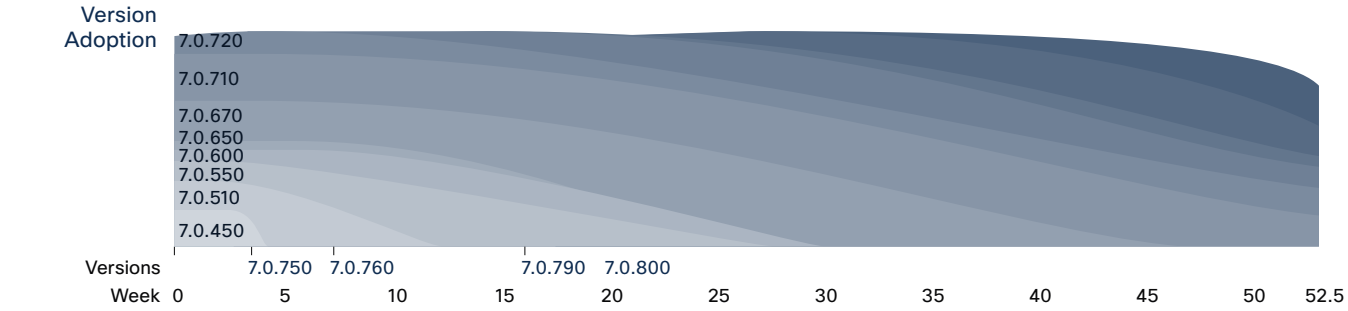
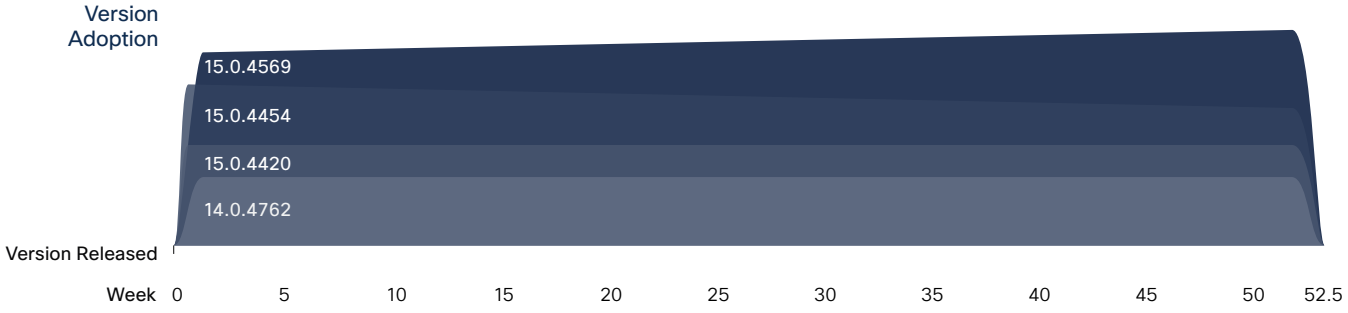


Figure 16. Microsoft Office Installations by Version (Top 50 Percent of Users)



Source: Cisco Security Research

When we shift from examining browsers to examining software, we can see the impact of the lack of auto-update policy. In studying installations of Java software on endpoints used by Cisco customers (Figure 15, shown on previous page), Cisco researchers also detected indicators of compromise (IOCs): one-third of the systems examined are running Java SE 6, which is being phased out by Oracle; the current version is SE 10. (The actual percentages were 33 percent at the beginning of the 1-year period examined, and 23 percent at the end of the 1-year period.)

In addition, many users who have installed the most recent versions of Java may still have old major versions remaining on their system used to support other software, or may simply have not removed them, which means versions with known vulnerabilities are still available—and in an exploitable state. Users' other defenses, such as intrusion prevention systems, may offer some protection, but it's not a guarantee. If the defenses on the endpoint do, in fact, lack other protections, then the risk is even greater.

In examining installations for Microsoft Office (Figure16, shown on previous page), we see the challenges of enterprise management of the suite. Although there are weak auto-update behaviors, the bulk of the population is on a set version and remains on that version. When the upgrades involve license or IT support costs, or users fear a functionality change that modifies the behavior of a productivity tool delivered in the same package as a security fix, these factors can add to existing patching challenges.

There are four major versions of Office available during the analyzed time period, though the newest version's release saw little meaningful uptake. Across the three major versions with significant adoption, the breakdown by percentage is roughly 28-52-20, with minor migrations upward over the course of the year. Major version jumps require a licensing event, while minor version updates are part of the normal software maintenance lifecycle. We would expect to see most of the population of a major version all operating on the newest service pack version, but when looking at the newest version (Office 2013/ version 15x), the three major security update points we divide by are split almost evenly.

The bottom line: Many large vendors are holding up their end of the security bargain by releasing notifications, fixes, and distributions of vulnerability patches in a timely manner. But this attention to patching is not reflected in end users—and, as a result, they are compromising the safety of themselves and their businesses.

In addition to taking advantage of rapid patch releases, security professionals should also examine the use of auto-update features as a useful tool for timely patching. Understandably, some systems are easier to apply auto-updating to than others. For example, browser updates are the lightest-weight updates for endpoints, while enterprise applications and server-side infrastructure are harder to update and can cause business continuity problems. They are therefore less likely to be addressed frequently. Security professionals must prioritize updating and patching in order to secure networks against known and obvious threats.

Adding to the challenge, security releases are often mixed with functionality releases, which can cause users to avoid updating because it will change the functionality they currently use. The mix of releases increases the support burden and complexity for the vendor.

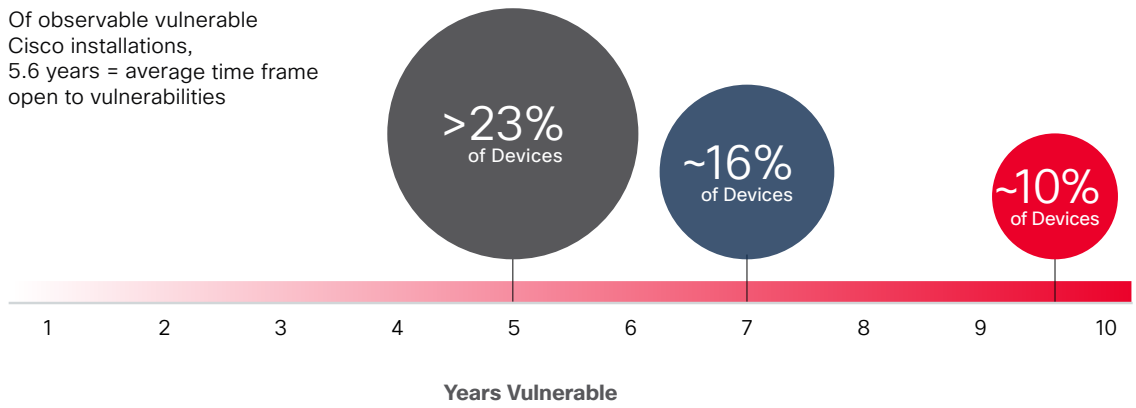
Aging Infrastructure: Ransomware's Rise Makes Patching Long-Standing Vulnerabilities an Urgent Imperative

In 2015, Cisco analyzed 115,000 Cisco devices on the Internet and across customer environments to draw attention to the security risks due to organizations not properly maintaining aging infrastructure or patching vulnerable operating systems.[4] We found that 106,000 of the 115,000 Cisco devices—92 percent—had known vulnerabilities in the software they were running.

For this report, we wanted to examine a sample set of Cisco devices to determine the ages of known vulnerabilities that are running on fundamental infrastructure (routers and switches). Our sample consisted of 103,121 Cisco devices on the Internet (observable installations with known CVEs dating from 2002–2016). Each device was running, on average, 28 known vulnerabilities.

The devices in this sample had been running known vulnerabilities for an average of 5.6 years. More than 23 percent of these devices had vulnerabilities dating back to 2011. Nearly 16 percent had vulnerabilities that were first published in 2009. And almost 10 percent had known vulnerabilities older than 10 years (Figure 17).

Figure 17. Percentage of Devices Running Known Vulnerabilities by Age

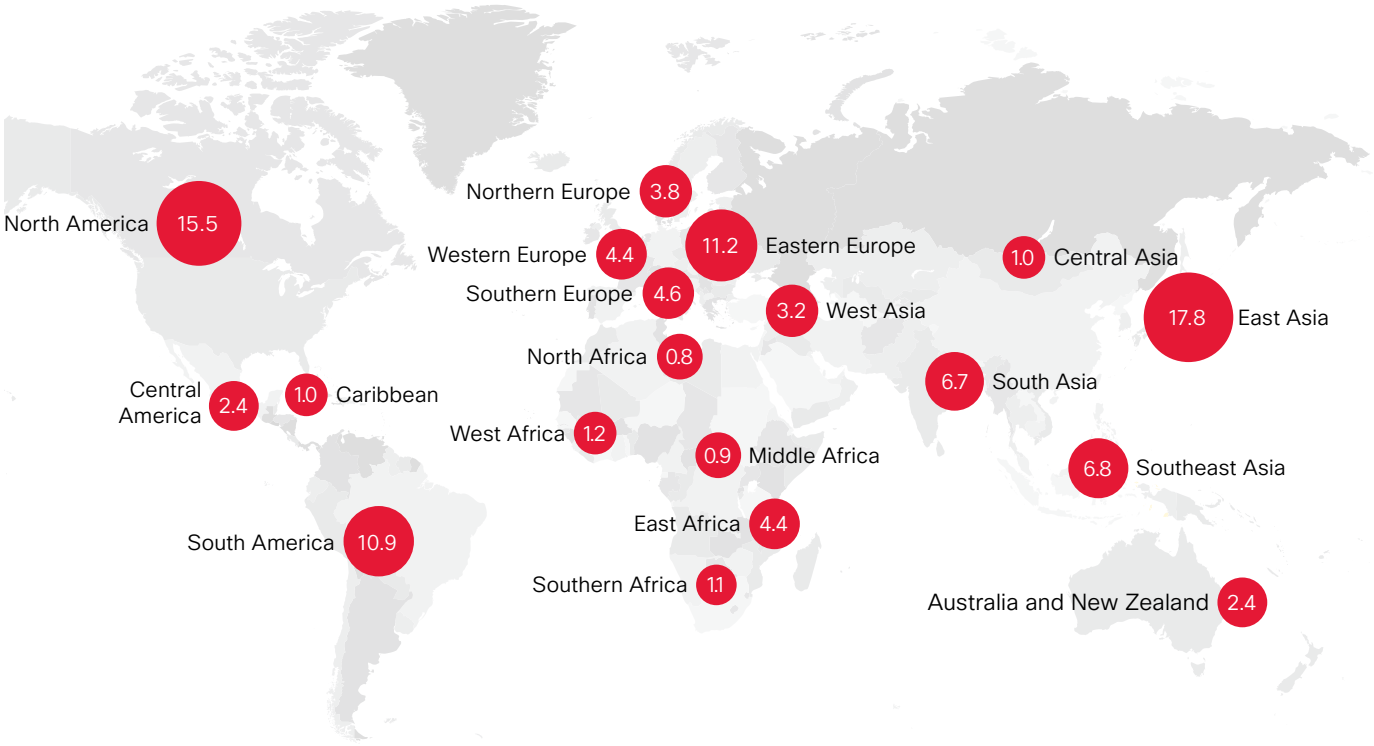


Source: Cisco Security Research

SHARE

[4] Cisco identified the 115,000 devices in our 1-day sample by scanning the Internet and then looking at the devices from the "outside in" (from the Internet view and into the enterprise). For more details on how the analysis was conducted, see the Cisco 2016 Annual Security Report, available here: **cisco.com/go/msr2015**.

Figure 18. Percentage of Vulnerable Cisco Devices by Region



Source: Cisco Security Research

The highest percentages of vulnerable Cisco devices are located in East Asia (17.8 percent) and North America (15.5 percent), according to Cisco researchers. (See Figure 18.)

SHARE

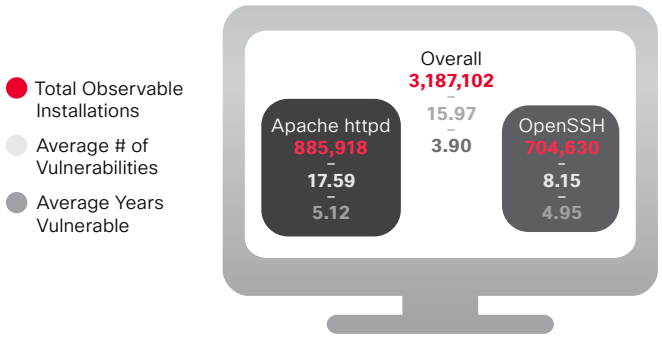
Point of Comparison: Vulnerable Software Infrastructure

Cisco researchers examined vulnerabilities in popular software infrastructure to determine whether organizations were more diligent about patching known vulnerabilities in these products (Figure 19). Our sample of more than 3 million observable installations with vulnerabilities included a wide range of products, but the majority were either Apache httpd (885,918) or OpenSSH (704,630). The average number of known vulnerabilities for these software products was nearly 16.

According to our research, organizations using web-server software have been running known vulnerabilities for 3.9 years, on average.

As for regional findings, we observed the highest number of vulnerable software installations in North America, Western Europe, and Eastern Europe (Figure 20).

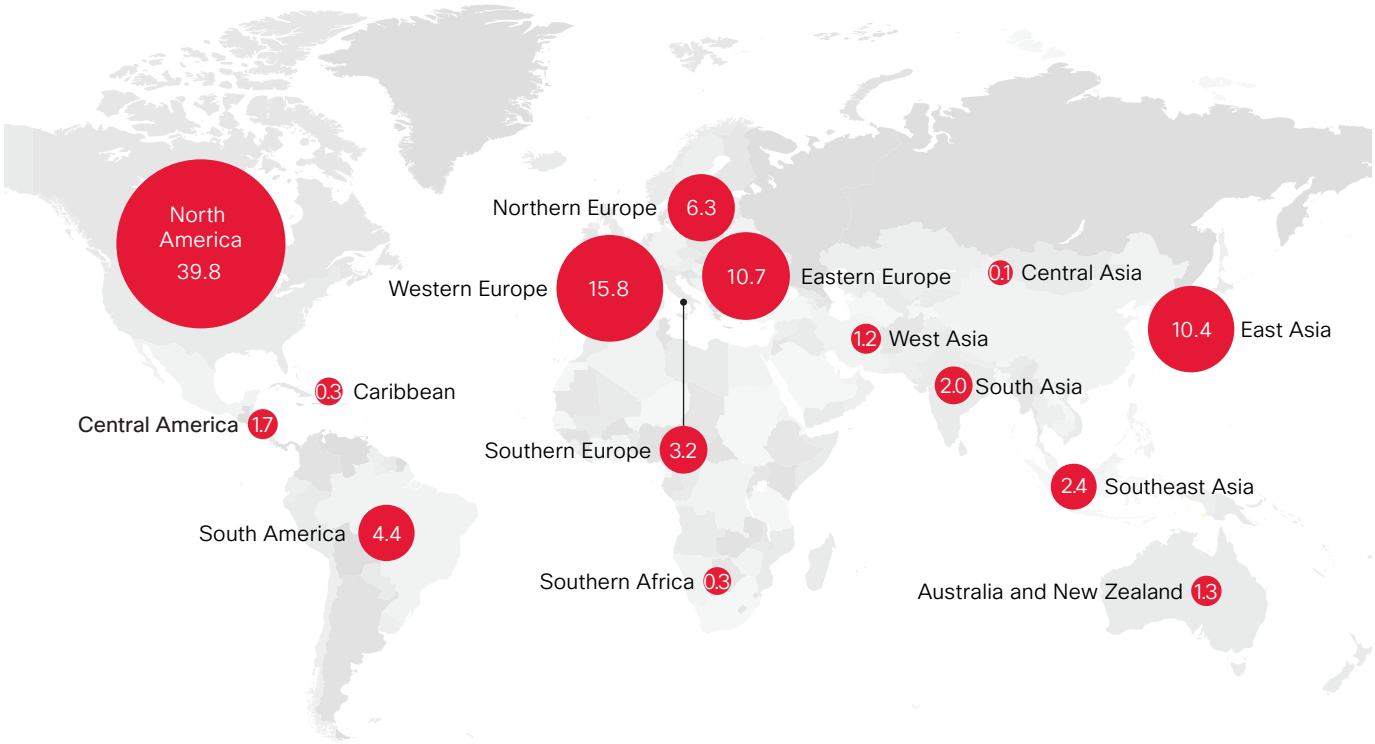
Figure 19. Number of Vulnerable Software Installations by Product



Source: Cisco Security Research

SHARE

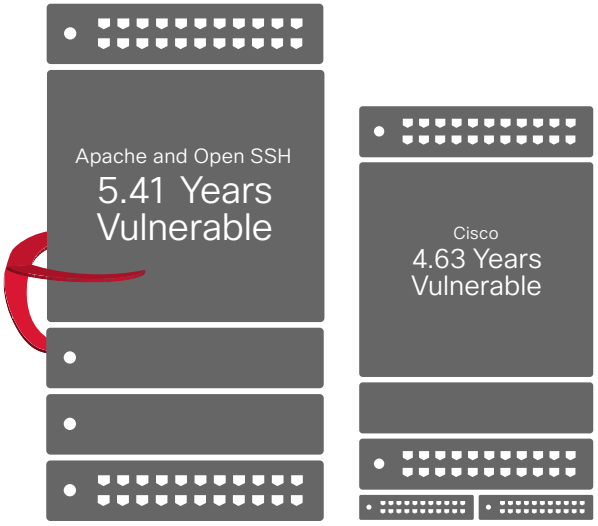
Figure 20. Percentage of Vulnerable Software Installations by Region



Source: Cisco Security Research

Our analysis of Cisco, Apache and OpenSSH products finds that organizations are not diligent about addressing known vulnerabilities in either group of products (Figure 21). Some may simply wait to replace their infrastructure rather than go through the hassle of upgrading—or they may find they have waited so long that they can't upgrade their products because they are no longer supported. In any case, we found that products run with known vulnerabilities for about 5 years, on average.

Figure 21. Software Hygiene Overview: Cisco Versus Apache and OpenSSH



Source: Cisco Security Research

SHARE

No More Delays: The Time for Action Is Now

Although it can be time-consuming and costly for organizations to upgrade their network infrastructure, a failure to make necessary updates offers greater opportunity for attackers. The SamSam ransomware campaign (see **page 7**) is proof that adversaries can take advantage of long-standing, known vulnerabilities in Internet infrastructure to launch highly targeted attacks that are paralyzing and costly for organizations caught unaware. (See "JBoss: Vulnerabilities in Infrastructure Provide Attackers with Time to Operate," **page 18**.)

It is especially important for organizations to keep in mind that all of the product installations included in our analysis can be observed externally by parties who have the right tools and expertise. These parties include threat actors.

It is imperative for organizations around the world to prioritize addressing the problem of aging infrastructure and systems. This is not just about patching old vulnerabilities that have been left to fester, but also assessing the overall strength and cyber-resilience of deployed infrastructure and systems. The time has come for many organizations to face the reality that they must move away from products that are no longer supported and cannot be upgraded to meet today's security challenges.

There are indications that developing nations are lagging behind in these efforts, as Figures 22 and 23 illustrate.

SHARE

Figure 22. Mean Years That Cisco Devices Have Been Vulnerable by Region

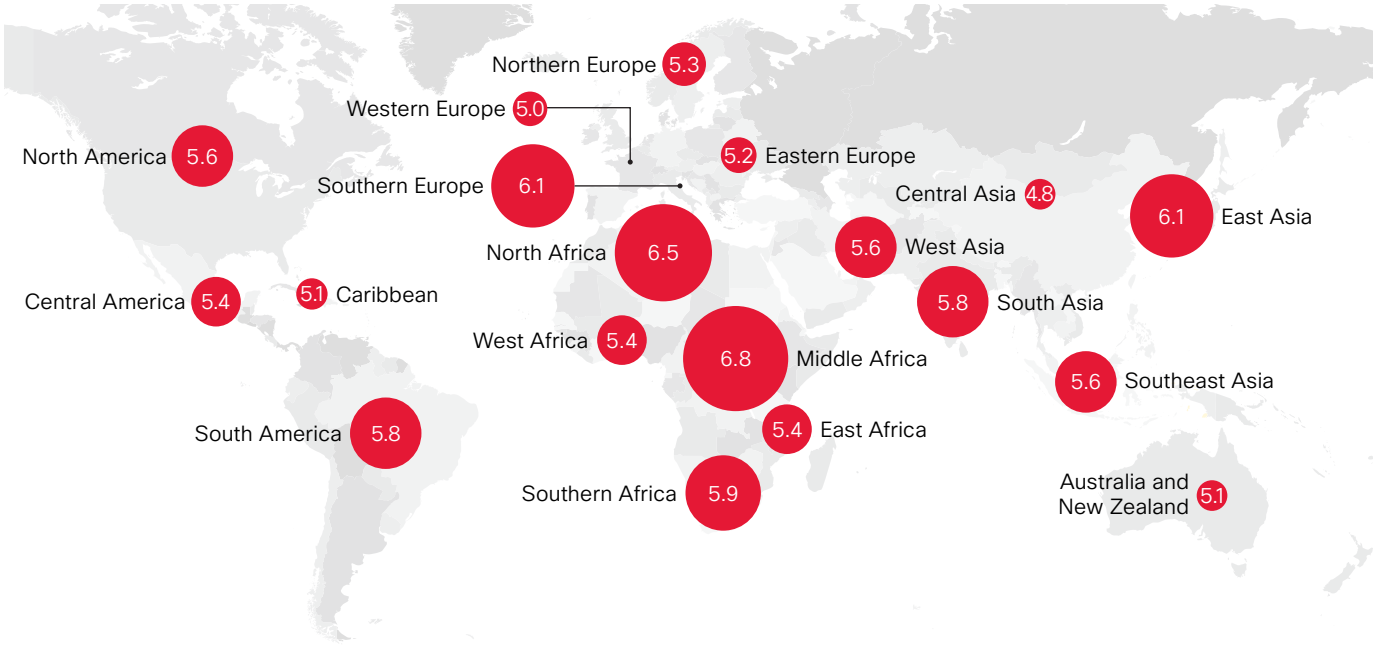
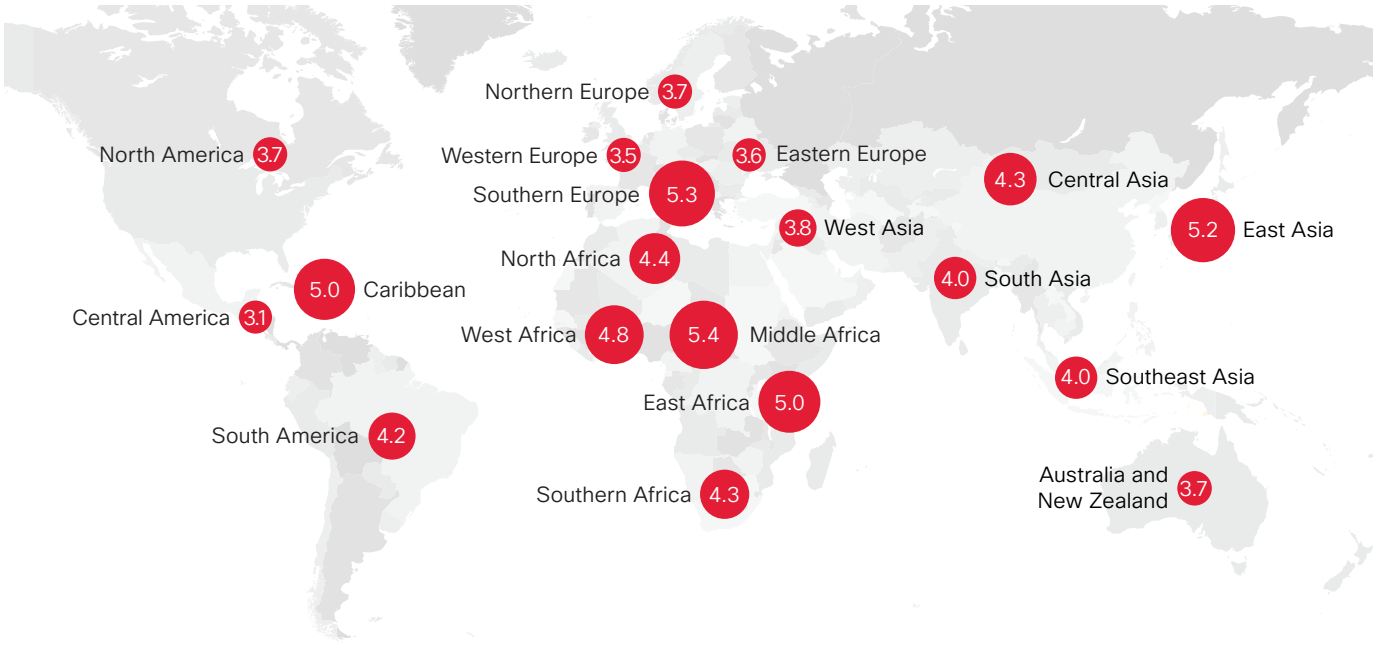


Figure 23. Mean Years That Various Types of Server Software Have Been Vulnerable by Region



Source: Cisco Security Research

Fragile, insecure infrastructure cannot support the emerging next-generation digital economy. To truly realize the benefits that digitization and the Internet of Things will bring, organizations need to tackle the security problems of the first digital wave.

These issues are due partly to lack of foresight about the need for security to be built into Internet infrastructure. No one knew in the early days of the Internet that infrastructure would become a target for attackers. But the security problems in aging infrastructure can also be attributed to simple procrastination by organizations aware of fixes for known vulnerabilities. Instead of facing the calculated risk of taking critical infrastructure offline temporarily for an upgrade, they are placing a bet on the slim-to-none chance they won't be targeted by attackers.

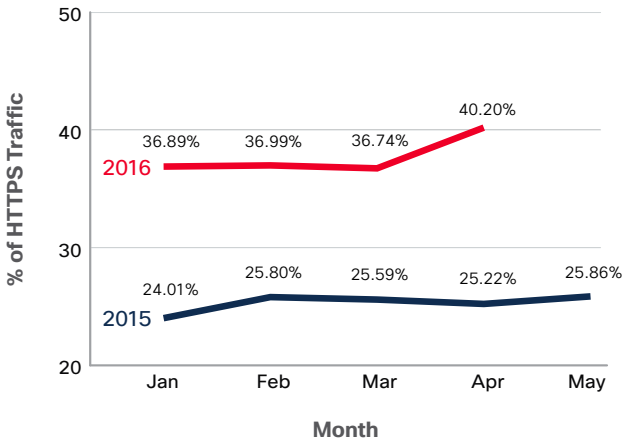
"Fragile, insecure infrastructure cannot support the emerging next-generation digital economy. To truly realize the benefits that digitization and the Internet of Things will bring, organizations need to tackle the security problems of the first digital wave."

Encryption: HTTPS Traffic Stable in 2016 ... So Far

As explained in our last security report, encryption has become a favored tool for organizations seeking to protect sensitive data as well as customer privacy. From January to April 2016, the volume of HTTPS requests remained relatively stable, following a gradual but significant increase overall during 2015.

Judging from the 2015 growth in use of encryption, security industry experts anticipate a greater use of encryption, even though 2016 traffic to date is showing only a small increase (Figure 24).

Figure 24. Encrypted HTTPS Traffic Relatively Stable in 2016 to Date

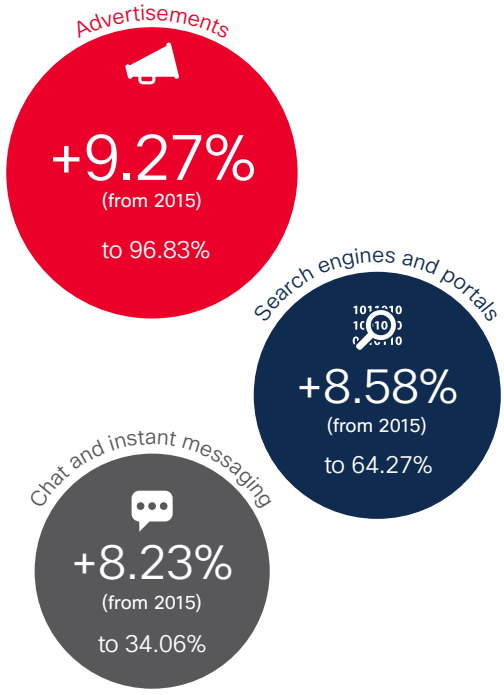


Source: Cisco Security Research

Advertising showed an increase in HTTPS traffic during the first four months of 2016 (see Figure 25). The increase is most likely due to the industry wishing to protect user privacy and to disrupt malicious campaigns. However, it is possible that the increase is a reflection of greater use of HTTPS by developers of malicious campaigns: ad injectors, which are the main component in adware infections, have become the major source of the increase in the number of malicious campaigns using HTTPS.

The top three applications using HTTPS are organizational email, chat and instant messaging, and web-based email, as seen in Figure 26.

Figure 25. HTTPS Malware Traffic Increase January 2015–April 2016



Source: Cisco Security Research

The steady use of encryption by legitimate organizations is generally good news for users—although not such good news for security professionals. Criminals have also recognized the value of encryption for hiding their activities from defenders, allowing bad actors more time to continue their activities uninterrupted (see **page 22** for details on malware authors' use of HTTPS). Without a view into the indicators of compromise (IOCs) hidden by encrypted traffic, the effectiveness of point solutions is reduced, and defenders have a tougher job of spotting malicious activity before it causes lasting damage.

SHARE

Figure 26. Top Applications Using HTTPS

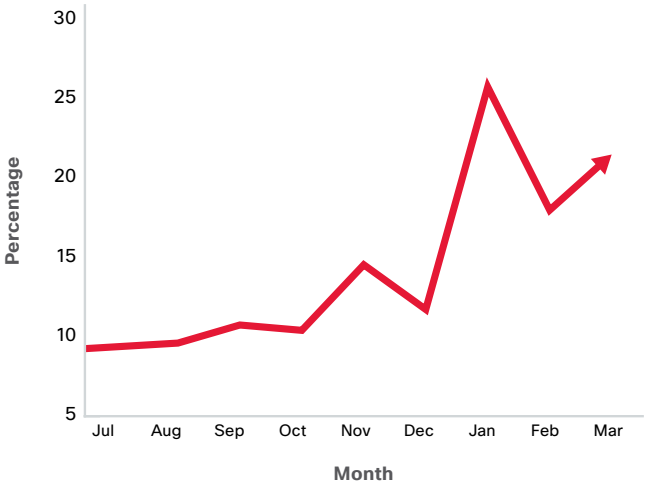
Category Jan–Apr	% Avg. HTTPS
Organizational Email	97.88%
Chat and Instant Messaging	96.83%
Web-Based Email	96.31%
Online Storage and Backup	95.70%
Internet Telephony	95.07%
Professional Networking	90.78%
Social Networking	81.15%
File Transfer Services	67.63%
Streaming Video	64.71%
Search Engines and Portals	64.27%
Photo Search/Images	61.90%
Webpage Translation	54.60%
SaaS and B2B	54.36%

Source: Cisco Security Research

TLS Encrypts Payloads but Doesn't Hide Malware Behavior

In their ongoing quest to operate undetected for longer periods of time, malware creators and users often choose technology tools commonly used for legitimate purposes. A new favored choice of attackers may be Transport Layer Security (TLS), the dominant protocol used to provide encryption for network traffic. By observing unencrypted TLS headers, Cisco researchers have found that a small but growing number of malware samples show the use of TLS for protected communications—a cause for concern among security professionals, since it makes deep-packet inspection ineffective as a security tool.

Figure 27. Percentage of Malware Samples Using TLS



Source: Cisco Security Research

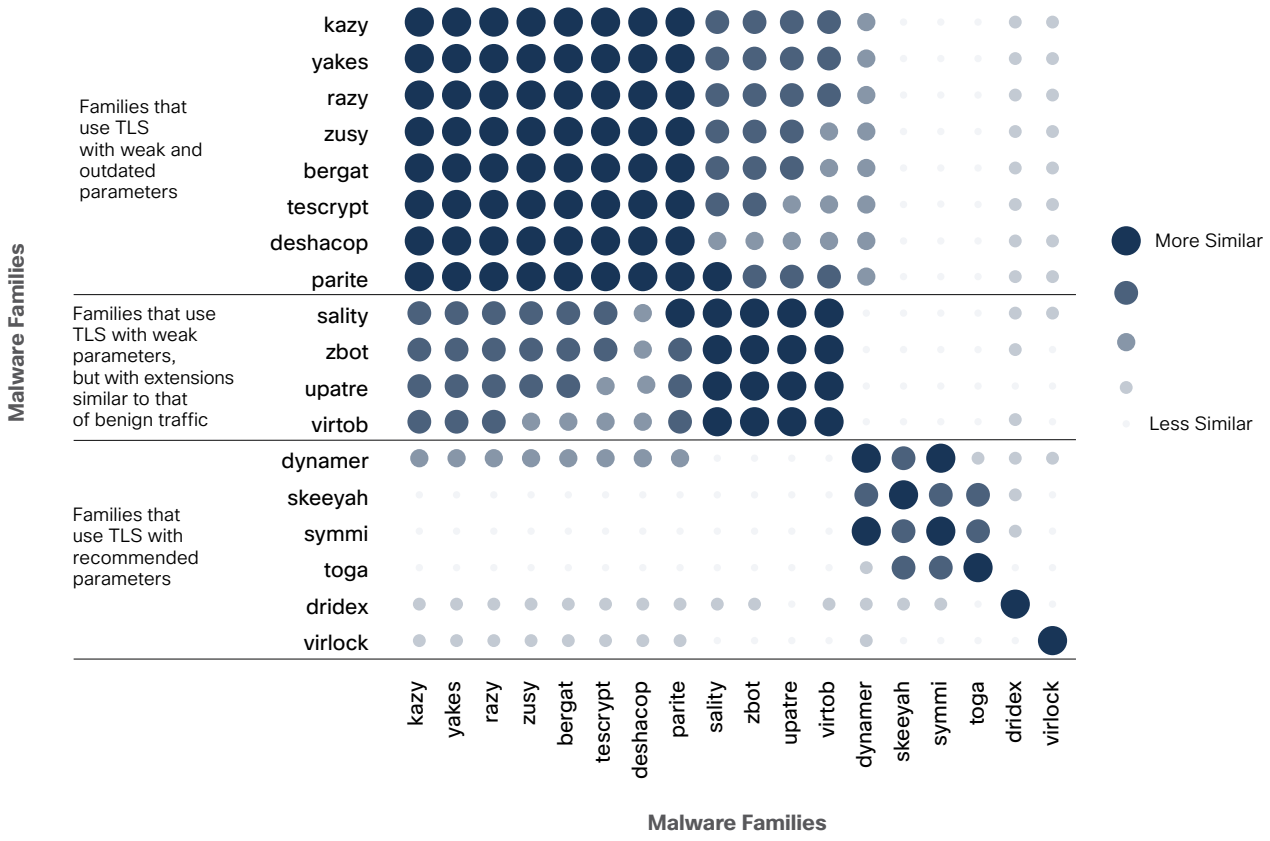
According to Cisco researchers, as much as 60 percent of all network traffic uses TLS for encryption. In the malware samples studied by researchers, about 10 percent of the malware used TLS. This percentage may seem low, but researchers believe the number will increase as the overall use of encryption in benign traffic increases. They observed an increase in malicious encrypted traffic between July 2015 and March 2016 (Figure 27).

Knowing that bad actors may be stepping up their use of TLS, how can security professionals use this knowledge to improve the detection of malware that uses such tactics? Malware's use of TLS is distinct from that of benign traffic, and for most malware families this fact can be used to classify malicious traffic patterns with high accuracy.

As researchers discovered, malware creators typically use older cryptographic parameters than what is seen in benign network traffic. The older cipher suites used for malware may offer an indication that the traffic is malicious. Benign applications are more likely to use current TLS best practices, probably because there is incentive to differentiate their products by providing more security.

Malware users, on the other hand, choose older cryptography libraries because they are proven to work in many operating environments and won't result in errors. As an example of the type of errors that could disrupt malware encryption, the libraries that the malware executable expected to be on the host were not there, in which case the executable could not run.

Figure 28. Similarity of Malware Families in Comparing TLS Parameters



Source: Cisco Security Research

In an effort to find patterns in the way malware families use TLS, researchers examined 18 malware families, thousands of unique malware samples, and tens of thousands of encrypted network flows. They identified malware families in several ways:

- Those that use TLS with recommended parameters, such as Skeeyah malware
- Those that use TLS with weak parameters but with extensions that are similar to that of benign traffic, such as Sality
- Those that use weak and outdated parameters, such as tescrypt

As seen in Figure 28, researchers were able to demonstrate that some malware families show similarities in how they use TLS encryption.

SHARE

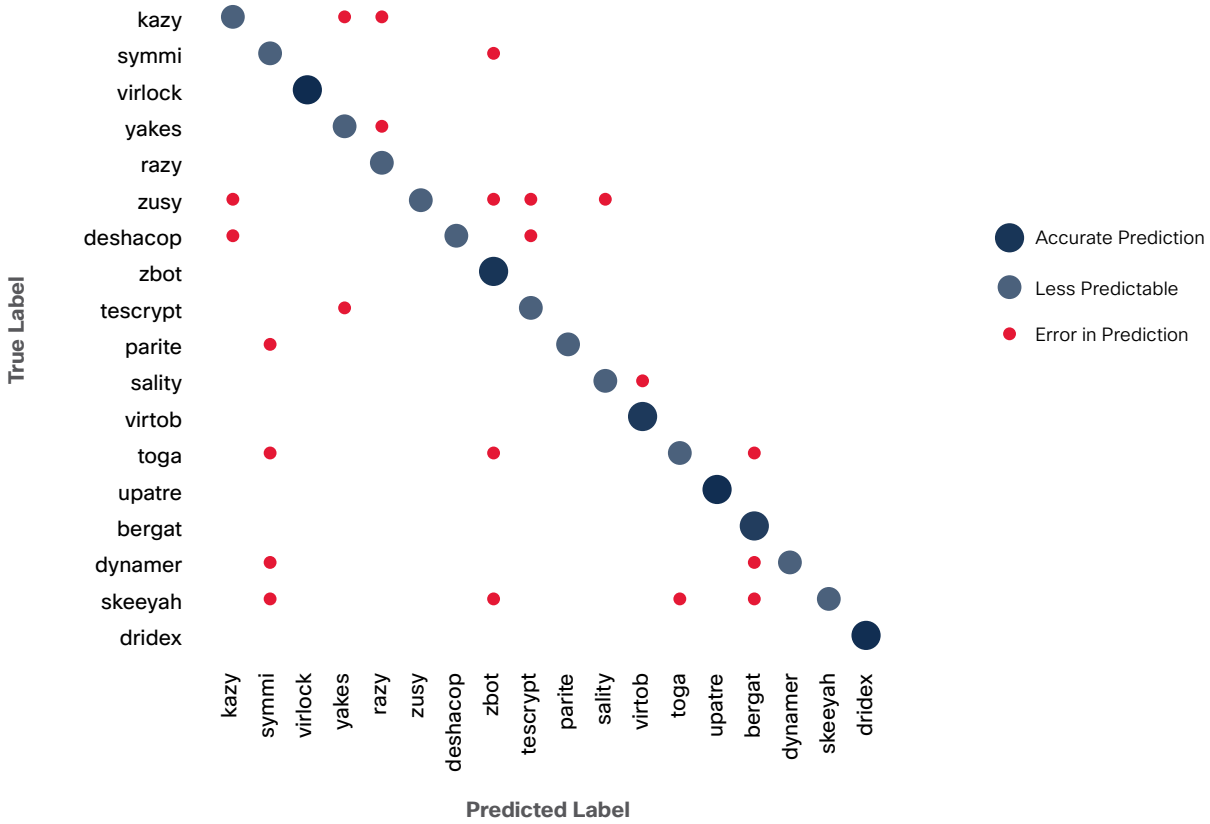
The confusion matrix (Figure 29) shows how easy it is to distinguish among different malware families. The predicted label is likely to match the true label (indicated by a large circle), and incorrect predictions are much less likely (indicated by a small circle).

Not surprisingly, malware families that actively evolve their use of TLS are more difficult to classify. However, researchers found that if they applied domain-specific knowledge about the traffic being examined, such as whether the TLS certificate was self-signed, they could identify patterns with greater accuracy. For example, they were able to accurately attribute network communications to a specific malware family, even when restricted to a single encrypted flow, with an accuracy of 86.8 percent. This validates the need for, and the advantage of, an integrated threat defense, specifically using machine-learning techniques in addition to naïve categorizations. The combination of machine-learning methods and novel data views provides higher-quality information to security professionals.

The ability to accurately attribute malware samples to a known malware family can be valuable to security professionals. Such attribution tells incident responders about the type of threat they may be dealing with before they begin to reverse-engineer the malware samples. In addition, examining encrypted traffic flows can help incident response teams better to prioritize their time—for example, assigning more resources to the most serious malware infections.

SHARE

Figure 29. Confusion Matrix: Distinguishing Among Various Malware Families



Source: Cisco Security Research

Time to Detection Trends Highlight a Heated "Arms Race"

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

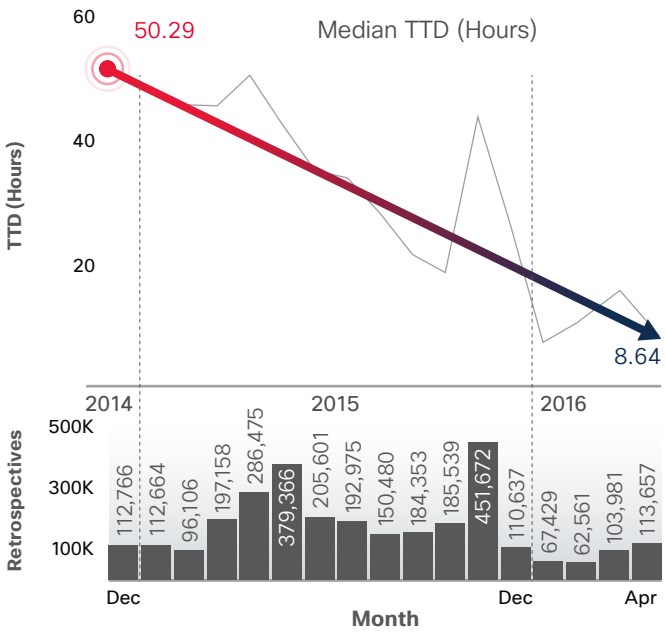
Since the end of 2014, we have been tracking our progress toward narrowing the window on TTD. A year ago, we reported that the median TTD was about two days (50 hours).[5] By October 2015, Cisco had dramatically reduced the median TTD to about 17 hours.

For the period from December 2015 through April 2016, the median TTD was even lower: about 13 hours. That figure is the weighted average of the five medians for the period observed.

Our median TTD is far below the industry estimate of 100–200 days, and we continue to accelerate our ability to detect a wide number of threats. The overall decline in TTD Cisco achieved from December 2014 through April 2016 is illustrated in Figure 30.

The steady downward trend in median TTD is clear in Figure 30. There are also a number of significant peaks and valleys along the line. They are evidence of the "arms race" between attackers and defenders.

Figure 30. Median TTD by Month, December 2014–April 2016



Source: Cisco Security Research

SHARE

"Our median TTD is far below the industry estimate of 100–200 days, and we continue to accelerate our ability to detect a wide number of threats."

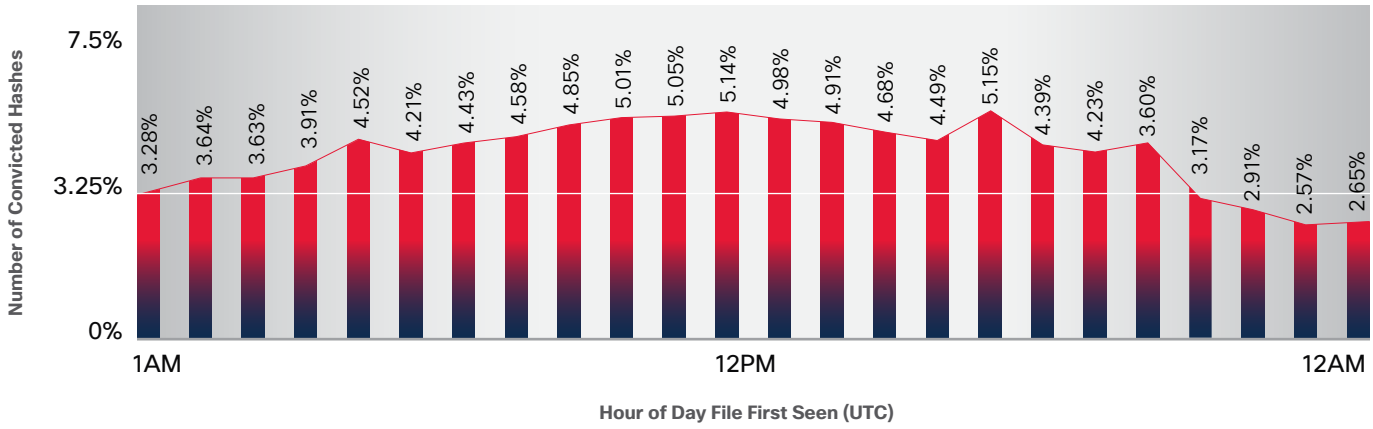
[5] Cisco 2015 Midyear Security Report, available here: **cisco.com/go/msr2015**.

Adversaries continually create stealthy techniques to avoid detection. Security vendors counter these efforts with better integration and threat detection. They then integrate the IOCs they identify into automated detection technologies and add context to that data so it becomes actionable threat intelligence for customers. (See "Indicators of Compromise Are Not Threat Intelligence," on **page 53**.)

Significant drops in TTD show periods when Cisco gained an edge on the adversaries–detecting threats at a rate faster than they could develop and launch new techniques. The peaks indicate periods when adversaries struck back with innovations that required analysts' work or other intelligence sources to detect–thus moving the median TTD upward.

The arms race between attackers and defenders is relentless. Adversaries unleash a constant barrage of new threats that security vendors must move swiftly to identify. Figure 31 shows the number of convicted hashes (files) seen on a typical day during the period observed (December 2015–April 2016). Overall, the rate of conviction is fairly consistent throughout the day.

Figure 31. Convicted Hashes by Hour of Day



Source: Cisco Security Research

SHARE

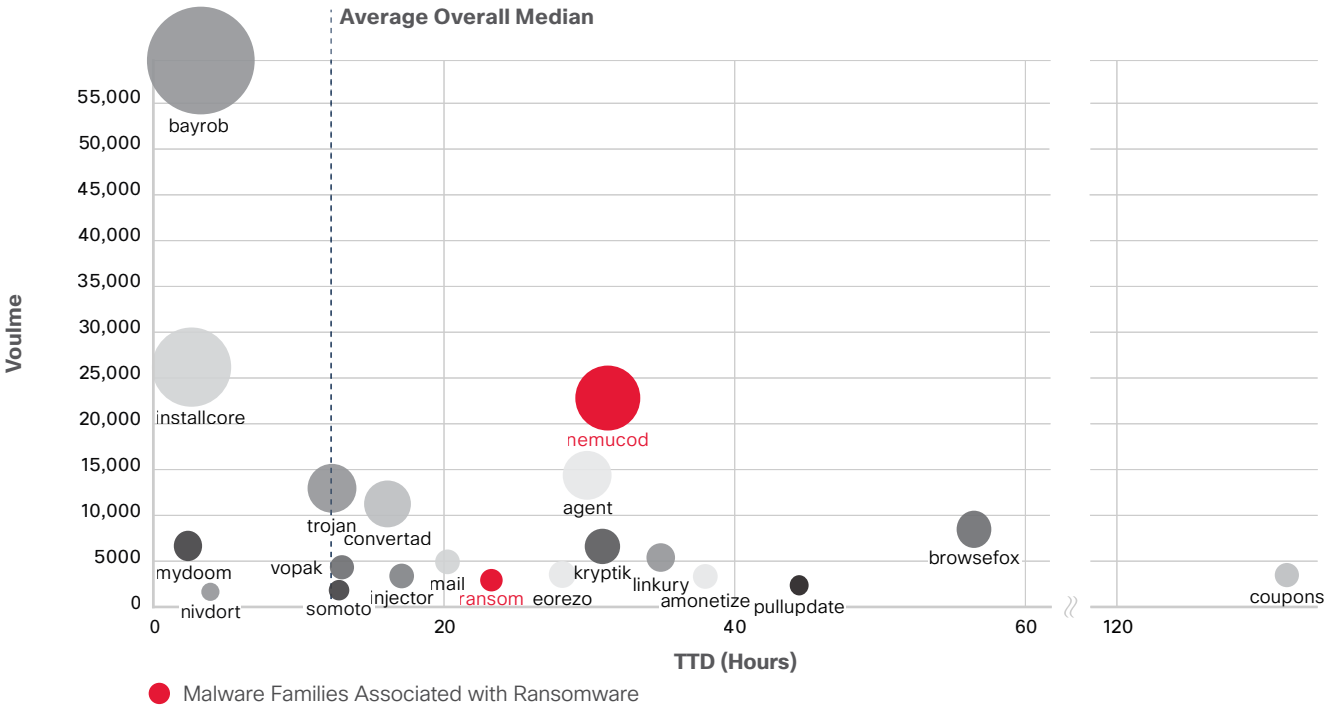
"Significant drops in TTD show periods when Cisco gained an edge on the adversaries–detecting threats at a rate faster than they could develop and launch new techniques."

Ransomware Explosion a Factor for Recent Median TTD Fluctuations

As we noted in our last cybersecurity report, the industrialization of the shadow economy and the greater use of commodity malware have been strong factors in our ability to reduce TTD consistently and significantly since December 2014. Industrialized threats quickly spread, making them easier to detect.

Malware families that Cisco detected at or near the median TTD (about 13 hours) in the first five months of 2016 are old but still pervasive threats. Two examples are Bayrob, botnet malware that has been around since 2007 and that saw a resurgence earlier this year, and Mydoom, a computer worm spread through email that was first observed in 2004 and affects Microsoft Windows. Well-known malicious adware InstallCore was also prevalent, likely because of its role in helping to distribute ransomware (Figure 32).

Figure 32: TTD Medians of Top Malware Families (Top 20 Families by Detection Count)



Source: Cisco Security Research

SHARE

The explosion in ransomware over the past year is a factor for increasing use—and therefore, more detections—of certain malware families.

TTD trended higher than the median for several malware families associated with ransomware due to the time required for analysts to investigate these threats when automated techniques such as heuristics and sandboxing were unable to provide early detection.

Figure 33 presents month-to-month trends in the top malware families that Cisco detected from January through April 2016. The highlighted names are examples of malware families associated with ransomware. Growth or decline in adversaries' use of certain malware families results in fluctuations in the median TTD. Threats that required investigation by Cisco analysts to detect pushed up the median TTD in March 2016 to more than 14 hours from just over 9 hours in February.

Figure 34 underscores the challenge for defenders working to reduce TTD—as well as the need for organizations to employ an integrated threat defense. Threats that can be detected earlier than the median TTD are identified through automated techniques, such as sandboxing. Emerging and more sophisticated threats require the use of internal or third-party investigation and intelligence, and therefore take longer to detect.

Malware campaigns come and go, but one thing is constant: the adversarial relationship between attackers and defenders. Adversaries must continually come up with threats that can evade detection so they can increase the time they have to operate. And defenders must counter these efforts by continually hunting for new and emerging malware, integrating the IOCs they find into their automated detection technologies, and turning their findings into real threat intelligence.

Cisco is committed to continually reducing our median TTD in the months ahead. We recommend that other organizations measure their own median TTD so that they can begin a track toward improvement and help reduce the current and unacceptable industry estimate of 100–200 days.

Better TTD and TTP (time to patch) practices and the use of encryption, along with proactively addressing the issue of aging infrastructure, all help to reduce the unconstrained operational space of adversaries. TTD and TTP, in particular, serve as key performance indicators that allow defenders to focus on where and how they can improve their ability to detect the presence of an adversary—and limit the attacker's ability to change tactics and escape identification.

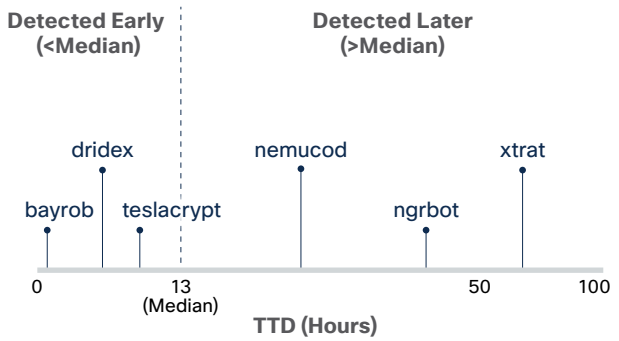
Figure 33. Top 10 Malware Families Detected by Month

	January	February	March	April
1.	bayrob	downloader	downloader	bayrob
2.	downloader	installcore	nemucod	downloader
3.	installcore	convertad	agent	installcore
4.	agent	msil	installcore	nemucod
5.	convertad	browsefox	convertad	agent
6.	ransom	linkury	mydoom	convertad
7.	linkury	nemucod	msil	fareit
8.	kryptik	agent	browsefox	msil
9.	browsefox	kryptik	kryptik	trojan
10.	msil	mydoom	vilsel	heur

● Malware Families Associated with Ransomware

Source: Cisco Security Research

Figure 34. Examples of Early and Late Detection of Malware Families, Based on Median TTD of 13 Hours



Source: Cisco Security Research

Incident Response: Practices That Impair Organizational Security

News of network breaches, ransomware attacks, and cleverly crafted malware makes the rounds in security media, as does the impact of such incidents, such as business shutdowns and brand reputation damage. However, the likelihood of such attacks still seems to take many organizations by surprise—organizations that believe their threat detection and incident response systems are robust, even when they're actually quite permeable.

These organizations are often using security technology and practices that may be a dozen years behind current offerings. So, when an attack does happen, generalist security professionals can quickly become overwhelmed by the demands of incident response, which can require specialist skills.

Cisco consults with organizations of all sizes about their security readiness and routinely sees a lack of best practices that could help harden security. The team also finds that bad actors recognize these weaknesses and use them as an opportunity to gain entry to networks.

For example, companies entering into merger and acquisition (M&A) deals may not conduct enough due diligence on the risk posture of the partner business. They may realize the shortcomings of the newly combined businesses after the deal is done, when it is too late to remediate problems or when it's harder to do so because the networks are now intertwined. Chief information security officers (CISOs) should fully assess security protections before entering into an M&A transaction. At the very least, they should make sure there is no evidence of suspicious activity in the respective networks before a cutover.

Poorly assessed networks can allow bad actors extra time to remain in networks, as can poor practices such as weak passwords or the frequent use of administrative rights. Another sign that organizations are not prepared to combat sophisticated threats is a lack of awareness about what has affected their networks in the past. An organization that reports it has never suffered a network breach is not one with true visibility into its own network activity. Any mature organization will experience some level of activity in terms of commodity malware and attempts to breach its defenses.

Cisco also observes organizations lacking self-awareness about their appeal to attackers. Industries such as healthcare have become more attractive to bad actors in recent years because they offer the combination of valuable data with traditionally weaker security (see **page 45**). In addition, Cisco has noted that attackers are turning their attention to vulnerable institutions such as schools because they know that security defenses may be minimal. For best practices that can support an effective incident response, see "Security Recommendations" on **page 52**.

"An organization that reports it has never suffered a network breach is not one with true visibility into its own network activity. Any mature organization will experience some level of activity in terms of commodity malware and attempts to breach its defenses."

Ransomware Attacks in Healthcare Offer Security Hygiene Lessons for All Organizations

The healthcare industry has faced several ransomware attacks this year. In our analysis of Cisco customers in the healthcare vertical that were hit by ransomware attacks, we identified a number of enterprise vulnerabilities that had made infections more likely for these organizations. They include:

- Shared passwords and "overprivileged" accounts
- Insufficient security logging that would allow the detection of compromised passwords
- Web applications with **OWASP** top 10 vulnerabilities
- Unpatched operating systems and applications

Cisco researchers also found that all the PCs in a hospital often run the same vulnerable versions of software like Windows XP, Adobe Flash player, or Java. Of note, most recent ransomware infections of healthcare workstations that we investigated could be traced to clinical staff web browsing from a workstation that was missing Flash player patches.

Lack of a formal process to ensure the timely installation of security patches was also a common theme across our healthcare customers.

In addition, most medical providers targeted by ransomware did not have incident response plans in place, which greatly undermined their efforts to respond effectively to attacks.

Also, few healthcare organizations have dedicated security teams. Maintenance of IT assets is typically handled by one or more IT generalists who lack security expertise.

We recommend that businesses with similar security challenges take the following actions, at minimum, to improve their overall security posture:[6]

- Conduct basic hardening of systems to resist malware and hacking attacks
- Assess the IT landscape in the organization: What and how many devices are on the network? Where are those devices located?
- Educate users about threats and best practices
- Develop an incident response plan
- Monitor the network actively for evidence of compromise

Addressing known security vulnerabilities is also an imperative. Long-standing vulnerabilities in JBoss servers provided threat actors behind the recent SamSam campaign with the ability to move laterally through Internet infrastructure to target healthcare networks (see **page 7**). Cisco researchers anticipate that adversaries will only increase their targeting of infrastructure to enable ransomware campaigns, given the number of vulnerable devices and software across the Internet. (For more information, see "Aging Infrastructure: Ransomware's Rise Makes Patching Long-Standing Vulnerabilities an Urgent Imperative," **page 30**.)

Organizations across industries can learn a great deal from the healthcare industry's experience with ransomware. They should consider taking steps to ensure that the technology staff responsible for managing their security have the tools, resources, and policies in place to do the job effectively.

[6] Note: When making security improvements, organizations should take into account any regulatory compliance mandates or other industry-related directives they must adhere to, as these mandates may impact how the organization specifically approaches certain aspects of security, such as data protection and data privacy.

Global Perspective and Security Recommendations

Global Perspective and Security Recommendations

Malware originates from various positions around the world, and attackers are quick to shift their base of operations from region to region when needed. One thing is clear for organizations that believe they are not a target for adversaries: No vertical is safe from attack. And organizations that try to improve their threat detection and incident response by relying on IOCs, and not true threat intelligence, are actually doing little to improve their security posture.

Meanwhile, businesses also face another uncertainty in an increasingly sophisticated threat landscape: Rising government concerns about the need to control or access data are creating contradicting signals, legislation, and requirements. These concerns may ultimately limit and conflict with international commerce, secure technology, and trustworthy public-private partnerships.

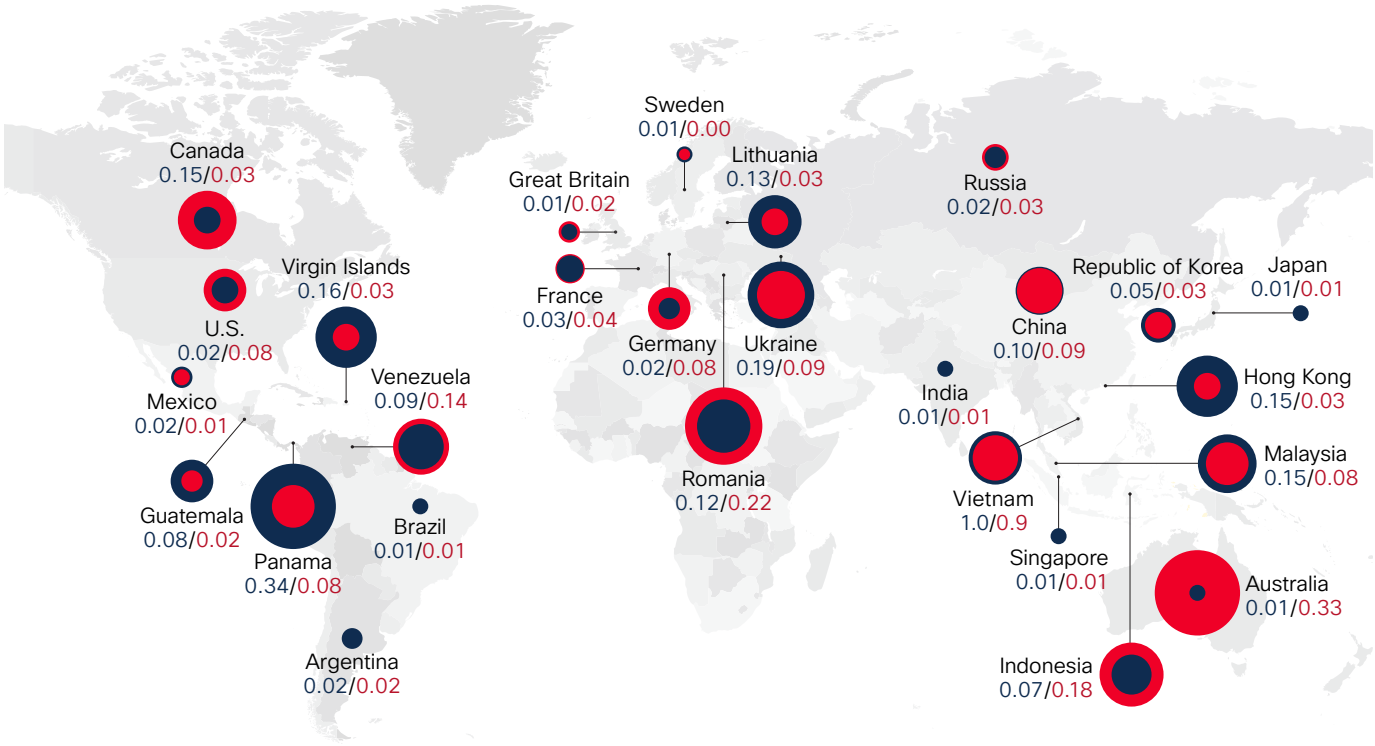
Regional Overview of Web Block Activity

By examining overall Internet traffic volume and block activity, Cisco researchers can offer insights on the origins of malware. In the Americas, Canada appears to be the highest source of blocked traffic outside the United States.

In the Europe, Middle East, and Africa region, Ukraine and Romania were the greatest sources of blocked traffic as a proportion of their overall traffic; and in Asia-Pacific, Australia topped the list (see Figure 35 on the next page).

For various reasons such as the availability of easily hacked servers, attackers will shift their base of operations from region to region.

Figure 35. Web Blocks by Country



Source: Cisco Security Research

SHARE

As with the examination of industry verticals (**page 49**), the bottom line is that no country or region is safe from malware traffic. Malware should be considered a global problem. Certainly some regions and countries may show proportionally higher block activity because attackers have found weaknesses in infrastructure that they can exploit. In addition, a spike in malware activity, which was observed in Australia in December 2015 and January 2016, will result in noticeable shifts in the weight of countries and their blocked traffic.

Vertical Risk of Malware Encounters: No Industry Is Safe

A message for security professionals who believe that their industry is unattractive to online attackers: Your confidence is misplaced. In Cisco's periodic examination of attack traffic ("block rates") and "normal" or expected traffic by industry, it's clear that no vertical is safe from malware. Any industry can fall victim to attackers who will look for space and time to carry out campaigns.

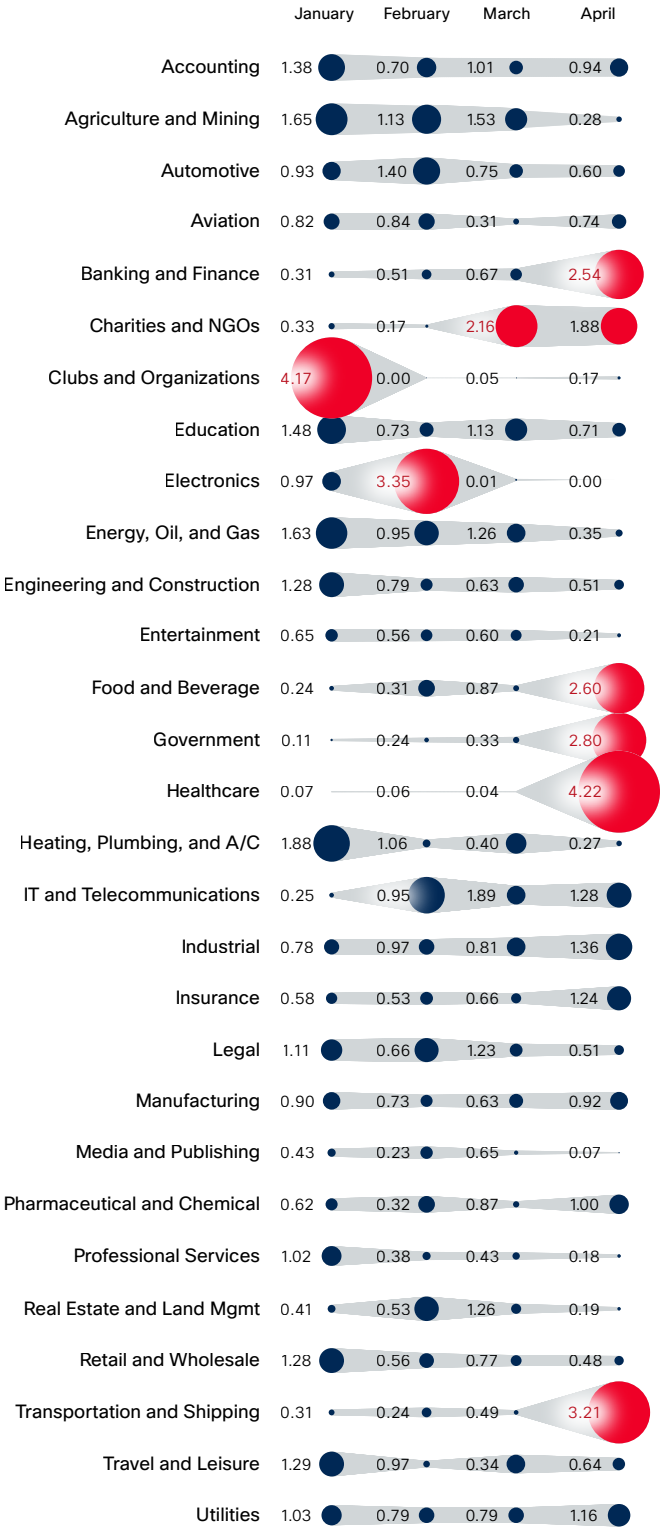
Although healthcare has been in the news as an industry favored by attackers (see **page 7**), Cisco data shows that, in the first few months of 2016, other industries show proportionately large volumes of malware. For example, clubs and organizations, charities and NGOs, and electronics businesses experienced the highest block rates.

The takeaway from this examination of block rates is that every industry is at risk. While the data shows occasional spikes in block traffic from industry to industry, it's clear that attackers are turning their attention to various industries as they see opportunities to compromise networks—and that once they achieve their goal, they move to whatever industry target presents the best return on investment. Campaigns are driven by opportunity, not the industry.

Figure 36 shows the top 29 industries and their relative block activity as a proportion of normal network traffic. A ratio of 1.0 means the number of blocks is proportional to the volume of observed traffic. Anything above 1.0 represents higher-than-expected block rates, and anything below 1.0 represents lower-than-expected block rates.

SHARE

Figure 36. Monthly Vertical Block Rates, January–April 2016



Source: Cisco Security Research

Geopolitical Update: Governments and Businesses Navigate the Data Protection Dilemma

Cybersecurity in a geopolitical context continues to provide technology vendors, telecoms, and other global companies with a complex and often contradictory regulatory world to navigate. It's a situation that sees competing elements of the security issue—governments and businesses on the one hand, privacy and security on the other—in tension with each other.

Data security has become a top-line priority among governments, whether it relates to securing citizens' personal data or to the integrity of physical infrastructure such as national power grids and water systems. Yet governments also want the ability to access data when they need it, such as through lawful intercept.

Governments perceive that they have lost control over technology and access to data and are moving to reestablish some of that control. The need to do so is intensified by terrorist attacks and sluggish global economic growth, forcing elected officials to demonstrate their ability to protect both citizens and commercial enterprises:

- In the aftermath of the Edward Snowden leaks, the debate over the rights of the individual versus the rights of the state has prompted a rethink of agreements such as Safe Harbor. The new EU-U.S. Privacy Shield imposes stronger obligations on U.S. companies to protect the personal data of European citizens from government access.
- The migrant crisis in the European Union (EU) and recent terrorist attacks in Paris, Brussels, Turkey, the United States, and elsewhere have prompted a debate over law enforcement access to encrypted private communications. Global concern over this issue explains the intense focus on the face-off between the U.S. Federal Bureau of Investigation (FBI) and Apple Inc., regarding unlocking an iPhone used by a terrorist.
- Governments and private security companies are also more willing to take action in response to state-sponsored espionage and theft. Attacks against banks using the international financial network SWIFT (Society for Worldwide Interbank Financial Telecommunication) are being attributed to North Korea; the German government recently attributed an attack on its Bundestag to Moscow.

Governments around the world are considering measures that they hope will provide them with a greater degree of control over technology so they can combat threats such as terrorism and cybercrime. In the process, they run the risk of unearthing new vulnerabilities and, in some cases, they are reserving the right to exploit those vulnerabilities. They do not necessarily share all this information with technology vendors, leading to the inevitable question: Where does the responsibility lie with regard to vulnerability disclosure? Commercial enterprises are very much on the front line when it comes to public reaction to heightened government intrusion.

Despite the rapid pace of globalization, there is no unified global response to the broad issue of cybersecurity or related issues such as transparency, accountability, data protection, and encryption. The effort to establish "rules of the road" for a global Internet continues, but differing priorities ensure that enterprises will continue to work in a politicized and legally risky environment.

"Despite the rapid pace of globalization, there is no unified global response to the broad issue of cybersecurity or related issues such as transparency, accountability, data protection, and encryption."

An Evolving Regulatory Landscape

Global telecoms and technology vendors must keep up with the regulations of each country, working within each sovereign nation's rules while satisfying their own country's legal framework and public expectations. But this is a tough road, given the many types of potential legislation that different countries are pursuing.

In the United Kingdom, for example, the government's Investigatory Powers Bill attempts to bring all of the U.K. security services' surveillance powers together under one piece of legislation by the end of this year. The bill is currently being debated in the U.K. Parliament. Politicians, businesses, and human rights groups have highlighted a number of controversial measures in the bill, including what has been cited as a "decrypt on demand" clause that requires technology vendors and telecom providers to potentially remove encryption at the request of U.K. security services.

Other countries are taking further steps—and looking to expedite such measures. For example:

- The EU's own Network and Information Security Directive will be finalized this summer.
- In France, an antiterrorism bill is being pushed through parliament. It carries provisions levying large fines on companies and recommending prison terms for corporate executives who refuse to cooperate in terrorism investigations. Backers of the bill hope it becomes law before the country's extended state of emergency—initiated after the Paris attacks in November—expires.
- The Hungarian government has mooted legislation that would make encryption software illegal.
- Russia and China's own growing concerns over terrorism are prompting measures to expand control over their domestic technology networks.

All of these measures are a matter of concern for telecoms and technology vendors because of their stringent requirements and potential legal ramifications.

Complexity Makes Us All Less Secure

This landscape of increasing regulatory complexity is challenging for commercial enterprises to navigate. Ultimately, complexity makes us all less secure, and attackers can and will exploit division.

- The United States has been in a unique position because, up to this point, much of the data useful for governments has been stored on U.S. servers. This is no longer the case. Countries such as Germany, Russia, and China are taking steps toward data localization laws and regulatory platforms.
- The United States is also mulling over legislation that would reach further than even the United Kingdom's Investigatory Powers legislation. The legislation would require any company producing software or hardware—or maintaining an app store—to provide data in a form the government can read and to build in the capability to "reverse-engineer" technology in order to turn over intelligible data.

Absent a global set of initiatives, better communication and greater understanding between governments and the private sector on cybersecurity are badly needed. More effective systems for exchanging data requests are a good start toward this goal. Information sharing between governments and commercial enterprises is also crucial, although misunderstandings remain to be worked out.

For example, enterprises are arguing that forcing technology vendors to provide a "back door" to data may provide short-term security benefits but could ultimately destroy the trust of consumers. In turn, that would hurt the very companies that form the backbone of their economies.

For both the public and private sectors, data protection is a dilemma. Agreements like the EU-U.S. Privacy Shield are designed to facilitate the international flow of data so that analytics can take place and give consumers confidence that the data flow can happen without risks to them or the data. It remains to be seen if consumers will embrace such measures.

"Absent a global set of initiatives, better communication and greater understanding between governments and the private sector on cybersecurity are badly needed."

Security Recommendations

As the next generation of ransomware evolves, organizations need to employ a "first line of defense" that will impede the opportunity for lateral movement and propagation and reduce adversaries' time to operate. That first line—in addition to basic best practices such as patching vulnerable Internet infrastructure and systems (see **page 22** and **page 29**) and improving password management (**page 44**)—includes network segmentation.

Organizations can use network segmentation to stop or slow the lateral movement of self-propagating threats as well as contain them. There are multiple components for segmented networks that organizations should consider implementing such as:

- VLANs and subnets for logically separating access to data, including at the workstation level
- Dedicated firewall and gateway segmentation
- Host-based firewalls with configured ingress and egress filtering
- Application blacklisting and whitelisting
- Role-based network share permissions (least privilege)
- Proper credential management

THE LAST LINE OF DEFENSE: BACKUP RECOVERY

Backup recovery is the last line of defense for organizations that want to avoid—today, and in the future—paying a "king's ransom" to attackers who have encrypted their data with ransomware (**page 10**). However, the ability to recover from a ransomware attack with minimal data loss and service interruption will depend on whether system backups and disaster recovery sites have been compromised.

In a ransomware scenario in which local backups are deleted, removed, or otherwise made inaccessible by attackers, off-site backups are often an organization's only hope of restoring service without paying the ransom. How often backups are sent off-site determines how much data, if any, would be inaccessible or lost.

DON'T DISMISS THE THREAT OF BROWSER INFECTIONS

When ad injectors deliver malicious advertising through HTTPS encrypted traffic, defenders can't readily identify the threat (see **page 21**). And as adversaries increase their use of HTTPS to conceal their activity, it is becoming even more imperative for security teams to stop viewing browser infections as a low-severity threat to their organization and its users.

A seemingly benign browser infection can quickly become a much bigger problem, and there is evidence that malicious ad injectors have become an important tool for adversaries laying the groundwork for higher-risk attacks.

By making monitoring of browser infections a higher priority, organizations will be better positioned to quickly identify and remediate these threats. Behavioral analytics tools and collaborative threat intelligence are critical resources for defenders in remediating these types of threats. Educating users to alert security teams to an increase in pop-up ads and other unwanted advertising is also vital for defense.

INCORPORATE A ROUTINE PATCHING LIFECYCLE

Organizations of all sizes and in all industries need to move beyond "checking off the boxes" approaches that are no longer sufficient for modern threats. A "security first" posture requires an integrated threat defense—in addition to a financial commitment to security defenses.

For example, security professionals should periodically check for the presence of unexpected system or administrator accounts, using the tools available to them. They should also log and analyze all network communications for malicious traffic, and review such suspicious traffic for IOCs. On their part, leadership should provide the tools that are needed to conduct such in-depth investigations.

In addition, they should ensure that the environment is up to date by incorporating a routine patching lifecycle with the most recent patches delivered to operating systems and commonly used software, where threat actors tend to find and exploit weaknesses.

Indicators of Compromise Are Not Threat Intelligence

IOCs are the language of threat intelligence—the building blocks of threat activity. However, valuable as this data can be to defenders conducting investigations, IOCs are not threat intelligence.

Organizations can spend millions of dollars on lists of IOCs that are marketed as threat intelligence. It is then up to their security teams to take that data and figure out how to make it relevant to the business. This resource-intensive process can take security practitioners away from higher-priority activities. In some cases, reliance on IOCs can create false assumptions that the organization may be secure and free from attackers that are more relevant to a different organization's security posture.

So, what is threat intelligence? It is data that has been converted into actionable information through an understanding of the context in which that data was produced. Threat intelligence comes with the targeted "what to do next because of the story that the data tells." Data without that business-level application is just data—like sand on the beach.

To ensure they are investing in and benefiting from true threat intelligence, organizations should look for security vendors that combine IOCs, context with organizationally relevant impacts, and instructions. They take care to add a human component to the process and blend those insights into their security tools so that threat intelligence is automated for the security teams that rely on it.

It is important to differentiate between IOCs and threat intelligence. Threat intelligence helps defenders to understand the totality of an attack and to improve their detection and incident response.

"It is important to differentiate between IOCs and threat intelligence. Threat intelligence helps defenders to understand the totality of an attack and to improve their detection and incident response."

Conclusion

Today's attacks currently outpace defenders' ability to respond. As long as attackers are permitted unconstrained time to operate, and innovate, their success is all but ensured. But if an organization can limit adversaries' time and opportunity to lay the foundation for and carry out an attack, they are forced to make decisions under pressure that place them at higher risk of becoming known—and taken down.

Turning the tables on attackers by pushing them to continuously evolve their threats is one strategy for reducing their time to operate. The more they need to adapt, the more likely they are to leave a trail that will ultimately lead to their identification—no matter how many ways they try to evade detection and cover their tracks.

This is why it is imperative to measure TTD. If defenders do not know where they stand with their ability to detect threats, they cannot improve. TTD and TTP (time to patch) should be viewed and applied as key performance indicators; doing so will enable security teams to home in on the techniques that constrain attackers and force them to change strategies.

As has always been the case, organizations and end users play an important role in helping to reduce the time that threat actors have to operate. For enterprises, there has perhaps never been a better time—or more urgent need—to improve security practices.

Upgrading aging infrastructure and systems and patching known vulnerabilities will undermine the ability of cybercriminals to use those assets to carry out their campaigns. The adversaries responsible for the SamSam ransomware attacks have already alerted the shadow economy to a new frontier ripe with old vulnerabilities that can be exploited to compromise users and reach new heights of profitability. (See "Ransomware: A Massive Revenue Generator with Undeniable Staying Power," **page 7**.)

Many organizations have reached a tipping point with their Internet infrastructure. They want to simplify and update their devices and software to reduce costs and build a strong IT foundation that will help enable their success in the emerging next-generation digital economy. This is their moment to harden security, and enable visibility, throughout their network—and help to reduce the unconstrained time to operate that adversaries currently enjoy.

"Many organizations have reached a tipping point with their Internet infrastructure.... This is their moment to harden security, and enable visibility, throughout their network—and help to reduce the unconstrained time to operate that adversaries currently enjoy."

About Cisco

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

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

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

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

Contributors to the Cisco 2016 Midyear Cybersecurity Report

TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

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

SECURITY AND TRUST ORGANIZATION

Cisco's Security and Trust Organization underscores Cisco's commitment to address two of the most critical issues that are top of mind for boardrooms and world leaders alike. The organization's core missions include protecting Cisco's public and private customers, enabling and ensuring Cisco Secure Development Lifecycle and Trustworthy Systems efforts across Cisco's product and service portfolio, and protecting the Cisco enterprise from ever-evolving cyber 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 **http://trust.cisco.com**.

GLOBAL GOVERNMENT AFFAIRS

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

COGNITIVE THREAT ANALYTICS

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

INTELLISHIELD TEAM

The IntelliShield team performs vulnerability and threat research, analysis, integration, and correlation of data and information from across Cisco Security Research & Operations and external sources to produce the IntelliShield Security Intelligence Service, which supports multiple Cisco products and services.

LANCOPE

Lancope, a Cisco company, is a leading provider of network visibility and security intelligence to protect enterprises against today's top threats. By analyzing NetFlow, IPFIX, and other types of network telemetry, Lancope's StealthWatch® System delivers Context-Aware Security Analytics to quickly detect a wide range of attacks from APTs and DDoS to zero-day malware and insider threats. Combining continuous lateral monitoring across enterprise networks with user, device, and application awareness, Lancope accelerates incident response, improves forensic investigations, and reduces enterprise risk.

ACTIVE THREAT ANALYTICS TEAM

The Cisco Active Threat Analytics (ATA) team helps organizations defend against known intrusions, zero-day attacks, and advanced persistent threats by taking advantage of advanced big data technologies. This fully managed service is delivered by our security experts and our global network of security operations centers. It provides constant vigilance and on-demand analysis 24 hours a day, seven days a week.

SECURITY RESEARCH AND OPERATIONS (SR&O)

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

ADVANCED SECURITY RESEARCH AND GOVERNMENT (ASRG)

Advanced Security Research and Government (ASRG) provides direction and guidance for Cisco's long-term security vision. To accomplish this goal, ASRG performs internal research in key security areas such as advanced cryptography and security analytics. ASRG also partners with and funds university researchers to help solve long-term problems.

CISCO SECURITY INCIDENT RESPONSE SERVICES (CSIRS)

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

Download the Graphics

All the graphics in this report are downloadable at: **www.cisco.com/go/mcr2016graphics**

Updates and Corrections

To see updates and corrections to the information in this report, visit: **www.cisco.com/go/mcr2016errata**

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Published July 2016

© 2016 Cisco and/or its affiliates. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Adobe, Acrobat, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.