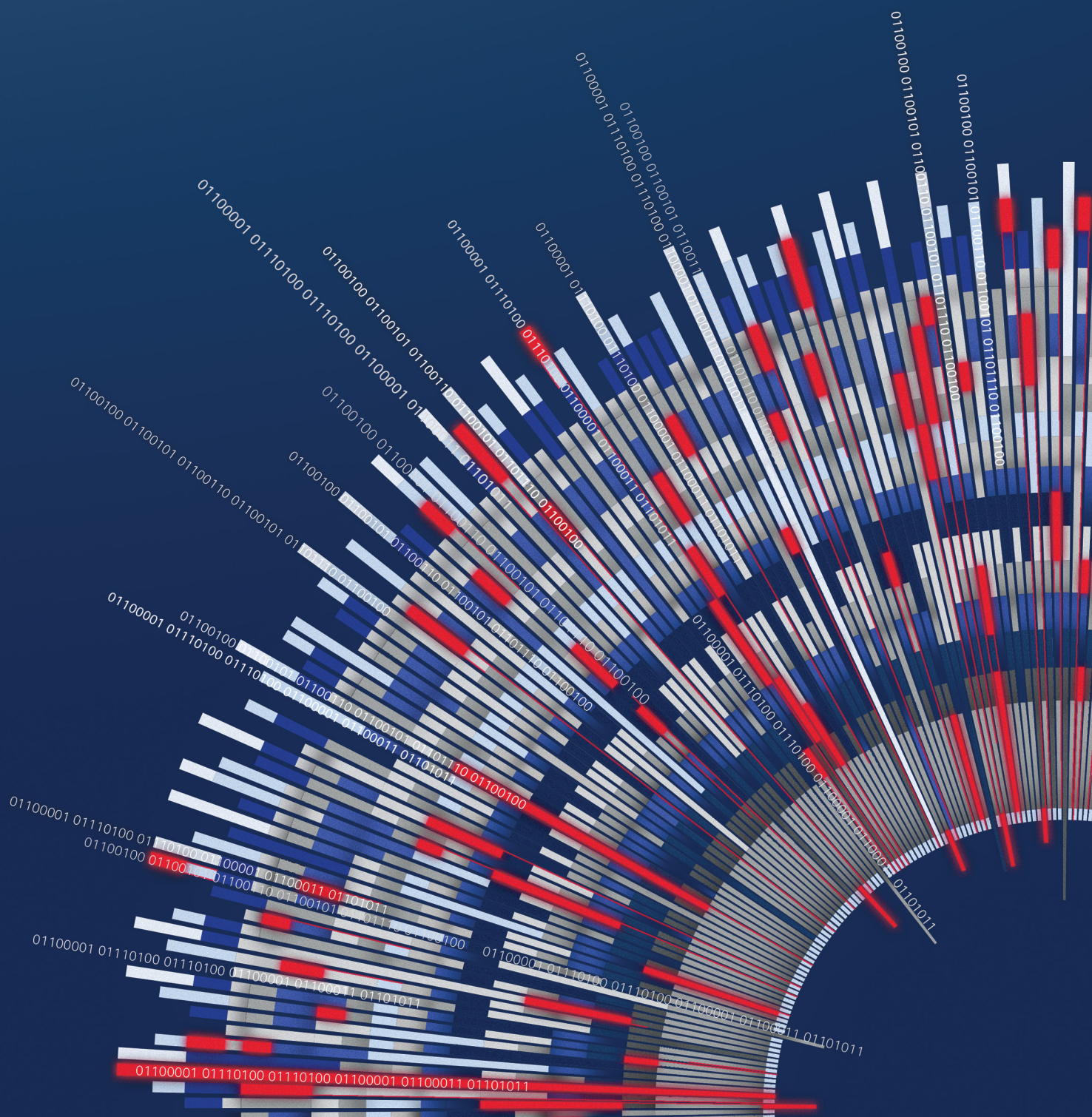
Cisco 2015
Midyear Security Report



Executive Summary

As adversaries rapidly refine their ability to develop and deploy malware that can breach network defenses and evade detection, the security industry, as a whole, struggles to innovate at a similar pace.

This dynamic creates a significant problem for organizations investing in security products and services: They often end up choosing individual solutions to address security gaps, only to create more weak points in their threat defenses.

The Cisco 2015 Midyear Security Report examines these intersecting challenges while also providing updates on some of the most compelling threats. Using research by our experts, it provides an overview of the major threats observed in the first half of 2015. This report also explores likely future trends and offers advice for small, midsize, and enterprise organizations that seek security solutions and services.

The report is divided into two main areas:

Threat Intelligence

This section gives an overview of the latest threat research from Cisco. We discuss:

- Updates on exploit kits such as Angler
- Criminals' increasing use of macros involving Microsoft Office
- New tactics from malware authors to evade detection
- Risk of malware encounters for specific industry verticals
- Time to detection of threats
- Updates on spam, threat alerts, Java exploits, and malvertising

Analysis and Observations

In this section we cover security industry consolidation and the emerging concept of integrated threat defense. Other topics in focus include the importance of building trust and security into products and the value of engaging security services organizations in a market where skilled security talent is scarce. Lastly, we discuss how a cohesive cybergovernance framework can be a step toward sustaining business innovation and economic growth on the global stage.

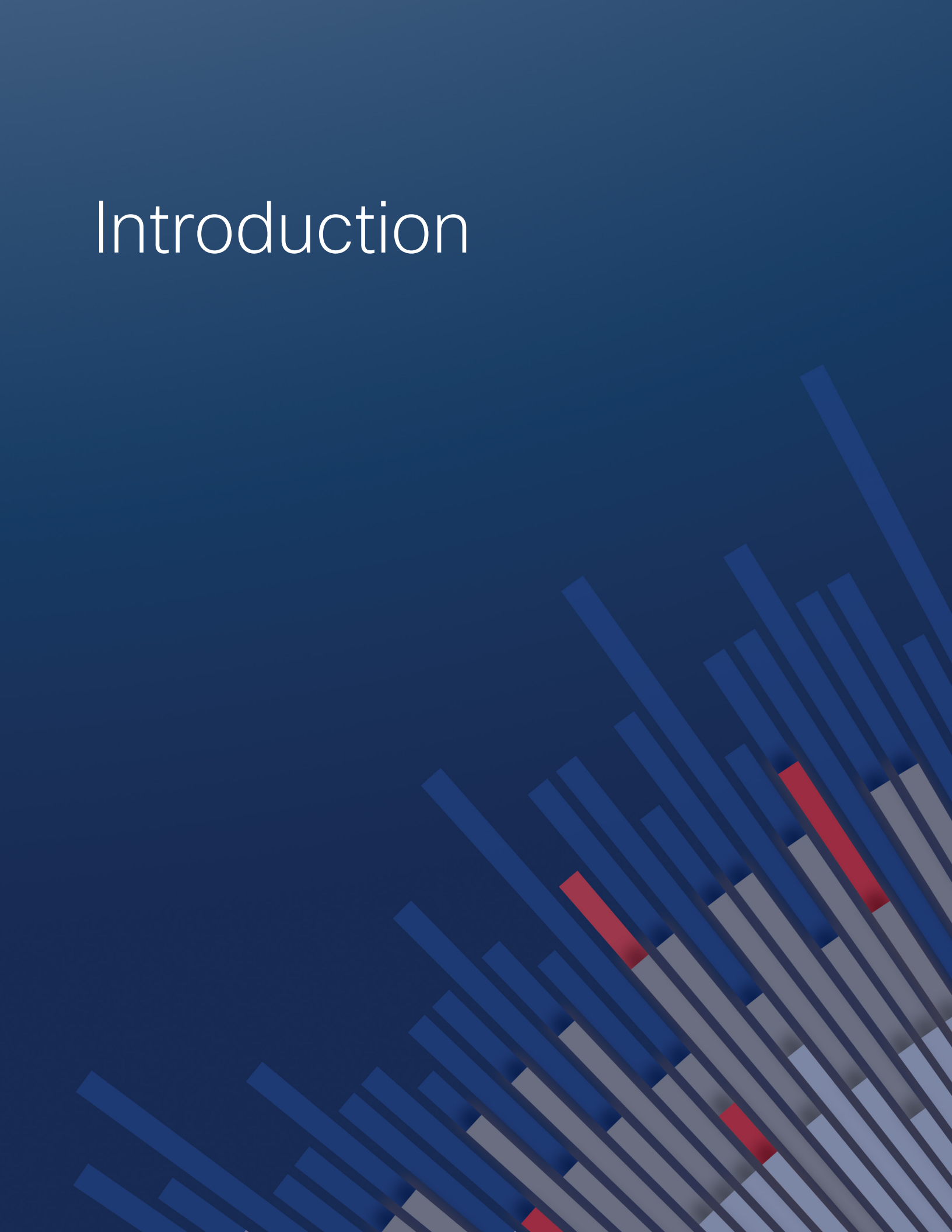
Major Discoveries

Adversaries continue to innovate as they slip into networks undetected and evade security measures.

- Exploits of Adobe Flash vulnerabilities are increasing. They are regularly integrated into widely used exploit kits such as Angler and Nuclear.
- Angler continues to lead the exploit kit market in terms of overall sophistication and effectiveness.
- Operators of crimeware, like ransomware, are hiring and funding professional development teams to help them make sure their tactics remain profitable.
- Criminals are turning to the anonymous web network Tor and the Invisible Internet Project (I2P) to relay command-and-control communications while evading detection.
- Adversaries are once again using Microsoft Office macros to deliver malware. It's an old tactic that fell out of favor, but it's being taken up again as malicious actors seek new ways to thwart security protections.
- Some exploit kit authors are incorporating text from Jane Austen's classic novel *Sense and Sensibility* into web landing pages that host their exploit kits. Antivirus and other security solutions are more likely to categorize these pages as legitimate after "reading" such text.
- Malware authors are increasing their use of techniques such as sandbox detection to conceal their presence on networks.
- Spam volume is increasing in the United States, China, and the Russian Federation, but remained relatively stable in other regions in the first five months of 2015.
- The security industry is paying more attention to mitigating vulnerabilities in open-source solutions.
- Continuing a trend covered in the Cisco 2015 Annual Security Report, exploits involving Java have been on the decline in the first half of 2015.

Contents

Introduction



Introduction

The tactics developed by malware authors and online criminals have shown increasing sophistication over the past several years. Recent Cisco security reports have chronicled such innovation in the shadow economy, along with security professionals' fight to stay ahead of adversaries.

What's new is the threat actors' growing ability to innovate rapidly and enhance their capacity to compromise systems and evade detection. In the first half of 2015, the hallmark of online attackers may be their willingness to evolve new tools and strategies—or recycle old ones—to dodge security defenses. Through tactics such as obfuscation, they can not only slip past network defenses but also carry out their exploits long before they are detected—if ever.

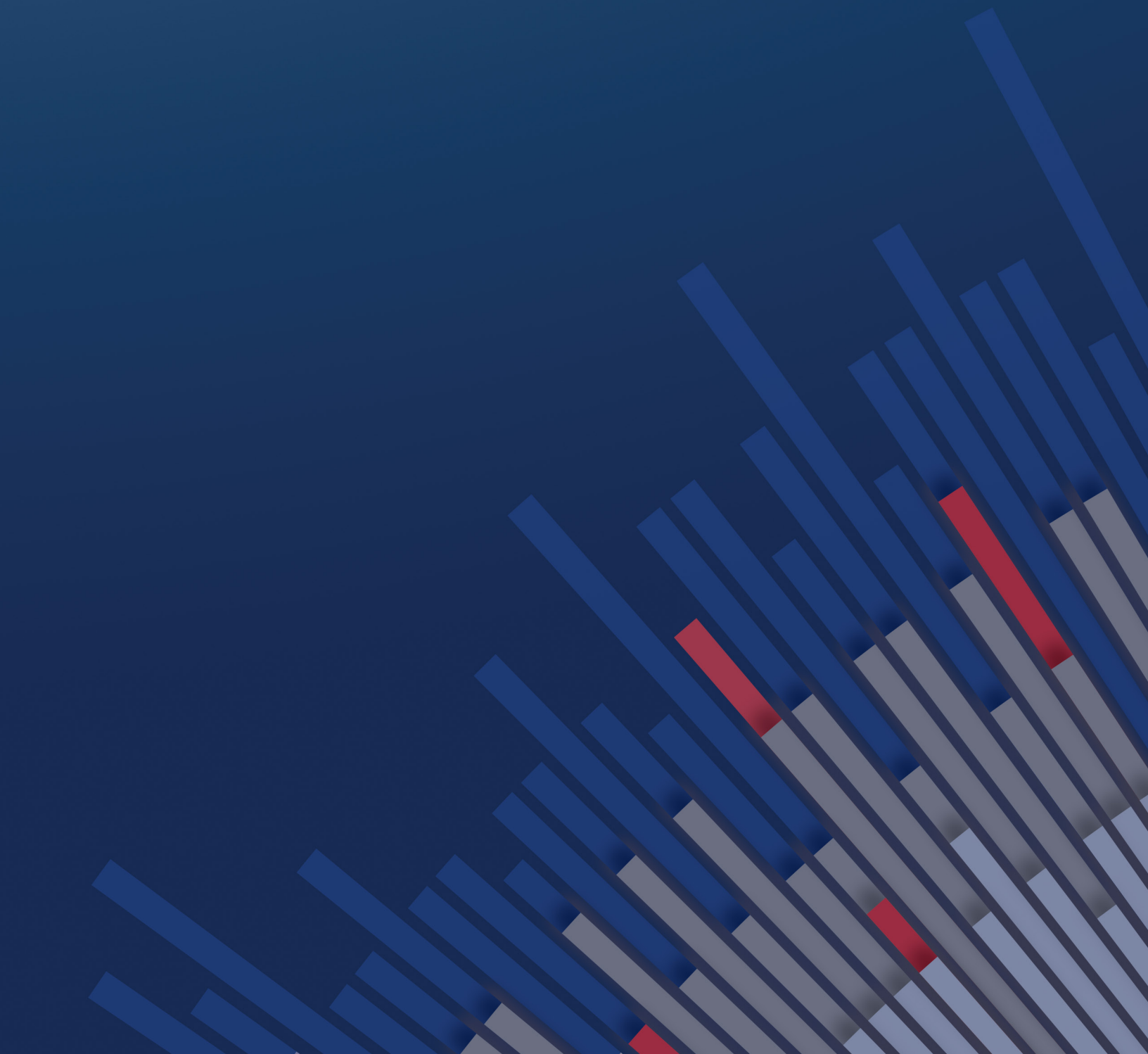
Security vendors are responding with their own innovations. For example, researchers are adding support for the analysis of new file formats such as .cab and .chm as new attacks are detected using those formats. In addition, vendors are developing new detection engines and constantly evaluating and evolving heuristics.

Security vendors know they need to stay agile. If they or their networks let down their guard even briefly, attackers will get the upper hand. But the pace of innovation in the industry is not as rapid as it needs to be.

Many vendors are offering piecemeal or individual solutions to security problems. And buyers—that is, the organizations that purchase security tools from vendors—are eagerly looking for stopgap products, not in-depth strategic solutions. But because they are not integrating technologies and processes across the entire security footprint, their management of security tools becomes unwieldy.

Security industry consolidation and a close integration of leading technologies can help, in time, to move organizations away from taking a product-by-product approach to implementing their defenses (see page 33). Meanwhile, a proactive and in-depth defense strategy, of which technology is just one component, can help small, midsize, and enterprise organizations and their security teams meet the threat of criminal innovation described in this report.

Threat Intelligence



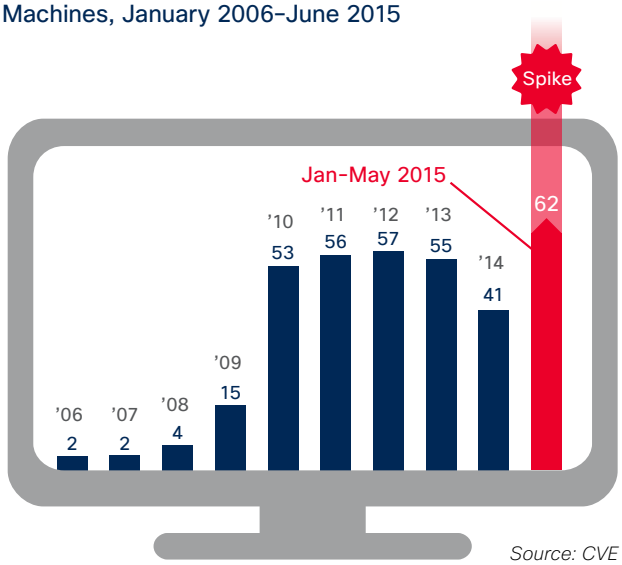
Threat Intelligence

Cisco has assembled and analyzed a global set of telemetry data for this report. Our ongoing research and analysis of discovered threats, such as malware traffic, can provide insights on possible future criminal behavior and aid in the detection of threats.

Flash Exploits Fire Up in First Half of 2015

For the first five months of 2015, the Common Vulnerabilities and Exposures (CVE) project published 62 vulnerabilities for Adobe Flash Player that resulted in code execution on users' machines. As Figure 1 shows, only 41 of these types of vulnerabilities were identified in 2014. The second most significant spike occurred in 2012, when 57 of these Flash vulnerabilities were observed. If the current pattern of activity is sustained through the remainder of the year, 2015 could see more than 100 of these exploits, which would be an all-time record.

Figure 1. Number of Vulnerabilities in Flash That Resulted in Code Execution on Users' Machines, January 2006–June 2015



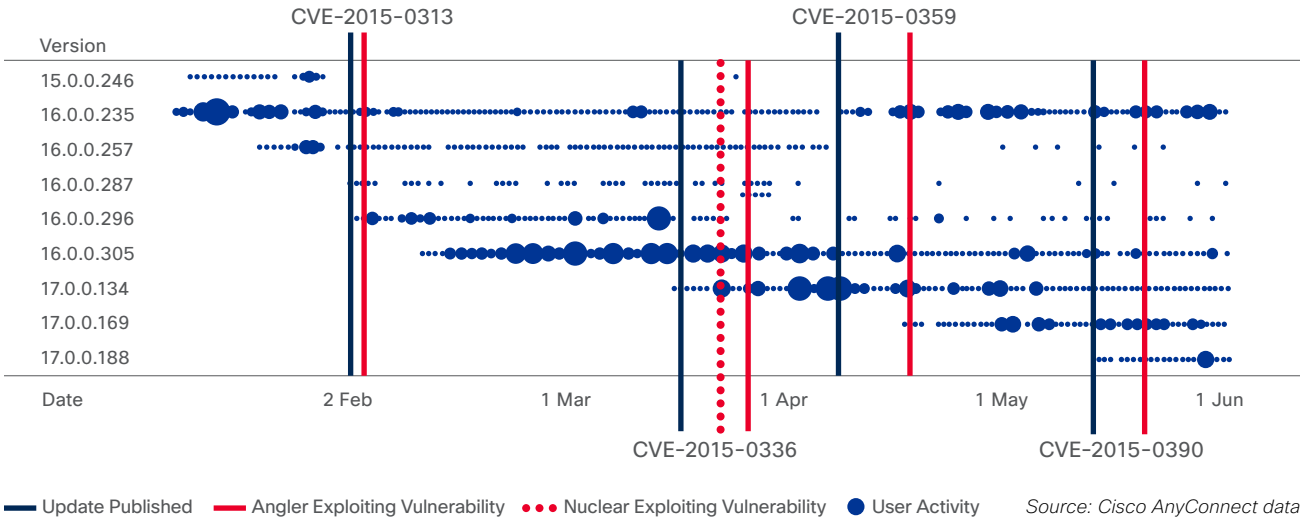
Source: CVE

We attribute the recent growth in exploits of Flash vulnerabilities to two primary factors:

- **Flash exploits are being integrated regularly into the latest versions of widely used exploit kits such as Angler (see page 9).**
- **Although Adobe frequently updates its Flash Player, many users are simply not quick enough to apply updates that would protect them from exploits targeting the vulnerability being patched.**

It appears many users have difficulty staying on top of Adobe Flash updates and perhaps may not even be aware of some upgrades. Figure 2 shows that Angler's authors are benefiting from this "patching gap"—the time between Adobe's release of an update and when users actually upgrade. (Cisco's technology allows researchers to monitor software versions of users at any point in time.)

Figure 2. Requests Made Per Version of Flash, by Date



For example, the February 2015 time frame depicted in Figure 2 shows that many users moved quickly to the latest version of Flash (16.0.0.305). That update, released February 2, 2015, addressed vulnerabilities in CVE-2015-0313. However, as users migrated to the new version of Flash, Angler actively exploited the known vulnerability in the previous version.

Figure 2 also shows that the authors of the Angler exploit kit were able to quickly develop and release a working exploit to target the vulnerability in CVE-2015-0313. We noted similar rapid innovation with other Flash exploits during the first half of 2015. For example, another sophisticated and constantly active exploit kit, Nuclear, was quick to target the vulnerability in CVE-2015-0336. Angler began exploiting the same vulnerability shortly thereafter.

The patching gap is one reason adversaries continue to find success exploiting users of Java (see Figure 3).

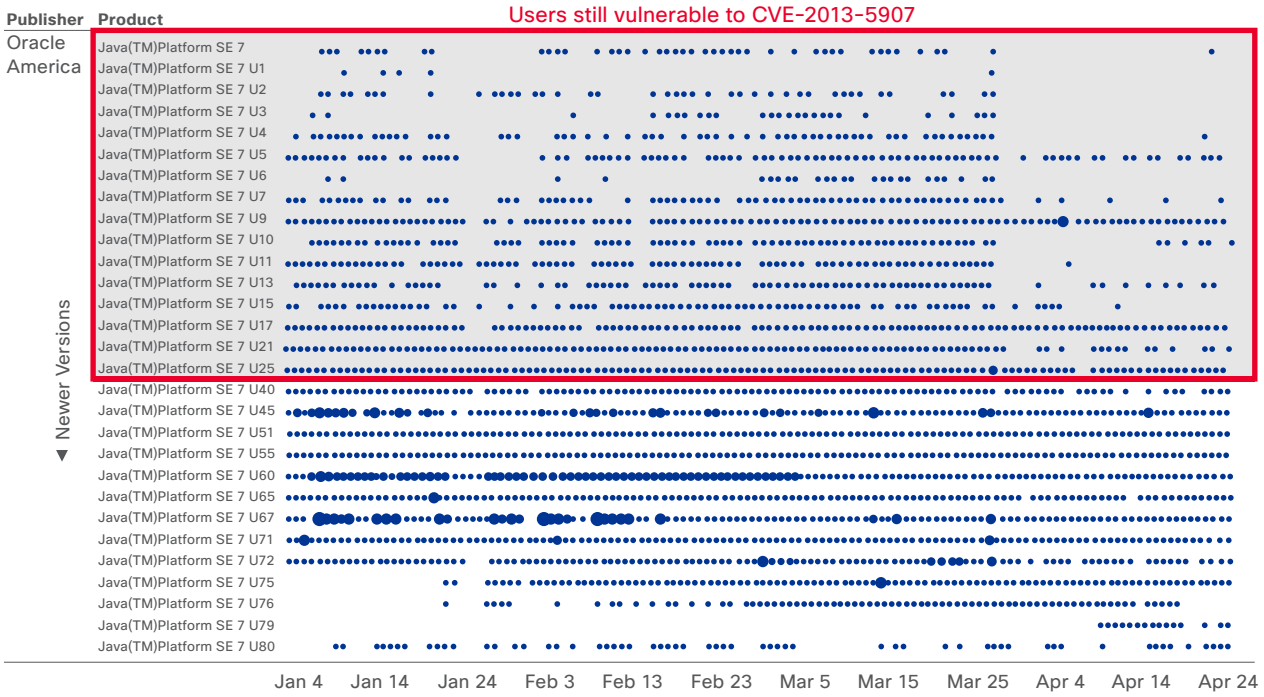
Attacks designed to target Flash and other new vulnerabilities are being integrated so quickly into exploit kits like Angler and Nuclear that it is increasingly harder for security teams to keep pace. The time to detection is also longer because retrospective analysis is often needed to identify these threats.

The risk of compromise for individual users and organizations relying strictly on a single detection engine is significant. And in environments without retrospective analysis capabilities, threats delivered through zero-day attacks or evasive means could remain undetected for long periods, or even never identified.

However, one fundamental measure—the prompt and routine patching of software—can help to significantly reduce the risk of compromise by threats that are designed to exploit known vulnerabilities in Flash and Java.

Figure 3. Number of Requests Made Per Version of Java, by Date

Share the report



Source: Cisco Cloud Web Security data

Focus on Flash Gives Angler a Significant Edge over Competitors

Share the report

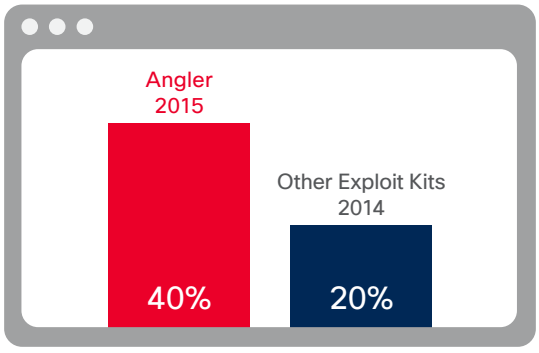
Earlier this year,[1] Cisco singled out the Angler exploit kit as the one to watch among known exploit kits observed in the wild because of its innovative use of Flash, Java, Microsoft Internet Explorer, and Silverlight vulnerabilities. So far in 2015, Angler stands as the leader in exploit kit sophistication and effectiveness.

The exploit kit's authors' recent concentration on, and quick work to take advantage of, vulnerabilities in Adobe Flash is an example of their commitment to innovation.

Cisco reports that, on average, 40 percent of users who encounter an Angler exploit kit landing page on the web are compromised. (See Figure 4.) This means Angler can identify a known Flash (or other) vulnerability that it can exploit. It then downloads the payload to the user's machine.

By comparison, in 2014, other widely used kits that featured a mix of exploits had an average success rate of just 20 percent, according to our research.

Figure 4. Rate of Visitors Exploited, December 2014–May 2015



Source: Cisco Security Research

1 Cisco 2015 Annual Security Report, Cisco, January 2015: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

Angler: Running in the Shadows

Angler's success in compromising users online can be attributed partly to its simple but well-constructed web landing pages. Cisco researchers suggest that the exploit kit's authors may be relying on data science to create computer-generated landing pages that resemble normal webpages and easily dupe users. Malvertising (malicious online advertising) is likely the key driver for a consistent stream of web traffic to these pages. (For more on malvertising, see page 29.)

Angler also excels at attempting to evade detection. "Domain shadowing" is one technique its authors have recently employed. Exploit kit authors compromise a domain name registrant's account, and then register a subdomain under the legitimate domain of the compromised user. Unless users review their account information, they will not know these subdomains exist. The subdomains point at malicious servers. They are very high volume, short-lived, and random, so they're difficult to block.

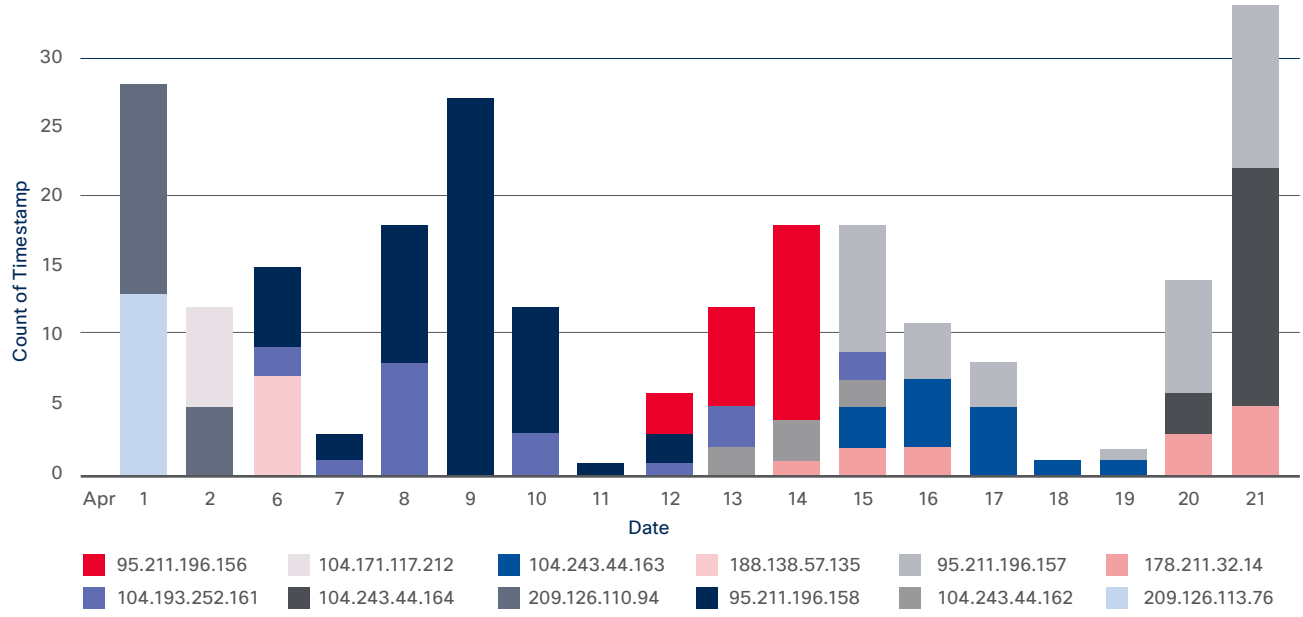
Domain shadowing is not new, but the use of this technique has been increasing since December 2014. According to our research, more than 75 percent of known subdomain activity by exploit kit authors since that time can be attributed to Angler. The exploit kit serves a range of malicious payloads, including the ransomware Trojan Cryptowall, through file exploits.

In addition to domain shadowing, the Angler exploit kit uses multiple IP addresses to make detection more difficult. The sample in Figure 5 shows how frequently Angler can switch IPs on a given day. The pattern appears random.

The Cisco Talos Security Intelligence and Research Group (Talos) blog post **"Threat Spotlight: Angler Lurking in the Domain Shadows"** discusses how Angler creates subdomains that can serve malicious content, and why a defense-in-depth approach to security is essential to detecting this type of attack.

Also, see the Talos Group blog post **"Domain Shadowing Goes Nuclear: A Story in Failed Sophistication,"** which examines a Nuclear campaign that includes domain shadowing. This work in progress will likely be a successful exploit kit platform once completed.

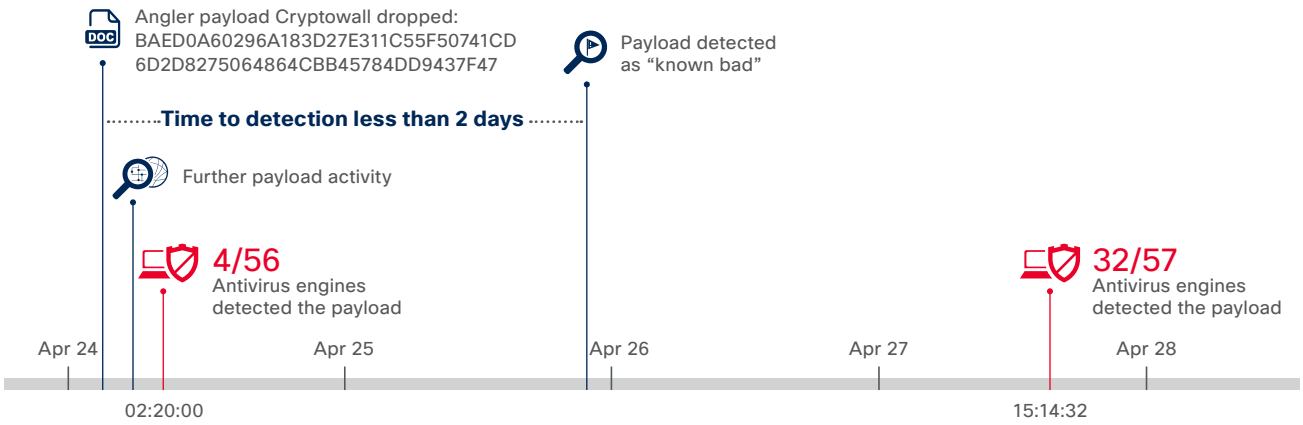
Figure 5. Successful Flash Exploits, April 2015



*Colors represent IP ranges.

Source: Cisco Security Research

Figure 6. Time to Detection for Angler Payload Dropped on April 24, 2015



Source: Cisco Security Research

Encrypted Payloads Slow Time to Detection for Angler

Angler usually delivers an encrypted payload, which is often the ransomware Trojan Cryptowall. If not initially blocked, this payload can be identified only retrospectively, and time to detection of the threat can take days.

Once a payload is detected, the exploit kit's authors, living up to their reputation for innovation, will quickly create a technique for delivering threats such as Cryptowall and evading antivirus solutions.

Figure 6 shows the time to detection for the Angler payload Cryptowall that was first dropped on April 24, 2015: BAED0A60296A183D27E311C55F50741CD6D-2D8275064864CBB45784DD9437F47.

On the first day, only 4 of 56 antivirus engines deployed by VirusTotal had identified the new instance of malware. However, by April 27, 32 of 57 antivirus engines were detecting the threat.

- 2015-04-24 02:20:00 **4/56** (4 of 56 antivirus engines deployed detected the payload)
- 2015-04-27 15:14:32 **32/57** (32 of 57 antivirus engines deployed detected the payload)

Cisco identified the threat as "unknown" on April 24, and then analyzed and retrospectively convicted the threat (categorizing it as "known bad") less than two days later.

See "Time to Detection: Defined," on page 30, for more information on how we define and calculate time to detection.

Exploit Kit Authors Go High-Brow to Keep Landing Pages on the Down-Low

Some exploit kit authors are looking to early 19th-century literature to help conceal their 21st-century threats. Specifically, some adversaries are incorporating text from Jane Austen's *Sense and Sensibility* into web landing pages that host their exploit kits.

Adding passages of classic text to an exploit kit landing page is a more effective obfuscation technique than the traditional approach of using random text. The use of text from more contemporary works such as magazines and blogs is another effective strategy. Antivirus and other security solutions are more likely to categorize the webpage as legitimate after "reading" such text.

For users, encountering unexpected references to beloved Austen characters such as Elinor Dashwood and Mrs. Jennings on a webpage may be perplexing but not a cause for immediate concern. But their lack of unease gives adversaries more opportunity to launch their exploits.

The use of known works instead of random text is just one example of how threat actors are evolving their schemes to avoid detection.

Figure 7. Sample of *Sense and Sensibility* Text Used on Exploit Kit Landing Page

```
https://rt1.mtd.cisco-services.com/Ticket/
Display.html?
id=137668&results=ad470ba70bfbd94464c2a0e9deff943b

Sense and sensibility - jane austin
    <small>
     Mr. Ferrars comfortable as a continual flow of
tears would permit her. In the society of both. Why
they should both attend through
    </small>
     She looked down as a difference of the three, by
their presence; and it will be so easily settled. it
    <i>
     the cruel situation in which she had by that
which only could convince her, a better match for
your mother--will you allow him to give rise to
conjectures, which might make it rare; for his
sisters by the hand, and speaking in an audible
voice, and walking the
    </i>
```

Source: Cisco Security Research

The Evolution of Ransomware: A Story of Innovation—and Lowering the Bar

Share the report

In today's flourishing malware economy, cryptocurrencies like bitcoin and anonymization networks such as Tor (see page 15) are making it even easier for miscreants to enter the malware market and quickly begin generating revenue. To become even more profitable while continuing to avoid detection, operators of crimeware, like ransomware, are hiring and funding their own professional development teams to create new variants and tactics.

Ransomware encrypts users' files—targeting everything from financial files to family photos—and provides the keys for decryption only after users pay a "ransom." Ransomware targets everyone from large companies to schools to individual users.

The malware is typically delivered through a number of vectors including email and exploit kits. The exploit kit Angler (see page 11), for example, is known to drop the Cryptowall payload. Cryptowall emerged after the original variant, Cryptolocker, was taken down by law enforcement in mid-2014.

Figure 8 depicts a sample message that users might receive when they encounter TeslaCrypt ransomware; TeslaCrypt pretends to be a derivative of Cryptolocker.

Figure 8. Example of On-Screen Message from TeslaCrypt Ransomware

Source: Cisco Security Research

The ransom demanded is not exorbitant. Usually, a payment between $300 and $500 is required. Why such a modest fee? Adversaries who deploy ransomware have done their market research to determine the ideal price point. The idea is that the ransom is not set so high that a user won't pay it or, worse, that it will motivate the user to contact law enforcement. Instead, the ransom is more of a nuisance fee. And users are paying up.

In fact, Cisco reports that nearly all ransomware-related transactions are carried out through the anonymous web network Tor (see page 15). Adversaries keep the risk of detection low, and profitability high, by using channels like Tor and the Invisible Internet Project (I2P). I2P is a computer network layer that allows applications to send messages to each other pseudonymously and securely. Many ransomware operations also have development teams that monitor updates from antivirus providers so that the authors know when a variant has been detected and it's time to change techniques.

Adversaries rely on the cryptocurrency bitcoin for payments, so transactions are more difficult for law enforcement to trace. And to maintain a good reputation in the marketplace—that is, being known to fulfill their promise to give users access to their encrypted files after the payment has been processed—many ransomware operators have established elaborate customer support operations.

We have recently observed a number of customized campaigns that were designed to compromise specific groups of users, such as online gamers. Some ransomware authors have also created variants in uncommon languages like Icelandic to make sure that users in areas where those languages are predominantly spoken do not ignore the ransomware message.

Users can protect themselves from ransomware by backing up their most valuable files and keeping them isolated, or "air gapped" from the network. Users should also realize that their system could be at risk even after they pay a ransom and decrypt their files. Almost all ransomware is multivector. The malware may have been dropped by another piece of malware, which means the initial infection vector must still be resolved before the system can be considered clean.

For more on ransomware trends, see the Talos Group blog posts **"Cryptowall 3.0: Back to Basics"** and **"Threat Spotlight: TeslaCrypt–Decrypt It Yourself."**

Tor Adopted by Cybercriminals to Hide Network Communication

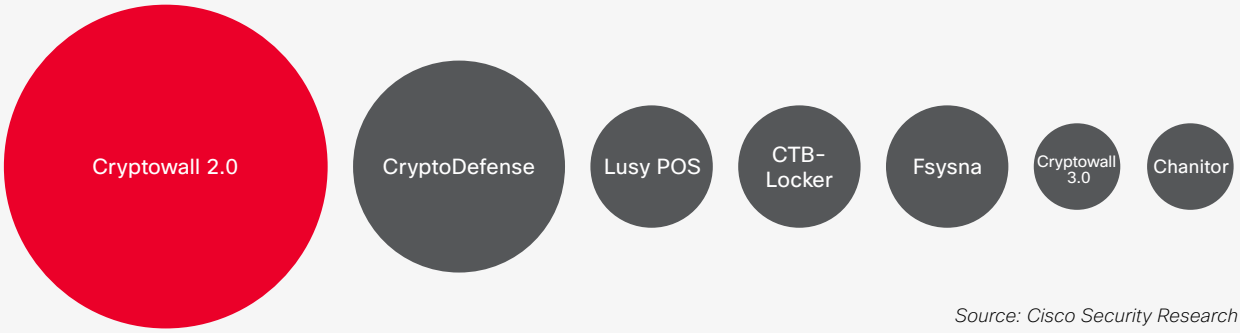
Malware authors naturally attempt to evade detection and keep their server locations unknown. To do this, many use the anonymous web network Tor to relay command-and-control communications.

Our researchers have detected several instances where malware families—especially ransomware variants—were generating Tor traffic. Although Tor is often used within enterprises for legitimate purposes (for example, by security professionals), its presence can indicate that there is malware traffic on a network. Some of the qualities that attract legitimate users to Tor are also attractive to wrongdoers.

If security professionals detect Tor activity in their networks, they should correlate this finding with other possible indicators of malicious activity—such as downloads of unknown executable files or connections to exploit kit servers—to determine whether the Tor traffic is legitimate.

As Figure 9 shows, adversaries deploying the ransomware Cryptowall 2.0, as well as several malware families, are users of Tor. (See "The Evolution of Ransomware: A Story of Innovation—and Lowering the Bar," page 13). The data comes from Cisco's monitoring of customer networks and shows incidents where Tor was used within malware families between October 2014 and May 2015.

Figure 9. Malware Families Using Tor for Communications



Source: Cisco Security Research

Microsoft Office Macros Make a Comeback as Vehicle for Launching Exploits

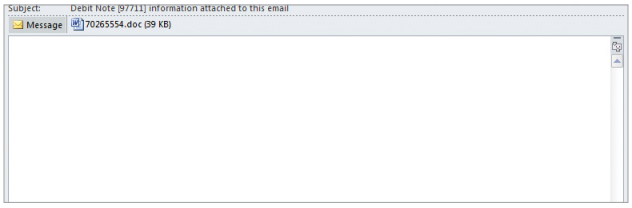
The upswing in the use of Microsoft Office macros to deliver banking Trojans shows the convergence of two trends in the world of online criminals: resurrecting old tools or threat vectors for reuse, and changing the threat so quickly and frequently that they can relaunch attacks over and over again and evade detection.

The old tools used by the perpetrators of these Trojans are macros in Microsoft Office products such as Microsoft Word. Popular with adversaries years ago, these macros had fallen out of favor because they were eventually turned off by default. However, using social engineering techniques, bad actors can persuade users to turn on macros, thereby adding a new tactic to their toolboxes.

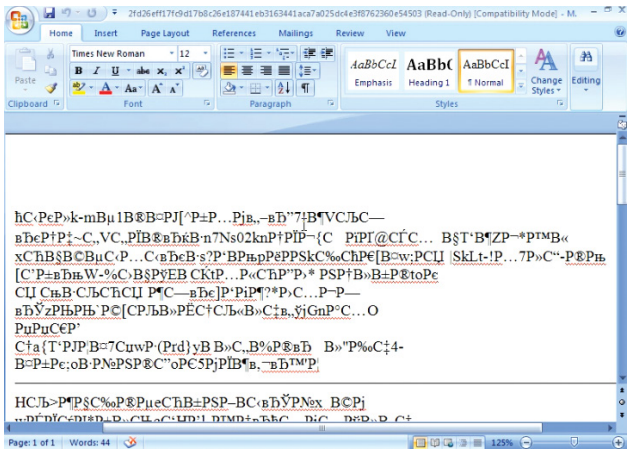
We studied two recent campaigns in which Dridex Trojans were delivered as attachments to emails—each sent to specific recipients—that purported to deliver invoices or other important documents. As of mid-2015, we are detecting new Dridex-related campaigns on a daily basis.

While the email subject lines in the first campaign (Campaign 1) attempted to fool recipients into thinking the attachments were crucial business documents, some of the emails themselves were blank.

Dridex: Campaign 1

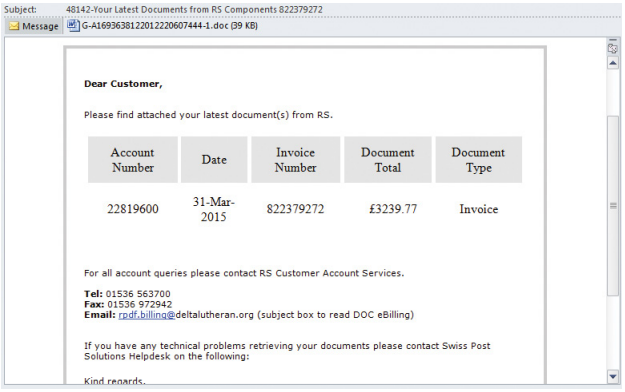


When the recipients opened the attachments, they saw a Word document filled with nonsense text.



Emails in the second campaign we analyzed (Campaign 2) included a message that appeared to be legitimate, referencing specific accounts and invoice numbers and claiming that the attached documents were invoices. But when recipients opened the Word attachment, they also saw nonsensical text, similar to what users in Campaign 1 encountered.

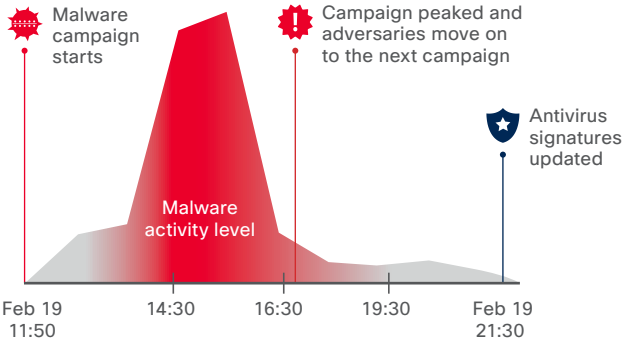
Dridex: Campaign 2



In both campaigns, as soon as an email recipient opened the attached Word document, malicious activity occurred: Behind the scenes, a macro used cmd.exe and PowerShell to download a malicious executable from a hardcoded IP address. In some campaigns that we observed, instructions were included to tell the user how to enable macros. Once the macros were enabled, Dridex could then attempt to steal logins and passwords to the victims' bank accounts.

Our researchers noticed that the spam campaigns carrying the Dridex payload tended to be very short-lived—perhaps just a few hours long—and that they also mutated frequently, as an evasion tactic. While antivirus solutions perform useful security functions, they are not well suited to detecting these short-lived spam campaigns. By the time a campaign is detected, attackers have already changed the emails' content, user agents, attachments, and refers. They then launch the campaign again, forcing antivirus systems to detect them anew. As seen in Figure 10 showing a DyrezaC malware campaign, antivirus updates can occur after a campaign has completed.

Figure 10. DyrezaC Can Work Faster than Antivirus Systems



Source: Cisco Security Research

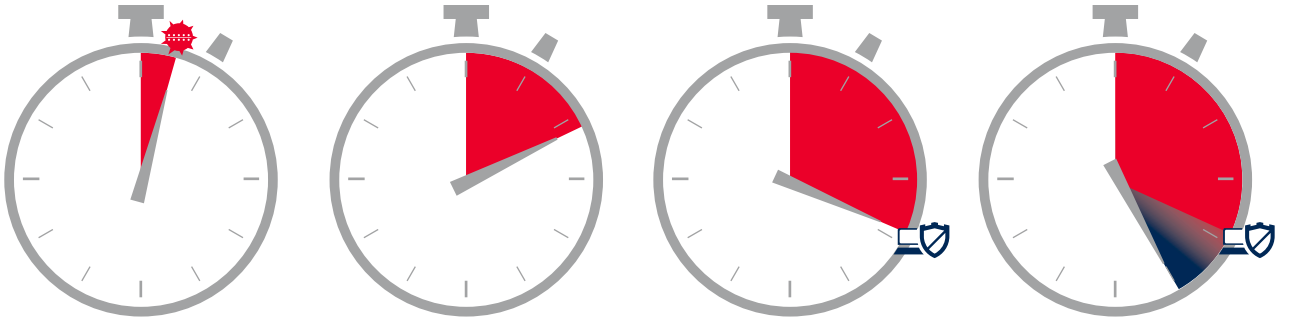
This approach—combining spam, Microsoft Office macros, and Dridex—appeared to be catching on with cybercriminals during the first half of 2015. We examined 850 unique samples of the emails and attached Microsoft Office files carrying this Trojan, a relatively large number of unique examples for a spam campaign. The creators of these quickly mutating campaigns appear to have a sophisticated understanding of evading security measures. They are aware of the reliance on antivirus detection for these threats, and they work to make sure they avoid detection.

In the example in Figure 11, the image shows that several hours passed before antivirus engines started to detect the Dridex threat. Because the campaign lasted for about five hours, antivirus solutions provided protection only for the tail end of the campaign.

Since they may view macro exploits as a thing of the past, security professionals may not be prepared to defend their networks against these threats. The best defense against them is a defense-in-depth strategy in which several security solutions work in tandem with antivirus. Virus outbreak filters, for instance, can quarantine suspect messages for up to 12 hours, allowing antivirus tools to catch up to the new threats.

For more information on the Dridex Trojan and Microsoft Office macros, read the Talos Group blog post **"Threat Spotlight: Spam Served With a Side of Dridex."**

Figure 11. Detection Graph for Dridex, March–April 2015



Source: Cisco Security Research

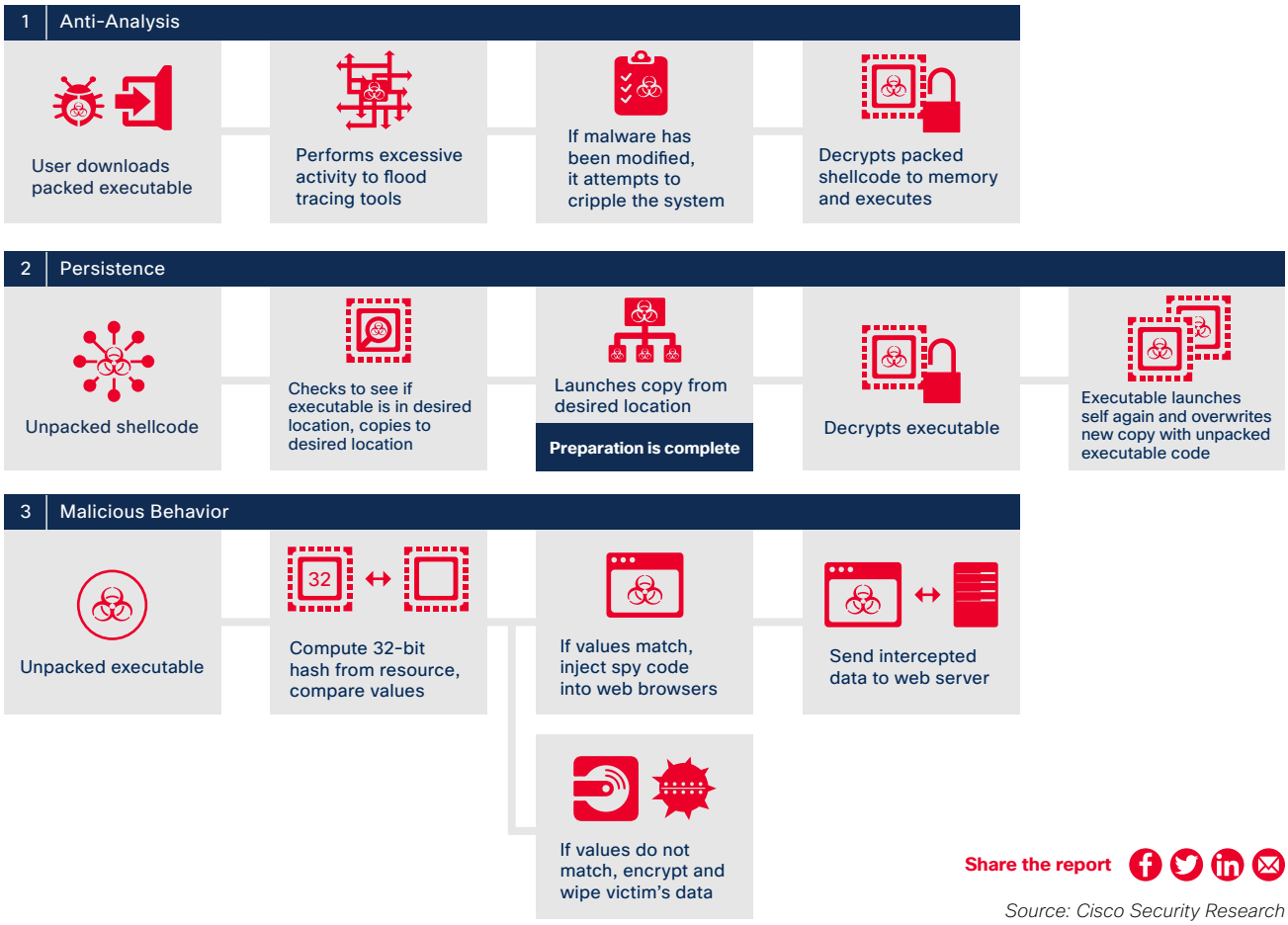
Rombertik: Malware That Not Only Can Steal Data But Also Destroy It

The authors of sophisticated malware design it to simply stop working in order to avoid being blocked or destroyed when it's examined by security systems. At the same time, security researchers are constantly on the lookout for new static, dynamic, and automated analysis tools that will make it more difficult for attackers to remain undetected.

Toward this goal, Cisco recently reverse-engineered Rombertik, a complex piece of malware that appears to detect attempts to tamper with its binary, similar to what occurs in reverse engineering. Rombertik tries to destroy the master boot record (MBR) of its host computer; if that isn't possible, it attempts to destroy the files in the user's home directory. Unlike malware that tries to divert attention from its activities, Rombertik seems to be designed to stand out from the crowd. Reverse-engineering is a crucial step used by Cisco and other threat researchers to understand how malware operates—including its evasive functionality.

The goal of Rombertik is to hook into a user's web browser to extract and deliver sensitive user information to a server controlled by attackers. In this way, Rombertik is similar to the malware known as Dyre.[2] However, Dyre exists to steal banking logins, while Rombertik appears to indiscriminately collect all kinds of user data.

Figure 12. Rombertik's Unique Combination of Anti-Analysis and Malicious Behavior



Share the report

Source: Cisco Security Research

Rombertik gains a foothold in users' systems through spam and phishing messages that use social engineering to entice recipients to download and unzip attachments carrying the malware. When a user unzips the file, it appears to be a PDF; in fact, it's a screensaver executable file that begins to compromise the system. As seen in Figure 12, if Rombertik detects that it is being modified, it attempts to destroy the system's MBR and then restart the computer, which will then be inoperable.

Advanced Anti-Analysis Tools in Today's Malware

Rombertik may be a harbinger of what's to come in the malware world, because malware authors are quick to adopt their colleagues' successful tactics. As our researchers discovered, Rombertik cleverly includes several features aimed at obfuscation and destruction. For instance, Rombertik includes excessive or "garbage" code to force security analysts to spend more time reviewing and analyzing the malware—overwhelming them so they don't have time to examine every function.

To evade detection and force a sandbox to time out before the malicious payload has a chance to execute, Rombertik takes a unique approach. Typically, malware "sleeps" if it's in a sandbox to force the timeout. But when security analysis tools became more effective at detecting the "sleeping" process, malware authors needed a new strategy.

In the case of Rombertik, the malware writes a byte of random data to memory 960 million times. This can affect both application-tracing tools and sandboxes. Sandboxes may not be able to determine that the application is intentionally stalling, since it's not actually sleeping. In addition, logging all 960 million write instructions takes a great deal of time and complicates analysis for both types of tools.

Rombertik has many such techniques for obfuscation when it's being analyzed or reverse-engineered, but its final anti-modification technique has the potential to cause significant damage. If the malware detects that it has been modified for analysis, it tries to overwrite the machine's MBR; if it does not gain permission to overwrite the MBR, it proceeds to destroy all of the files in the user's home folder. When the machine is rebooted, it becomes inoperable.

If Rombertik passes through all of its anti-modification checks, it will finally begin its primary task: stealing any data that users type into their browsers and forwarding that information to its server.

Rombertik: Raising the Bar for Security Defenders

The sobering characteristics of Rombertik are its enhanced techniques for evading analysis and its capability to damage the operating system software of the machines on which it is running. This approach certainly raises the bar for security defenders, who will no doubt run afoul of malware like this in the future. It's a solid bet other malware authors will not only appropriate Rombertik's tactics but may make them even more destructive.

Good security practices can help protect users, as can educating users to avoid clicking attachments from unknown senders. However, meeting the threat of well-crafted and dangerous malware like Rombertik also calls for a defense-in-depth approach that covers the entire attack continuum—before, during, and after an attack.

See the Talos Group blog post **"Threat Spotlight: Rombertik - Gazing Past the Smoke, Mirrors, and Trapdoors"** for further analysis of Rombertik malware.

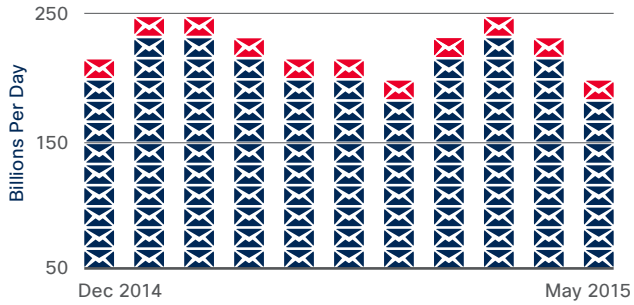
2 "Threat Spotlight: Dyre/Dyreza: An Analysis to Discover the DGA," Cisco Security blog, March 30, 2015, http://blogs.cisco.com/security/talos/threat-spotlight-dyre.

Spam Volume Remains Consistent

As adversaries develop more sophisticated methods of breaching network defenses, spam and phishing emails continue to play a major role in these attacks. Yet the volume of worldwide spam has remained relatively consistent, as seen in Figure 13.

As shown in Figure 14, a country-by-country analysis indicates that while spam volume is increasing in the United States, China, and the Russian Federation, it remains relatively stable in other regions. We attribute these shifts to fluctuations in the relative activity of the underlying spammer networks.

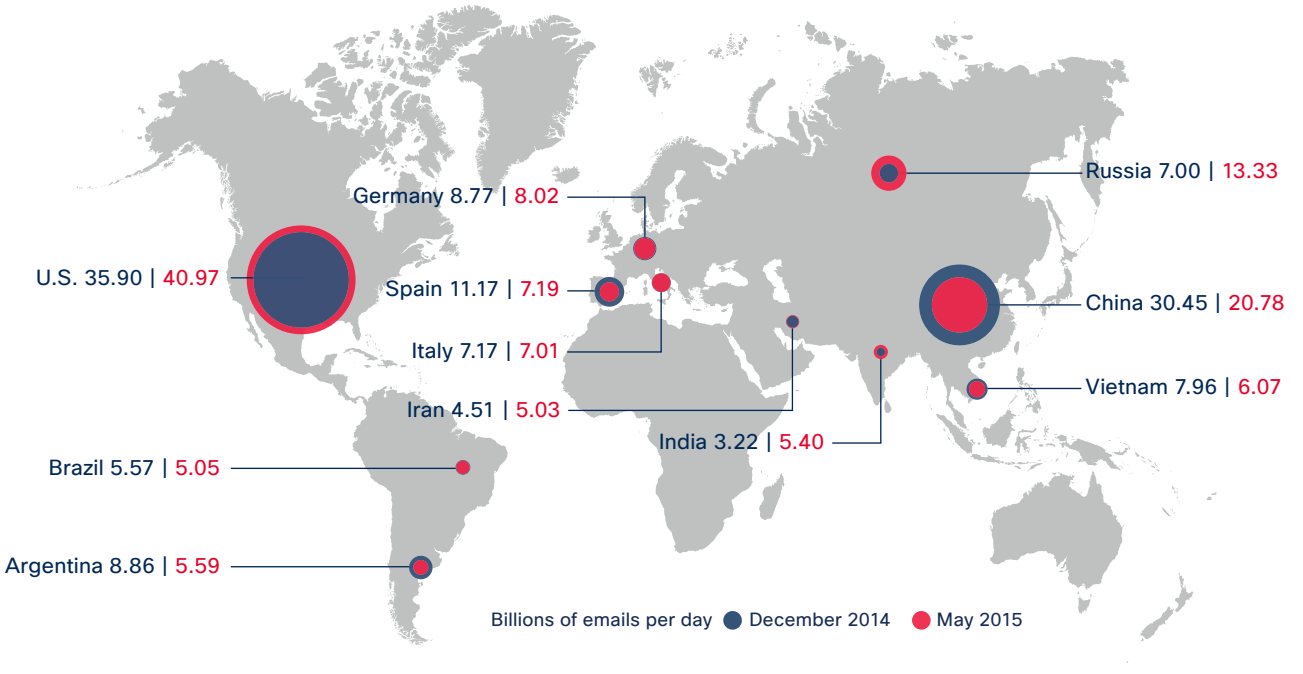
Figure 13. Spam Volume Is Steady



Source: Cisco Security Research

Figure 14. Spam Volumes by Country

Share the report



Source: Cisco Security Research

Threats and Vulnerabilities: Common Coding Errors Create Avenues for Exploits

In examining the most common vulnerabilities for the first half of 2015, we find the same types of errors showing up year after year. For example, as seen in Figure 15, buffer errors are once again at the head of the list of Common Weakness Enumeration (CWE) threat categories, as defined by the National Vulnerability Database (https://nvd.nist.gov/cwe.cfm).

Buffer errors, input validation, and resource management errors, the three most frequent CWEs in Figure 15, are perennially among the five most common coding errors being exploited by criminals. Assuming vendors are aware of the CWE list, why do these errors keep occurring with such regularity?

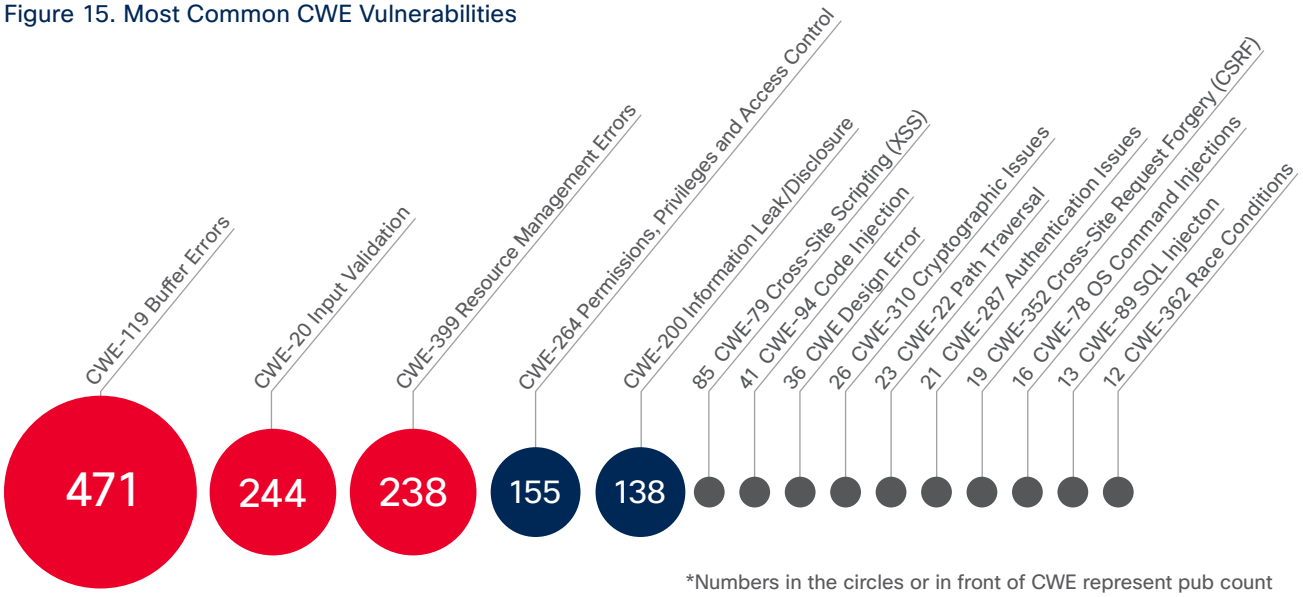
The problem lies in insufficient attention being paid to the secure development lifecycle. Security safeguards and vulnerability tests should be built in as a product is being developed. Instead, vendors wait until the product reaches the market and then address its vulnerabilities.

Vendors need to place more emphasis on security within the development lifecycle, or they will continue to spend time and money on catch-up efforts to detect, fix, and report vulnerabilities. In addition, security vendors must assure customers that they are doing everything possible to make their solutions trustworthy and secure—in this case, by making vulnerability testing a crucial component of product development.

Third-Party Vulnerabilities

Since the April 2014 release of Heartbleed, the security flaw in the handling of Transport Layer Security (TLS), third-party software vulnerabilities have become an aggravating problem for enterprises seeking to repel attackers. Heartbleed signaled the beginning of closer examinations of third-party software (TPS) vulnerabilities, particularly as open-source solutions became more popular.

Figure 15. Most Common CWE Vulnerabilities



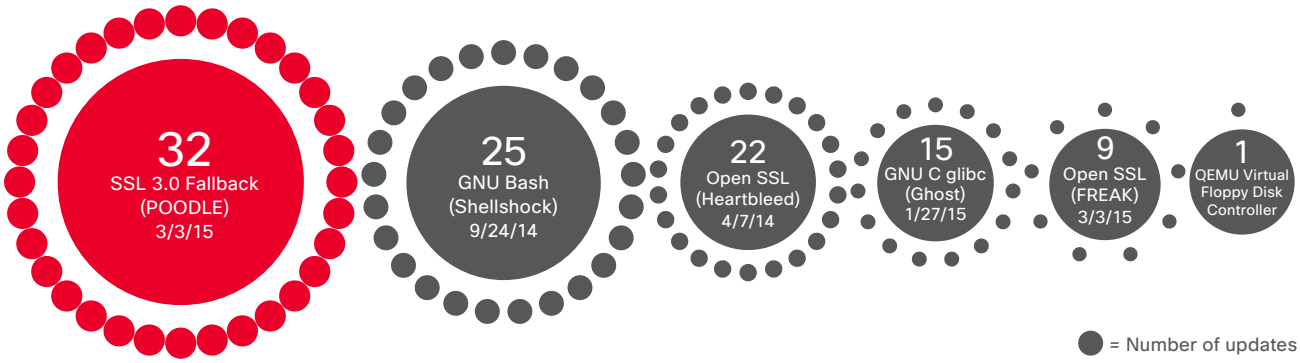
*Numbers in the circles or in front of CWE represent pub count

Source: Cisco Security Research

Share the report

Figure 16. Open-Source Vulnerabilities

Share the report



Source: Cisco Security Research

Figure 16 shows six of the most common open-source vulnerabilities that we tracked in the first half of 2015. (For timeline details of vendor responses, click on the vulnerabilities above, and scroll down to Alert History.)

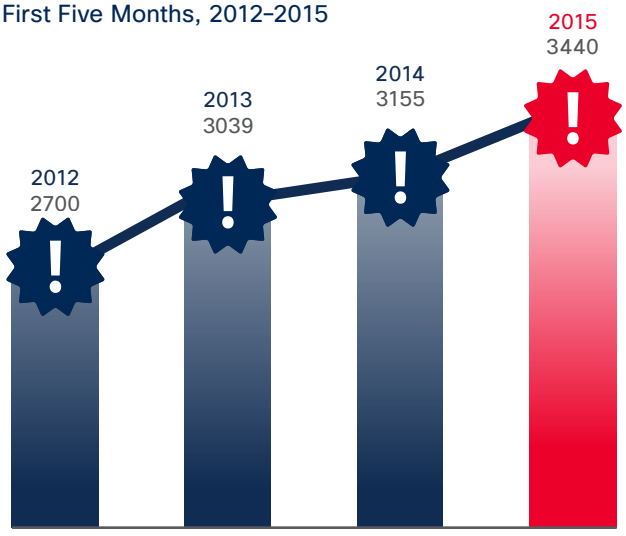
Open-source vulnerabilities pose an inherent challenge: Shutting down a vulnerability requires coordination by many vendors. The community of developers who maintain open-source solutions may quickly provide a fix or a patch, but the fixes then need to be integrated into all versions of the product.

The good news: As awareness of open-source vulnerabilities grows, the security community is responding more quickly to them. For example, when the VENOM (Virtualized Environment Neglected Operations Manipulation) vulnerability, which affected open-source code for virtualization systems, first emerged, vendors released patches even before the vulnerability was publicly announced.

Recent investments in OpenSSL by several leading technology companies, including Cisco, are helping to improve the OpenSSL infrastructure. The investments take the form of donations to the Linux Foundation. These investments are helping security researchers conduct code reviews that should help identify fixes and patches for open-source solutions.[3]

With open-source software in place in many enterprises, security professionals need to gain a deeper understanding of where and how open-source is used in their organizations, and whether their open-source packages or libraries are up to date. This means that, moving forward, software supply chain management becomes even more critical.

Figure 17. Cumulative Annual Alert Totals, First Five Months, 2012–2015



Source: Cisco Security Research

Share the report

3 "Cisco, Linux Foundation, and OpenSSL," Cisco Security blog, April 25, 2014: http://blogs.cisco.com/security/cisco-linux-foundation-and-openssl.

Cumulative annual IntelliShield alert totals for the first five months of 2015 are rising slightly compared to the same period in 2014 (Table 1). As Cisco has noted previously, the ongoing increase in alert totals is a likely result of vendors' focus on security testing and on finding and correcting their own vulnerabilities.

Table 1. Alert Activity Levels

	Updated	New	Total
January	211	359	570
February	255	379	634
March	285	471	756
April	321	450	771
May	237	472	709
	1309	**2131**	**3440**
Jan – May 2014		**Total Alerts: 3155**	

Source: Cisco Security Research

Table 1 shows activity for reported alerts as well as updated alerts. We saw an increase of 9 percent in the number of total alerts in May 2015 over those reported for May 2014. Security vendors and researchers are finding a growing number of new alerts, while the number of updated alerts has dropped. Organizations must therefore increase their focus on patch management.

Table 2 illustrates some of the most commonly exploited vulnerabilities, according to the Common Vulnerability Scoring System (CVSS). The U.S. National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD) provides a framework for communicating the characteristics and impacts of IT vulnerabilities and supports the CVSS.

The Urgency score in the CVSS table indicates that these vulnerabilities are being actively exploited. By scanning the list of products being exploited, enterprises can also determine which of these products they are using and therefore need to monitor and patch.

Table 2. Most Commonly Exploited Vulnerabilities

Alert ID	Headline	Urgency	Credibility	Severity	CVSS Base	CVSS Temp
35845	GNU Bash Environment Variable String Value Handling	●●●●○	●●●●●	●●●●○	10.0	9.0
35816	GNU Bash Environment Variable Command Injection Vulnerability	●●●●○	●●●●●	●●●●○	10.0	8.6
37181	GNU glibc gethost Function Calls Buffer Overflow Vulnerability	●●○○○	●●●●●	●●●●○	10.0	7.8
37318	Adobe Flash Play Remote Code Execution Vulnerability	●●○○○	●●●●●	●●●●○	9.3	7.7
37848	Elasticsearch Groovy Scripting Engine Sandbox Bypass	●●○○○	●●●●●	●●●●○	9.3	7.7
37123	Adobe Flash Player Use After Free Arbitrary Code Execution	●●○○○	●●●●●	●●●●○	9.3	7.7
36849	Network Time Protocol Daemon Stack Buffer Overflow Vulnerability	●●○○○	●●●●●	●●●○○	7.5	5.5
37181	GNU glibc gethost Function Calls Buffer Overflow Vulnerability	●●○○○	●●●●●	●●●●○	10.0	7.8
36956	OpenSSL RSA Temporary Key Cryptographic Downgrade Vulnerability (FREAK)	●●○○○	●●●●●	●●○○○	5.0	4.1

Source: Cisco Security Research

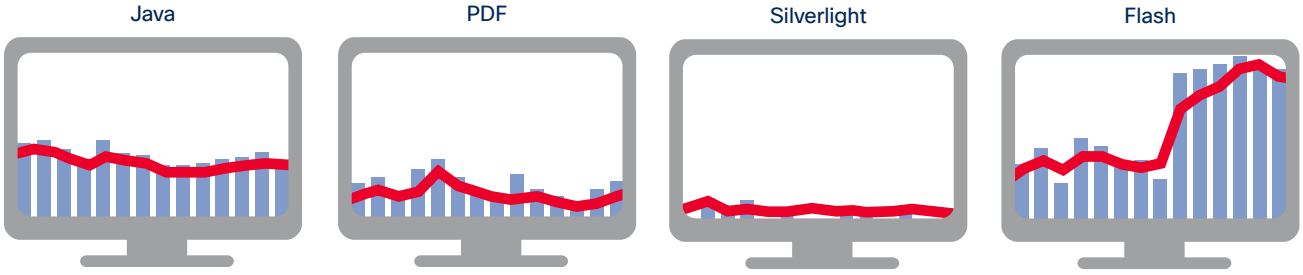
Decline in Exploits Using Java

Continuing a trend we monitored and covered in the Cisco 2015 Annual Security Report,[4] exploits involving Java were on the decline in the first half of 2015. Java used to be a favored attack vector for online criminals, but security improvements and stepped-up patching efforts have forced attackers away from it. No zero-day exploits for Java have been disclosed since 2013.

Oracle has taken several steps to improve Java's security, such as phasing out unsigned applets. The latest version, Java 8, also includes stronger controls than prior releases. It is more difficult to exploit because it requires input from human users, such as dialog boxes that ask the user to enable Java.

Oracle announced in April 2015 that it would end support for Java 7.[5] Unfortunately, when vendors end support for a given version of a product, enterprises do not fully adopt the new version immediately. This lag time leaves a window of opportunity for criminals to exploit vulnerabilities in the now-unsupported version. As the year progresses, we may see an uptick in the number of Java exploits as enterprises move from Java 7 to Java 8.

Figure 18. Most Common Malware Vectors



Source: Cisco Security Research

Figure 18 shows the log volume of Java, PDF, and Flash exploits for the first half of 2015. PDF exploits vary on a month-to-month basis, but in general, are not as common as Flash exploits. Flash is a favored tool of developers of exploit kits, so its presence in the log volume chart above may be directly tied to outbreaks of criminal activity involving exploit kits such as Angler (see page 10). In addition, the volume of Silverlight exploits is very small compared with the number of exploits based on Flash, PDF, and Java.

4 Cisco 2015 Annual Security Report, Cisco, January 2015: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

5 "Oracle to End Publicly Available Security Fixes for Java 7 This Month," by Paul Krill, *InfoWorld*, April 15, 2015: http://www.infoworld.com/article/2909685/application-development/oracle-cutting-publicly-available-security-fixes-for-java-7-this-month.

Malware Authors Adopt Detection and Evasion Tactics

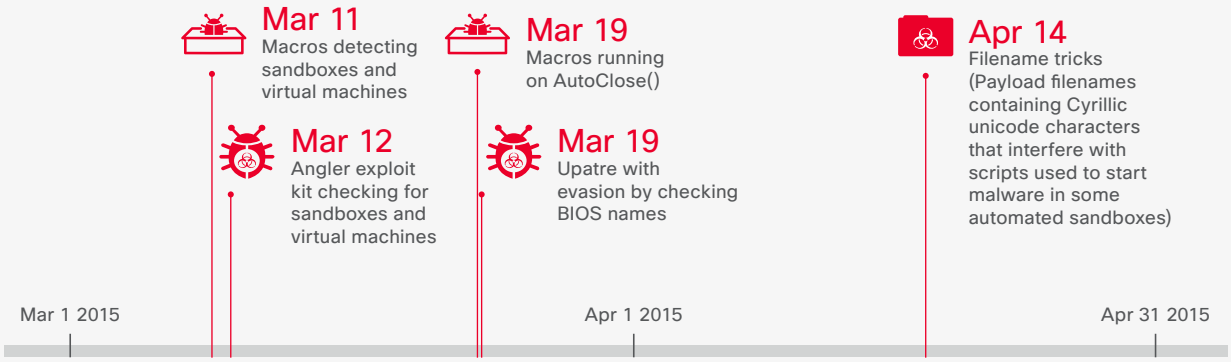
Online criminals have become adept at hiding their activities from security researchers and technology solutions. For example, they create malware that attempts to evade traditional controls such as the sandboxes that researchers use to launch malware and record its activity.

In the cases we examined, such malware would fail to detonate if it detected sandbox activity. This tactic was seen in a variant of the Angler exploit kit, some variants of Upatre malware, and malicious Microsoft Office documents.

To combat malware using these evasion tactics, organizations need to adopt a defense-in-depth approach that ideally includes the capability to scan and identify malware retrospectively, after it slips through initial lines of defense.

Recent Sandbox Detection

Sandbox detection is not a new tactic on the part of malware authors, but it is becoming more commonplace, according to our researchers, who found the following incidents between March and April 2015:



Vertical Risk of Malware Encounters: No Industry Is Immune to Attack

Cisco has refined and simplified its methodology for tracking high-risk verticals for web malware encounters in order to deliver more precise results. We no longer compare the median encounter rate for all organizations that use Cisco® Cloud Web Security with the median encounter rate for all companies in a specific sector that are using the service. We now compare the relative volumes of attack traffic ("block rates") with those of "normal" or expected traffic.

Figure 19 shows 25 major industries and their relevant 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.

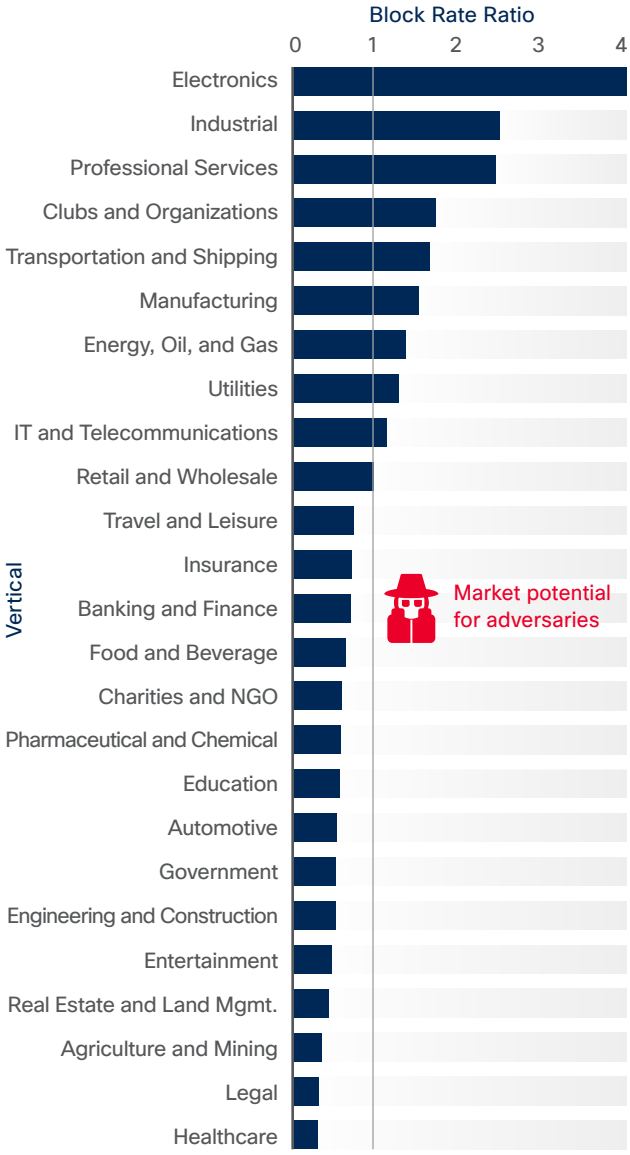
For example, block rates for the retail and wholesale industry are in proportion to the volume of traffic that was observed for that industry.

In examining the block rates of Cisco customers, we determined that the electronics industry has the most blocked attacks among the 25 industries tracked. Cisco attributes the electronic industry's high proportion of block rates to an outbreak of Android spyware.

As seen in Figure 19, most industries hover at the "normal" level (the 1.0 line) for the ratio of attacks to normal network traffic. However, singling out industries currently above the 1.0 line as being significantly more vulnerable to attacks may be misleading, especially as this analysis only covers the first half of 2015.

In addition, no industry should consider itself "safer" than other industries in terms of being a target. Every organization in every industry should assume that it is vulnerable, that attacks will happen, and that it should implement defense-in-depth strategies accordingly.

Figure 19. Block Rates of Verticals Compared with Observed Traffic Volume



Source: Cisco Security Research

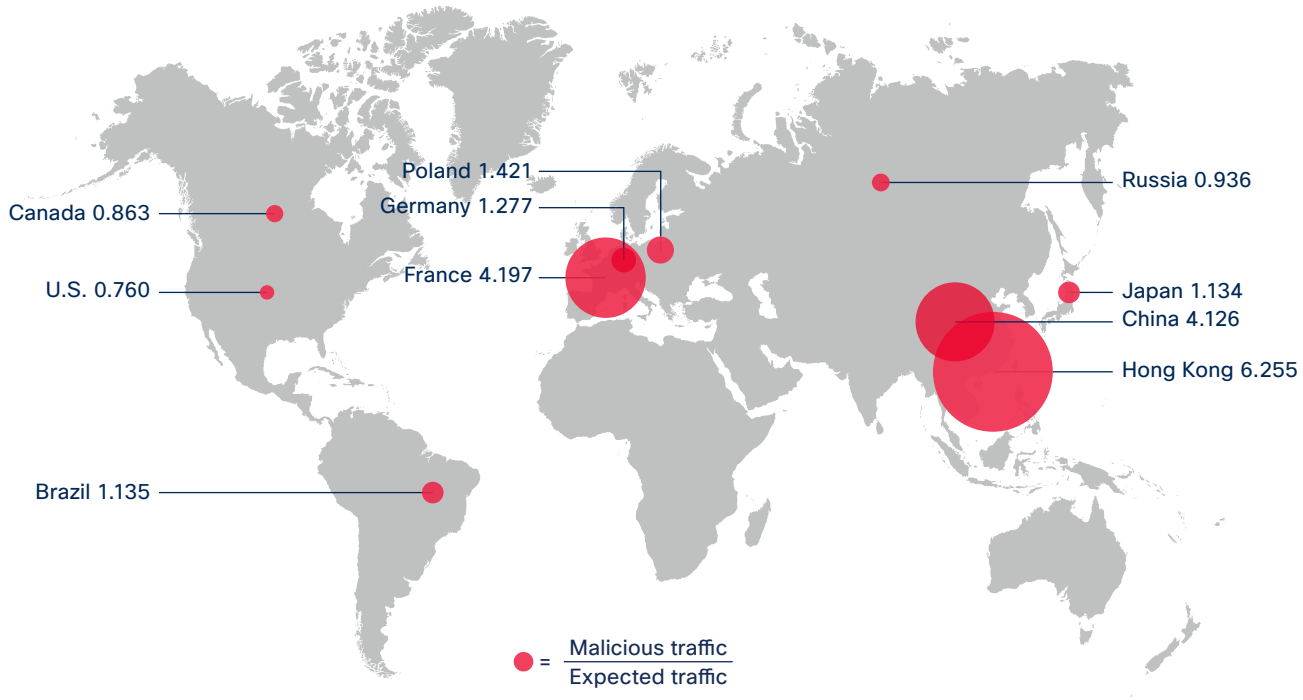
Block Activity: Geographic Overview

Cisco researchers also examined the countries and regions where malware-based block activity originates, as seen in Figure 20. The countries were selected for study based on their volume of Internet traffic. A block ratio of 1.0 indicates that the number of blocks observed is proportional to network size.

Malware acquires a foothold on vulnerable devices. Countries and regions with block activity that we consider higher than normal likely have many web servers and hosts with unpatched vulnerabilities on their networks. A presence in large, commercially viable networks that handle high Internet volume is another factor for high block activity.

Figure 20 relates to where servers are hosted. This graphic does not attribute patterns of malicious web activity to the depicted countries or regions. Hong Kong, which ranks number one on the list, is an example of a region where a high percentage of vulnerable web servers are observed. A small number of networks hosted in France participated in an outbreak midway through the reporting time period, which raised its profile more than expected.

Figure 20. Web Blocks by Country or Region



Source: Cisco Security Research

Types of Web-Based Attacks

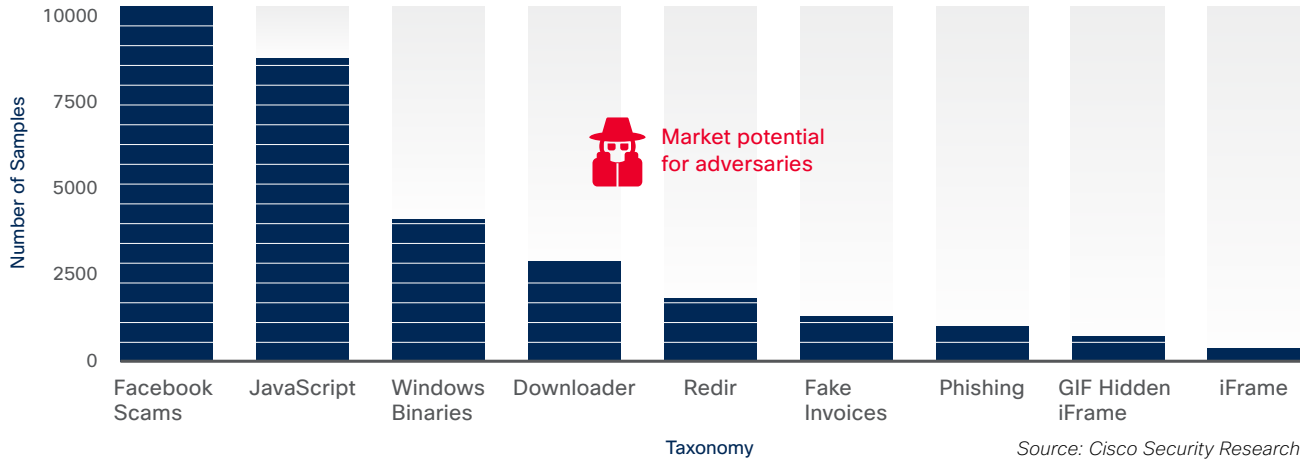
Figures 21 and 22 show the various types of techniques that adversaries are using to gain access to organizational networks. Figure 21 illustrates the most commonly seen methods, including Facebook scams and malicious redirects.

Figure 22 shows lower-volume attack methods observed in the blind sample we examined. Note that "lower volume" does not mean "less effective." Lower-volume attack methods, and the malware associated with them, can represent emerging threats or highly targeted campaigns.

Therefore, when monitoring web malware, it is not enough to simply focus on the types of threats most commonly seen. The full spectrum of attacks must be considered.

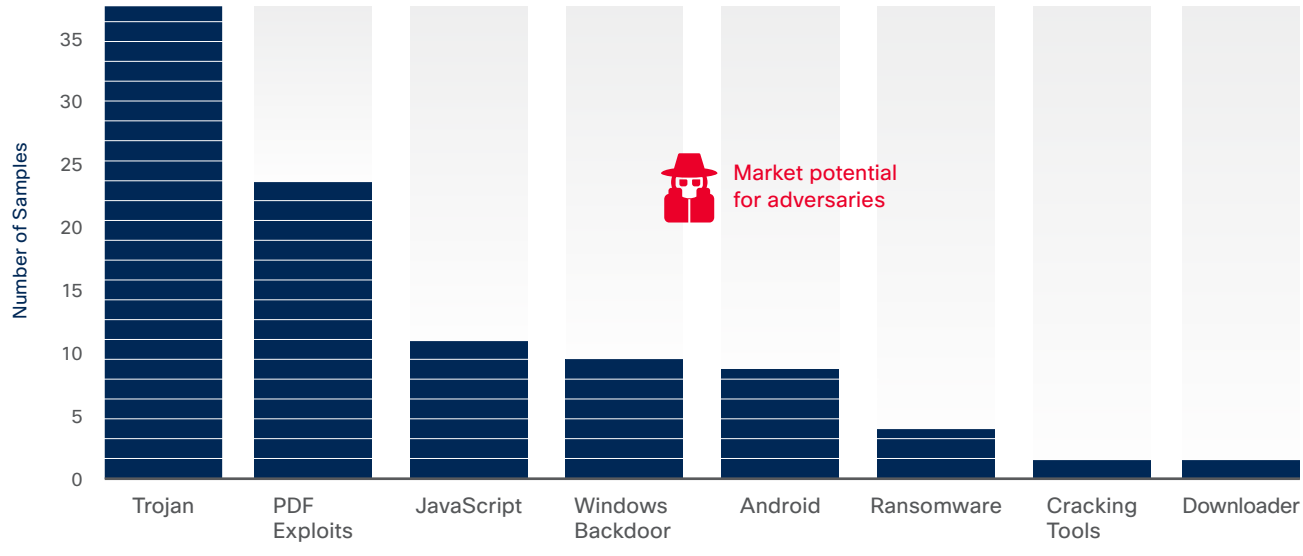
Figure 21. Most Commonly Observed Methods

Share the report



Source: Cisco Security Research

Figure 22. Sample of Lower-Volume Methods Observed



Source: Cisco Security Research

Malvertising Update: Widespread Web-Based Threat Mutates to Evade Detection, Increase Effectiveness

As reported in the Cisco 2015 Annual Security Report,[6] we conducted an in-depth analysis in 2014 of a highly sophisticated, botnet-like, web-based threat that uses malvertising from web browser add-ons as a medium for distributing malware and unwanted applications. This family of malware has a clear signature: Adware MultiPlug. The browser extensions are bundled with other seemingly useful yet unwanted applications, such as PDF tools and video players.

Users are compromised when they install these unwanted applications and the bundled software that comes with it. In many cases these are browser add-ons, which they either inherently trust or view as benign. User information—specifically, the internal or external webpage the user is visiting (and not user credientials)—is exfiltrated by these browser extensions once installed.

Distribution of the malware follows a pay-per-install (PPI) monetization scheme, in which the publisher is paid for every installation of software bundled in the original application. This leads to the increased prevalence of malware deliberately engineered for lower impact on the affected host and optimized for long-term monetization over a large affected population.

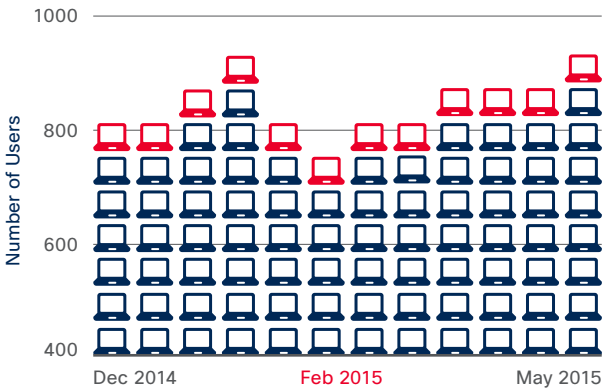
Cloaked in Common Web Traffic

Cisco has been monitoring this threat for more than a year. We have observed that the threat is constantly changing in order to remain undetected. The average time period that the threat uses a domain name is three months, and add-on names still change continuously. As reported in the Cisco 2015 Annual Security Report, we have so far discovered more than 4000 different add-on names and over 500 domains associated with this threat.

In January 2015, the researchers started to notice that the threat was mutating. Specifically, it abandoned its URL-encoding scheme for evading detection so it could cloak itself in common web traffic instead. This shift in tactics appears to be increasing the threat's effectiveness at compromising users.

We traced traffic associated with this new pattern back to August 2014, but it only became noticeable due to the volume of traffic in the December 2014–January 2015 time frame. As Figure 23 shows, the number of affected users associated with this threat has been trending upward overall since February.

Figure 23. Number of Users Affected, by Month, December 2014–May 2015



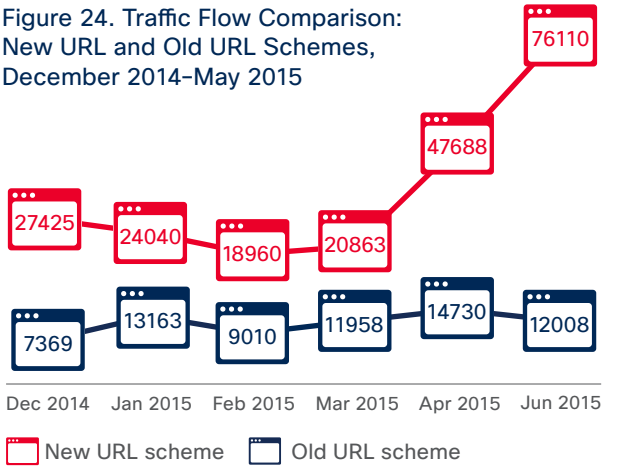
Source: Cisco Security Research

For more detail on this research, see the Talos Group blog post **"Bad Browser Plug-Ins Gone Wild: Malvertising, Data Exfiltration, and Malware, Oh My!"**

6 Cisco 2015 Annual Security Report, Cisco, January 2015: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

Figure 24 illustrates how the number of traffic flows related to the new URL scheme has been dramatically outpacing those of the old scheme, especially since March 2015.

Figure 24. Traffic Flow Comparison: New URL and Old URL Schemes, December 2014–May 2015



Source: Cisco Security Research

Time to Detection: Defined

We define "time to detection," or "TTD," as the window of time between the first observation of a file 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.

The "retrospectives" category in Figure 25 shows the number of files that Cisco initially categorized as "unknown" that were later converted to "known bad."

The number of retrospectives has been increasing since December 2014. This trend is yet another indicator that malware creators are innovating rapidly to stay one step ahead of security vendors. However, at the same time, the median TTD for threat detection by Cisco has been declining.

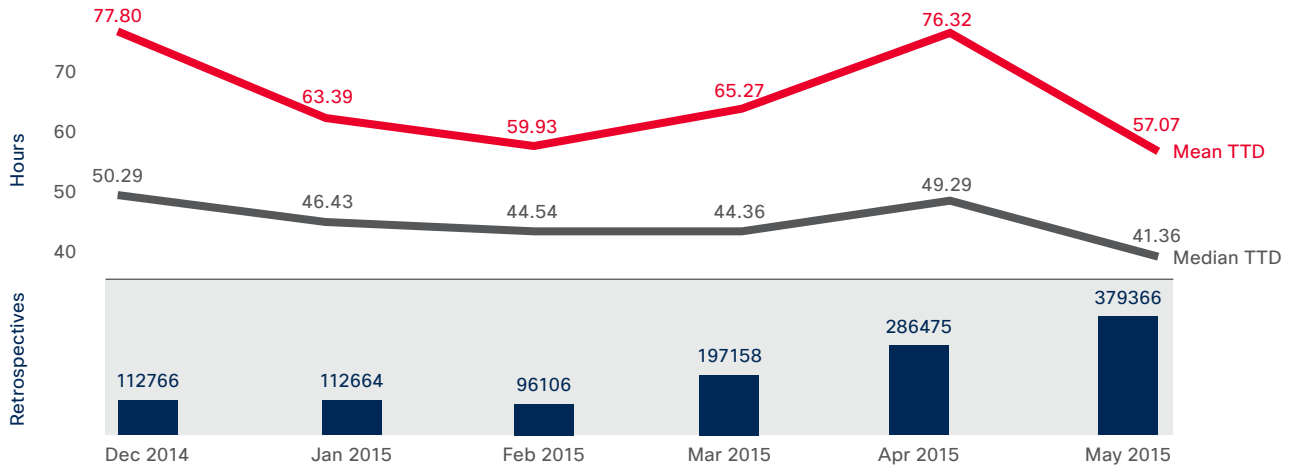
In December 2014, the median TTD—meaning when analysis revealed an unknown file to be a threat—was about two days (50 hours). The current industry standard for time to detection is 100 to 200 days, an unacceptable level, given how rapidly today's malware authors are able to innovate.

We attribute the recent upward trend in retrospectives to an increase in evasive activity (see "Malware Authors Adopt Detection and Evasion Tactics," page 25) and to successful payload deliveries of new Flash exploits by the Angler and Nuclear exploit kits (see page 9).

From January to March, the median TTD was roughly the same—between 44 and 46 hours, but with a slight trend downwards. In April, it had edged up slightly to 49 hours.

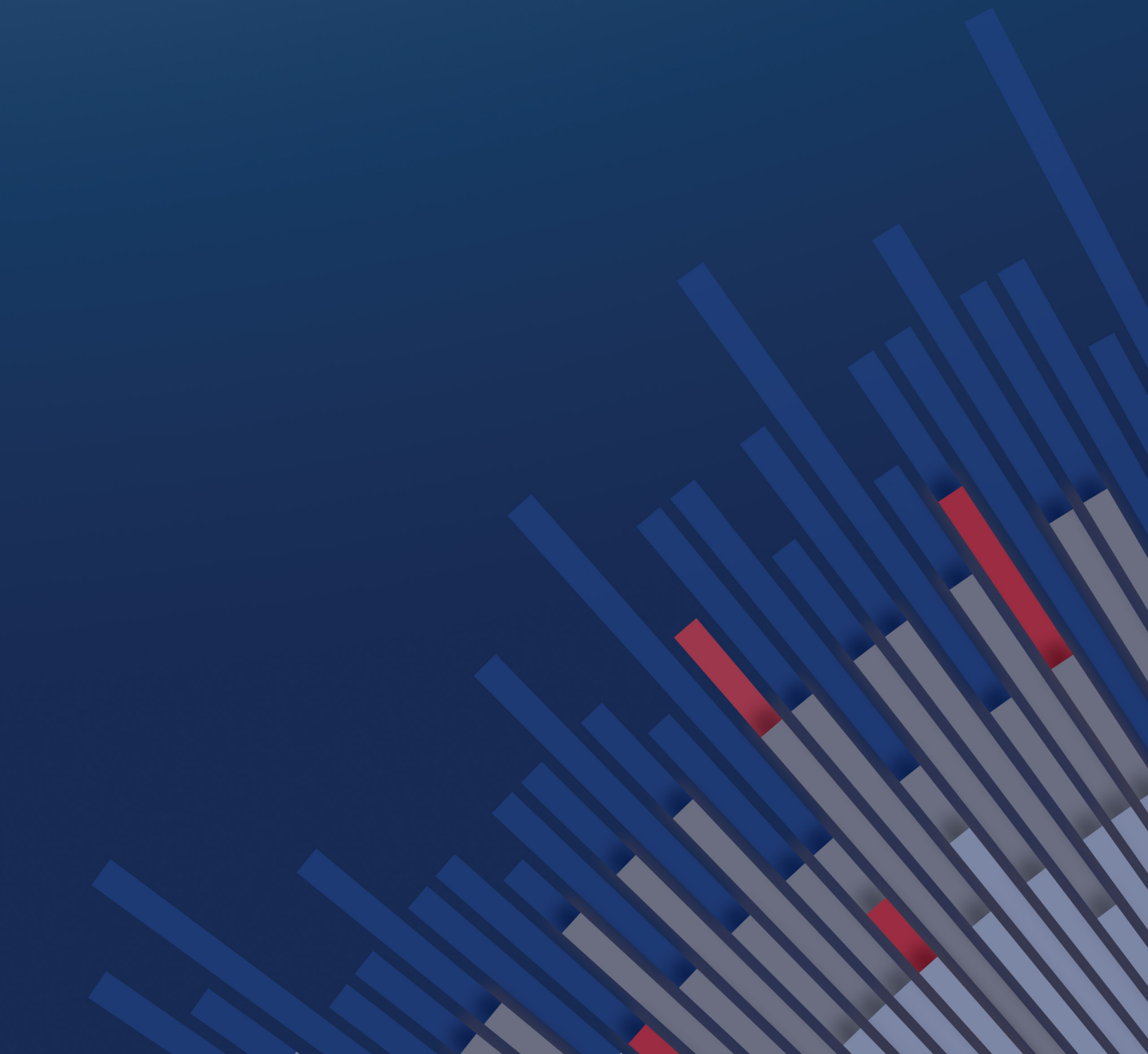
However, by the end of May, TTD for Cisco had decreased to about 41 hours. This improvement is due partly to Cisco's ability to quickly identify commodity malware such as Cryptowall, which is evasive but not novel.

Figure 25. Retrospectives, Mean TTD, and Median TTD, December 2014–May 2015



Source: Cisco Security Research

Analysis and Observations



Cybersecurity Call to Action: Faster Innovation by Security Vendors

Cisco security experts suggest that change is imminent for the security industry. A wave of consolidation and integration is needed to develop innovative, adaptive, and trustworthy security solutions that can reduce time to detection and prevent attacks. In addition, our geopolitical experts provide insight into the importance of cybergovernance for supporting innovation and economic growth in business on the global stage.

In a world where the compromise of users and systems is both assured and assumed, detection of evasive threats is obviously a necessary focus for organizations and security teams. Threat activity, including activity from nation-states, is only increasing. Many organizations are therefore thinking even more seriously about developing business continuity plans that can help them recover critical services following a cyberattack against their business or the infrastructure that helps to support it.

However, we also see noticeable demand from both businesses and individual users for the security industry to develop capabilities that can more effectively deflect—and not just detect—cyberattacks. At the very least, they seek solutions that provide faster time to detection and resolution.

Security complexity stands in the way of meeting these demands—for now.

On one side of the security industry are large, well-established players building security suites based on one or more standout products. However, these suites may also contain other solutions that are not as effective as, or do not work with, other leading solutions.

Niche vendors, meanwhile, are developing products to help fill specific security gaps. Many organizations are quick to invest in the latest innovation that fills a known gap, instead of stepping back to look at security holistically.

The result is a "patchwork quilt" of products that is difficult for security teams to manage. The solutions may have overlapping capabilities, may not meet industry standards, and are likely not interoperable. And niche technologies that cannot be deployed at scale to meet the needs of average users are typically short-lived, no matter how effective they may be.

Additionally, many security technologies require organizations to overhaul their security architecture just to adapt to the latest risks. These technologies, whether they're from one side of the security industry spectrum or the other, are not capable of evolving with the changing threat landscape. This is not a sustainable model.

Industry Consolidation and Integrated Threat Defense

Our security experts suggest that the need for adaptive solutions will lead to significant change in the security industry within the next five years. We will see industry consolidation and a movement toward an integrated threat defense architecture that provides visibility, control, intelligence, and context across many solutions.

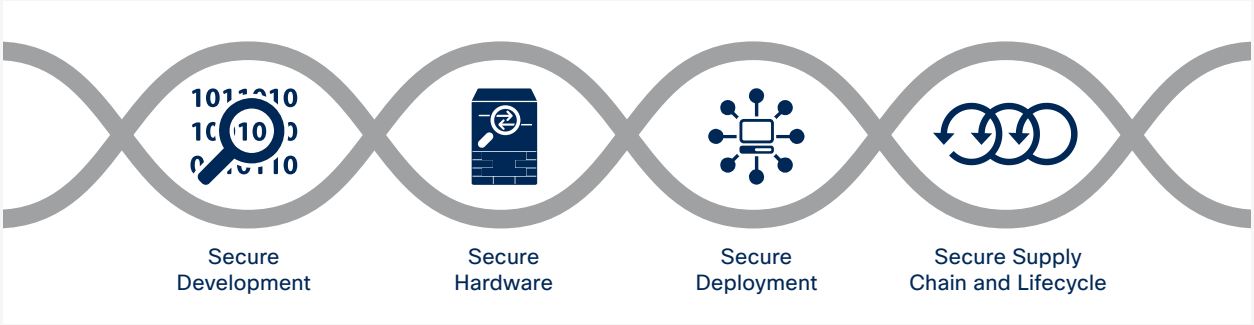
This detection-and-response framework will support a faster response to both known and emerging threats. Core to this architecture is a visibility platform that delivers full contextual awareness. It must be continuously updated to assess threats, correlate local and global intelligence, and optimize defenses. Local intelligence will provide context regarding infrastructure while global intelligence correlates all detected events and indicators of compromise for analysis and immediate, shared protection.

The intent of the visibility platform is to build a foundation that all vendors can operate on and contribute to. This system would take in and act on the massive volume of security information available from the security community. The visibility it provides would give security teams more control, so they can deliver better protection across more threat vectors and thwart more attacks.

This is the direction the security industry must take to help all end users defend themselves from the sophisticated tactics of today's threat actors. However, developing an integrated threat defense, as it is described here, will require better cooperation, dialogue, and coordinated action among all security vendors—niche innovators and long-standing players alike.

The industry is making strides to share information more proactively and in appropriate ways, especially through alliances. But real-time, automated exchange of threat information is required to spur necessary innovation in security defense and to achieve systemic response across the stack of deployed security. The faster the industry can distribute knowledge and intelligence throughout the network in a cohesive and acceptable way, the less likely adversaries will enjoy continued success and anonymity.

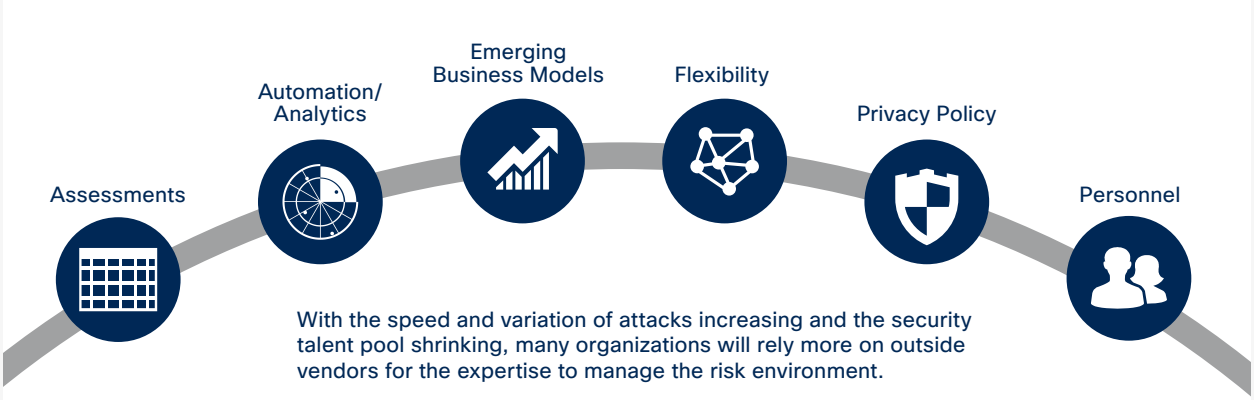
Trustworthy Products



As more consolidation and integration in the security industry unfolds over the next five years, organizations that purchase new security products and services will need to make sure those solutions are effective, sustainable, and trusted.

They should take time to understand what security and other IT vendors are doing to build security into their products. They must verify that these products remain trustworthy through every point in the supply chain that delivers those products to them. More than that, they should ask vendors to demonstrate that their products can be trusted and to back up their claims contractually.

The Value of Expertise



Security vendors have an important role to play in helping end users understand the importance of investing in trustworthy solutions and keeping security technology up to date. Organizations that rely on outdated infrastructure are placing their data, systems, and users—their entire business—at risk.

The worsening shortage of security talent means that many organizations have limited skilled resources to monitor developments in both the risk environment and vendor landscape. Lack of access to in-house security expertise is a key factor for the piecemeal or "patchwork quilt" approach that many companies take when building their security defenses (see page 32).

Enlisting third-party expertise offers organizations the flexibility to pivot with the shifting threat landscape. Security services providers are well positioned to look at security holistically and to help businesses invest in and get the most from their security investments.

In addition to augmenting lean security teams, third-party experts can offer assessments that test the strength of an organization's security posture. And they can help identify effective strategies for addressing vulnerabilities and other risks. They can also help organizations deploy automation and manage solutions that provide the analytics and real-time threat correlation needed to combat hard-to-detect and rapidly emerging threats.

Some organizations look to security services providers for guidance as they embrace mobile, social, cloud, and other emerging business models. Some seek help in navigating data privacy and data sovereignty requirements in markets where they operate. Others, including small and midsize businesses looking to take advantage of security technologies and operations that larger enterprises use, tap third-party experts to help them find managed and hosted models that meet the needs of their business.

A Global Cybergovernance Framework to Support Future Innovation

Businesses around the globe are becoming increasingly reliant on the Internet to support business models that make them more competitive and benefit their consumers. But they face adversaries who are deploying tactics that can undermine their success. If left unchecked, cyber risks will have profound consequences on innovation and economic growth for all businesses.

Cisco geopolitical experts see a cohesive, multi-stakeholder cybergovernance framework as a positive step toward sustaining business innovation and economic growth on the global stage, supporting organizations' investments in the digital economy. However, the current governance framework does not protect businesses from cyberattacks. These include not just those that lead to data breaches and the theft of intellectual property, but also those capable of disrupting global supply chains, damaging critical infrastructure, or worse.

Many companies don't pursue remedies to cyberattacks because they lack the support of law enforcement from other countries. However, more governments are becoming open to the concept of public attribution of attacks and the imposition of sanctions.

The lack of effective global cybergovernance can also prevent the collaboration necessary in the security industry to create adaptive technologies that can detect and prevent new threats. Recent changes were proposed to the Wassenaar Arrangement,[7] a voluntary multinational agreement intended to control the export of certain "dual-use" technologies, including intrusion software such as digital surveillance tools. These proposals threaten to constrain this control and prevent security researchers from sharing information with their industry peers without heavy regulatory burdens. This development may have a significant impact on security research capabilities and further exacerbate the talent shortage in the industry.

Greater Harmonization of Rulemaking: A Future Path?

The question of boundaries—especially with regard to how governments collect data about citizens and businesses and share, or not share, that information between jurisdictions—is a significant hurdle to the type of cooperation needed to achieve cohesive cybergovernance. As the Internet of Things takes shape and the world becomes more interconnected, industry, governments, and society will need to work together more effectively to address growing security and privacy challenges.

Currently, cooperation—and trust—between entities on the global stage is limited at best between some players, and nonexistent between others. Even entities with strong alliances have competing philosophies about cybergovernance, and they are naturally focused on enacting laws that benefit their sovereign interests and their citizens. Much like discussions about climate change, only a handful of players will come to the table to talk, and consensus is hard to achieve even for small measures.

At the regional level, at least, there are some efforts to look beyond national borders. For instance, within the European Union (EU), there is movement to improve the coordination of information sharing through the proposed Network and Information Security (NIS) Directive. This directive "aims to ensure a high common level of cybersecurity in the EU" by, among other things, "improving cooperation between Member States, and between public and private sectors."[8]

The EU and the United States also appear to be close to signing a data protection "umbrella agreement" that will set data protection standards for data shared between law enforcement authorities. This agreement will not answer the bigger questions as to how and what type of data can be accessed. But it may go some way to improve the tense atmosphere between the two powers, which has threatened to put companies in the middle of the jurisdictional conflict. Legal, technical, and security teams for organizations that operate in the EU and the United States will need to work together on access requirements if the umbrella agreement is signed.

7 "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items," *Federal Register*: https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

8 "Network and Information Security (NIS) Directive," European Commission: http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive.

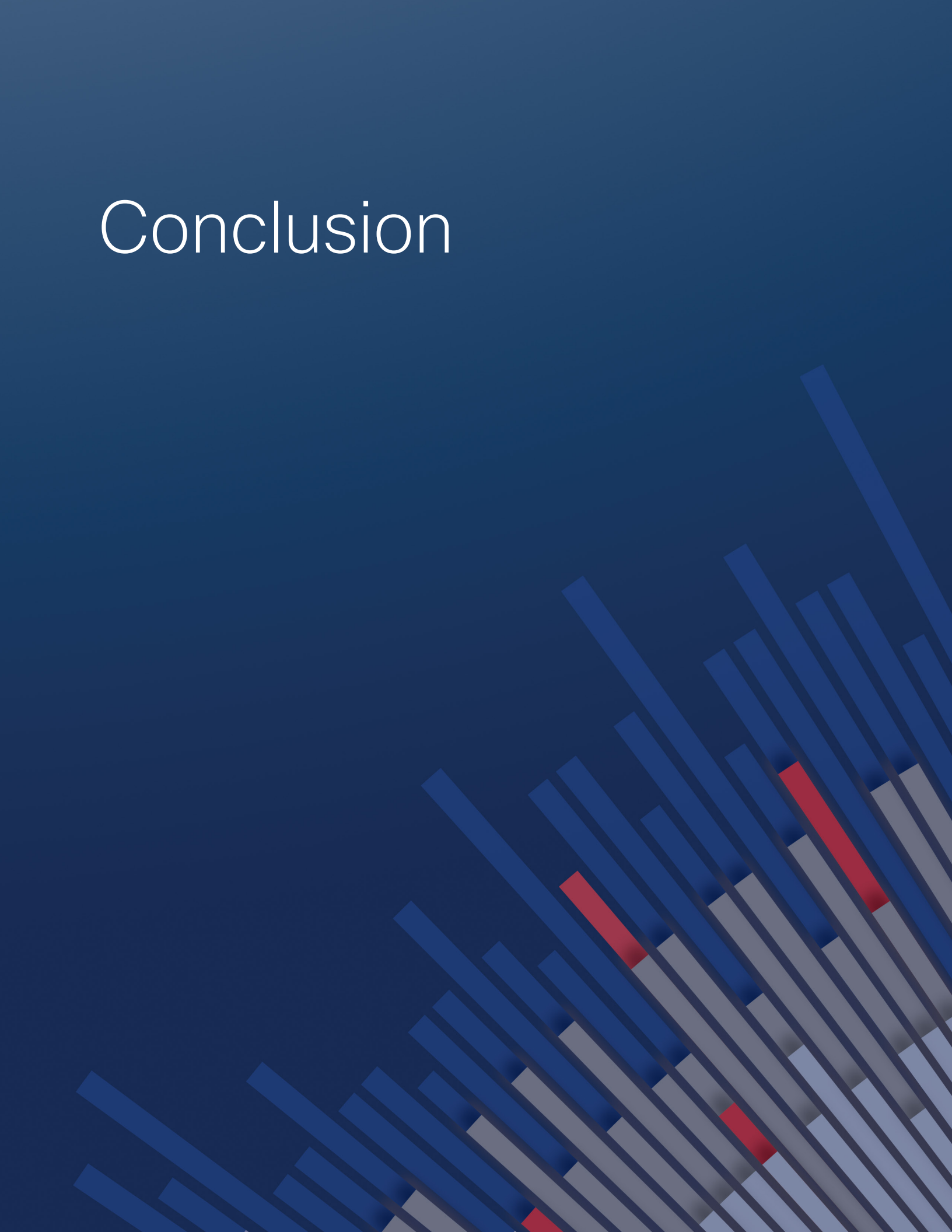
There is other legislation in the works in Europe that could end up creating more boundaries, however, especially for businesses. EU institutions are looking to finalize the new General Data Protection Regulation (GDPR) by the end of the year, replacing the existing EU Data Protection Directive.

This regulation contains a broad definition of personal data and prescriptive rules on how such data should be managed under the threat of huge fines. It will have a significant impact on how organizations that do business with and in the EU gather, store, and use customer data, and how they report data breaches. Intended to create greater accountability and transparency, the GDPR will, at least, compel many organizations to examine their approach to data privacy and governance and adopt best practices.

Technical teams, for example, will need to take into account design considerations around limitations or difficulties associated with moving data across borders. They will need to be aware of different regional sensitivities of data that is characterized as "personal" or not. Security teams will also need to be mindful of developments that affect data transfer, the definition of personal data, the legal basis for network and information security processing, and data breach reporting requirements.

Greater harmonization of rulemaking could serve as a path toward building a cybergovernance framework that elevates the advocacy of negotiations between governments regarding data protection regulations and at the same time prevents industry from getting caught in the middle. Until that happens, security practitioners need to play an active role in making sure decision makers in their organizations understand the impact that regulations issued by different countries may have on operations. Incompatible systems, burdensome or conflicting data requirements, privacy law violations, and data transfer and handling requirements are among the challenges.

Conclusion



Conclusion

The threats discussed in this report represent only a small sample of the cybersecurity challenges that organizations, their security teams, and individual users face. So far, 2015 is proving to be a year of unprecedented speed in the innovation, resiliency, and evasiveness of cyberattacks. Adversaries are intent on overcoming all barriers to their success. As fast as the security industry can develop technologies to block and detect threats, miscreants pivot or change their tactics altogether.

The innovation race between adversaries and security vendors is only accelerating, and organizations are at risk of becoming more vulnerable to attack if they sit back and watch. They need to be proactive about identifying and addressing cybersecurity risks that can affect their business and aligning the right people, processes, and technology to help them meet those challenges.

"Security needs to be part of the way organizations think–holistically–about their business," says David Goeckeler, senior vice president and general manager for the Security business group at Cisco. "There is a great deal at stake: their brand, their reputation, their intellectual property, and their customers' data. All of these things are at risk. Organizations need to take a systemic approach to minimizing that risk through an appropriate security posture."

Trustworthy products are an essential component of an effective security posture, says John N. Stewart, chief security and trust officer for Cisco. "Organizations no longer want to accept that compromise is inevitable," he says. "They are looking to the security industry to provide them with products that are reliable and resilient, and capable of deflecting even the most sophisticated threats."

About Cisco

About Cisco

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

Threat researchers from the Cisco Collective Security Intelligence (CSI) ecosystem bring together, under a single umbrella, the industry's leading threat intelligence, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open-source community 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 2015 Midyear Security Report

Collective Security Intelligence

Cisco Collective Security Intelligence (CSI) is shared across multiple security solutions and provides industry-leading security protections and efficacy. In addition to threat researchers, CSI is driven by intelligence infrastructure, product and service telemetry, public and private feeds, and the open-source community.

Talos Security Intelligence and Research Group

The Talos Security Intelligence and Research Group is made up 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.

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.

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.

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.

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.