Cisco 2014
Annual Security Report

CISCO

Executive Summary

The Trust Problem

The exploitation of trust is a common mode of operation for online attackers and other malicious actors. They take advantage of users' trust in systems, applications, and the people and businesses they interact with on a regular basis. And this approach works: There is ample evidence that adversaries are coming up with new methods for embedding their malware in networks, remaining undetected for long periods, and stealing data or disrupting critical systems.

Using methods ranging from the socially engineered theft of passwords and credentials to stealthy, hide-in-plain-sight infiltrations that execute in minutes, malicious actors continue to exploit public trust to effect harmful consequences. However, the trust problem goes beyond criminals exploiting vulnerabilities or preying on users through social engineering: it undermines confidence in both public and private organizations.

Today's networks are facing two forms of trust erosion. One is a decline in customer confidence in the integrity of products. The other is mounting evidence that malicious actors are defeating trust mechanisms, thus calling into question the effectiveness of network and application assurance, authentication, and authorization architectures.

In this report, Cisco offers data on and insights into top security concerns, such as shifts in malware, trends in vulnerabilities, and the resurgence of distributed denial-of-service (DDoS) attacks. The report also looks at campaigns that target specific organizations, groups, and industries, and the growing sophistication of those who attempt to steal sensitive information. The report concludes with recommendations for examining security models holistically and gaining visibility across the entire attack continuum—before, during, and after an attack.

Key Discoveries

Below are three key findings from the *Cisco 2014 Annual Security Report*:

Attacks against infrastructure are targeting significant resources across the Internet.

- Malicious exploits are gaining access to web hosting servers, nameservers, and data centers. This suggests the forming of überbots that seek high-reputation and resource-rich assets.
- Buffer errors are a leading threat, at 21 percent of the Common Weakness Enumeration (CWE) threat categories.
- Malware encounters are shifting toward electronics manufacturing and the agriculture and mining industries at about six times the average encounter rate across industry verticals.

Malicious actors are using trusted applications to exploit gaps in perimeter security.

- Spam continues its downward trend, although the proportion of maliciously intended spam remains constant.
- Java comprises 91 percent of web exploits; 76 percent of companies using Cisco Web Security services are running Java 6, an end-of-life, unsupported version.
- "Watering hole" attacks are targeting specific industry-related websites to deliver malware.

Investigations of multinational companies show evidence of internal compromise. Suspicious traffic is emanating from their networks and attempting to connect to questionable sites (100 percent of companies are calling malicious malware hosts).

- Indicators of compromise suggest network penetrations may be undetected over long periods.
- Threat alerts grew 14 percent year over year; new alerts (not updated alerts) are on the rise.
- Ninety-nine percent of all mobile malware in 2013 targeted Android devices. Android users also have the highest encounter rate (71 percent) with all forms of web-delivered malware.

Report Content

The *Cisco 2014 Annual Security Report* presents security insights across four key areas:

Trust

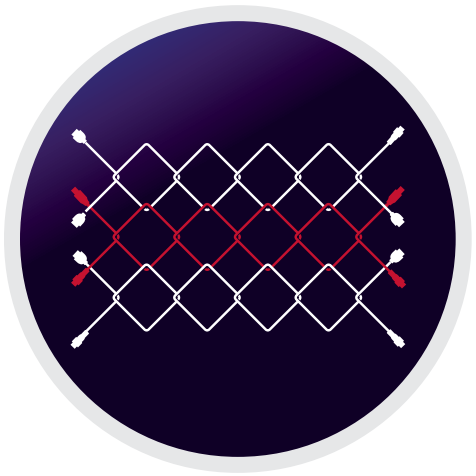
All organizations should be concerned about finding the right balance of trust, transparency, and privacy because much is at stake. In this area, we address three pressures that make security practitioners' attempts to help their organizations achieve this balance even more challenging:

- Greater attack surface area
- Proliferation and sophistication of the attack model
- Complexity of threats and solutions

Threat Intelligence

Using the largest set of detection telemetry available, Cisco and Sourcefire together have analyzed and assembled security insights from the past year:

- Attacks against infrastructure are targeting significant resources across the Internet.
- Malicious actors are using trusted applications to exploit gaps in perimeter security.
- Indicators of compromise suggest that network penetrations may be undetected over long periods.



Industry

In this section, Cisco Security Intelligence Operations (SIO) investigators elevate the discussion around industry trends that extend beyond Cisco's telemetry, yet still affect security practices—from brute-force login attempts, large-scale DDoS activity, and ransomware efforts to the growing reliance on the cloud, lack of security talent, and other concerns.

Recommendations

Organizations are facing a greater attack surface, the growing proliferation and sophistication of attack models, and increasing complexity within the network. Many are struggling to solidify a security vision supported by an effective strategy that uses new technologies, simplifies their architecture and operations, and strengthens their security teams.

This section covers how a threat-centric security model enables defenders to address the full attack continuum, across all attack vectors, and to respond at any time, all the time, in a continuous fashion—before, during, and after an attack.

How Cisco Evaluates the Threat Landscape

Cisco plays a critical role in evaluating threats, given the prevalence of its solutions and the breadth of its security intelligence:

- **16 billion web requests** are inspected every day through Cisco Cloud Web Security
- **93 billion emails** are inspected every day by Cisco's hosted email solution
- **200,000 IP addresses** are evaluated daily
- **400,000 malware samples** are evaluated daily
- **33 million endpoint files** are evaluated every day by FireAMP
- **28 million network connects** are evaluated every day by FireAMP

This activity results in the following threats being detected by Cisco:

- **4.5 billion emails** are blocked every day
- **80 million web requests** are blocked every day
- **6450 endpoint file** detections occur every day in FireAMP
- **3186 endpoint network detections** occur every day in FireAMP
- **50,000 network intrusions** are detected every day

Table of Contents

About This Document

This document contains searchable and shareable content.

Look for this icon to open the find feature in Adobe Acrobat.

Look for these icons to share content.

Recommended Software

Adobe Acrobat Version 7.0 and above

Trust

All organizations should be concerned about finding the right balance of trust, transparency, and privacy because much is at stake.

New Ways of Doing Business, New Security Gaps

Weak links in the technology supply chain are one facet of today's complex cyberthreat and risk landscape.

So, too, is the emergence of the any-to-any infrastructure, where any device in any location may be coming over any instantiation of the network.[1] There is also a growing abundance of Internet-enabled devices—smartphones, tablets, and more—trying to connect to applications that could be running anywhere, including a public software-as-a-service (SaaS) cloud, a private cloud, or a hybrid cloud.[2] Even basic Internet infrastructure services have become a target for hackers who want to take advantage of the reputation, bandwidth, and continuous uptime and availability of web hosting servers, nameservers, and data centers to launch increasingly larger campaigns. (See "Fractures in a Fragile Ecosystem," page 43.)

While trends such as cloud computing and mobility are reducing visibility and increasing security complexity, organizations must still embrace them because they're critical to their competitive advantage and business success. But security gaps are emerging—and widening—as security teams try to align traditional solutions with new and rapidly evolving ways of doing business. Meanwhile, malicious actors are working faster to exploit the gaps that nonintegrated point solutions simply cannot address. And they are succeeding because they have the resources to be more nimble.

Basic Internet infrastructure has become a target for hackers.

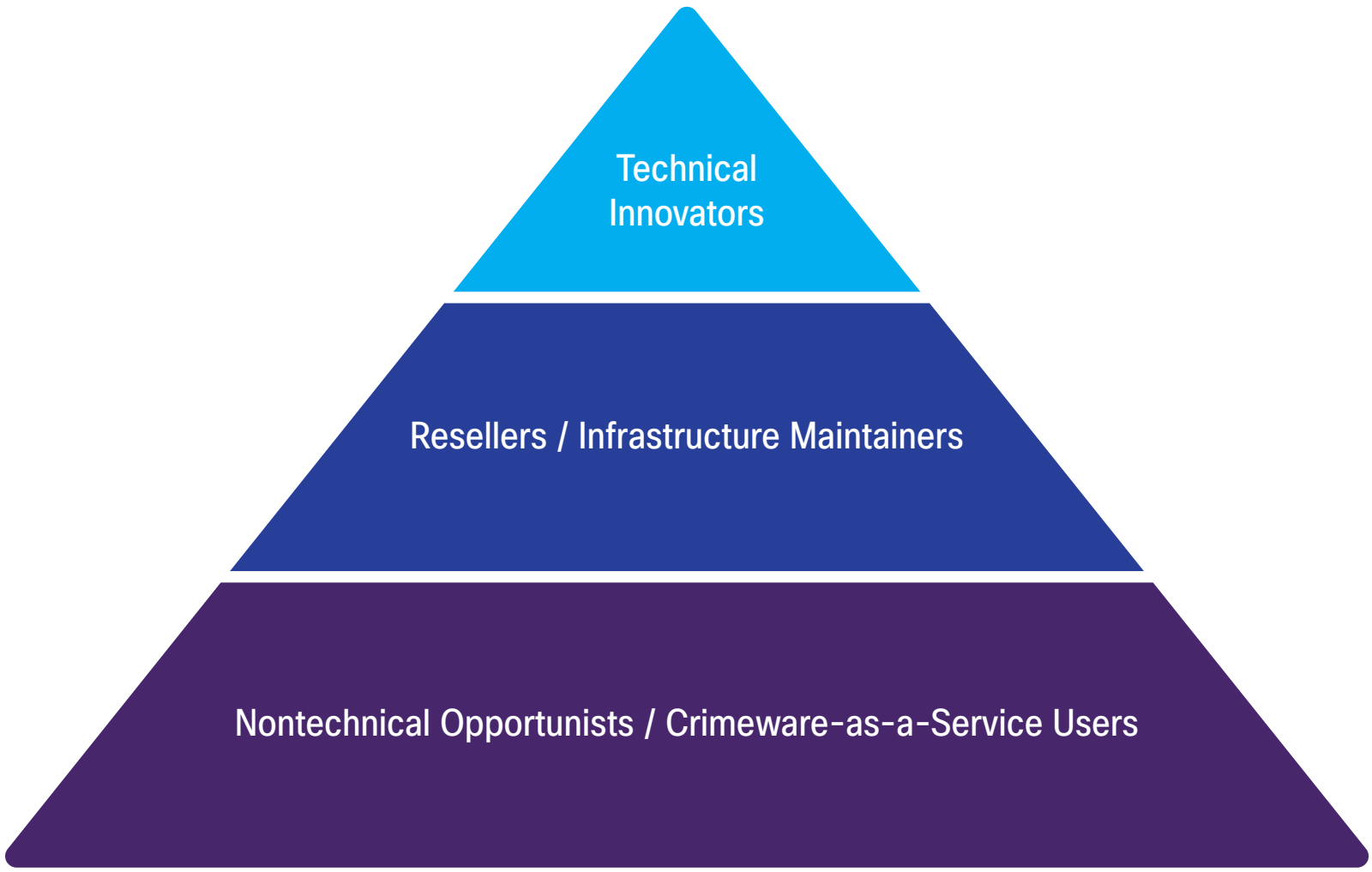
The cybercrime network is expanding, strengthening, and, increasingly, operating like any legitimate, sophisticated business network. Today's cybercriminal hierarchy is like a pyramid (see Figure 1). At the bottom are the nontechnical opportunists and "crimeware-as-a-service" users who want to make money, a statement, or both with their campaigns. In the middle are the resellers and infrastructure maintainers—the "middlemen." At the top are the technical innovators—the major players who law enforcement seeks most, but struggles to find.

Modern cybercriminals usually have clear business objectives when launching their exploits. They know what information they're seeking or what outcomes they want to achieve, and they know the path they need to take to reach these goals. Adversaries will spend significant time researching their targets, often through publicly available information on social networks, and planning their objectives strategically.

Many actors in the so-called "shadow economy" also now send surveillance malware to collect information about an environment, including what security technology is deployed, so they can target their attacks. This pre-exploit reconnaissance is how some malware writers can be sure their malware will work. Once embedded in a network, the advanced malware they design can communicate with command-and-control servers on the outside and spread laterally across infrastructure to carry out its mission—whether it's the theft of vital data or the disruption of critical systems.

FIGURE 1

The Cybercriminal Hierarchy



An Erosion of Trust

Threats designed to take advantage of users' trust in systems, applications, and the people and businesses they know are now permanent fixtures in the cyber world.

Dissect almost any scheme and at the core is some abuse of trust: Malware delivered to users legitimately browsing mainstream websites. Spam emails that appear to be sent by well-known companies but contain links to malicious sites. Third-party mobile applications laced with malware and downloaded from popular online marketplaces. Insiders using information access privileges to steal intellectual property from employers.

There should be an assumption by all users, perhaps, that nothing in the cyber world can or should be trusted. And security professionals may do their organizations a service by not trusting any network traffic[3]—or by not having full faith in the security practices of vendors or the supply chains that provide technology to the enterprise. Yet organizations in the public and private sectors, individual users, and even nation-states still want assurance that they can trust the foundational technologies they rely on every day.

This need for confidence in security has helped to further the advancement of the Common Criteria for Information Technology Security Evaluation (Common Criteria), the language and framework that allows government agencies and other groups to define the requirements that technology products must meet to assure they are trustworthy. Today, 26 countries, including the United States, are participating in the Common Criteria Recognition Arrangement, a multilateral agreement that provides for mutual recognition of evaluated products by participating governments.

However, in 2013, trust, in general, suffered a setback. The catalyst: Edward Snowden. The former U.S. government contractor leaked classified information to *The Guardian*, a U.K. newspaper–information he obtained while working on assignment for the U.S. National Security Agency (NSA).[4]

Snowden's disclosures to the media to date include details about the NSA's electronic surveillance and data collection program, PRISM,[5] as well as a separate NSA-GCHQ[6] program known as MUSCULAR, through which fiber-optic networks carrying traffic from the overseas data centers of major Internet companies were allegedly tapped.[7]

These and other revelations by Snowden about government surveillance practices have eroded trust on many levels: between nation-states, between governments and the private sector, between private citizens and their governments, and between private citizens and organizations in the public and private sector. They also have naturally raised concerns about the presence and potential risks of both unintentional vulnerabilities and intentional "backdoors" in technology products—and whether vendors are doing enough to prevent these weaknesses and protect end users.

Primary Security Challenges for 2014

[As trust erodes—and it becomes harder to define which systems and relationships are trustworthy and which are not—organizations face several key issues that undermine their ability to address security:

1 | Greater attack surface area
2 | Proliferation and sophistication of the attack model
3 | Complexity of threats and solutions]

These combined issues create and exacerbate the security gaps that allow malicious actors to launch exploits faster than organizations can address their security weaknesses.

These threats and risks are examined in more detail on the following pages.

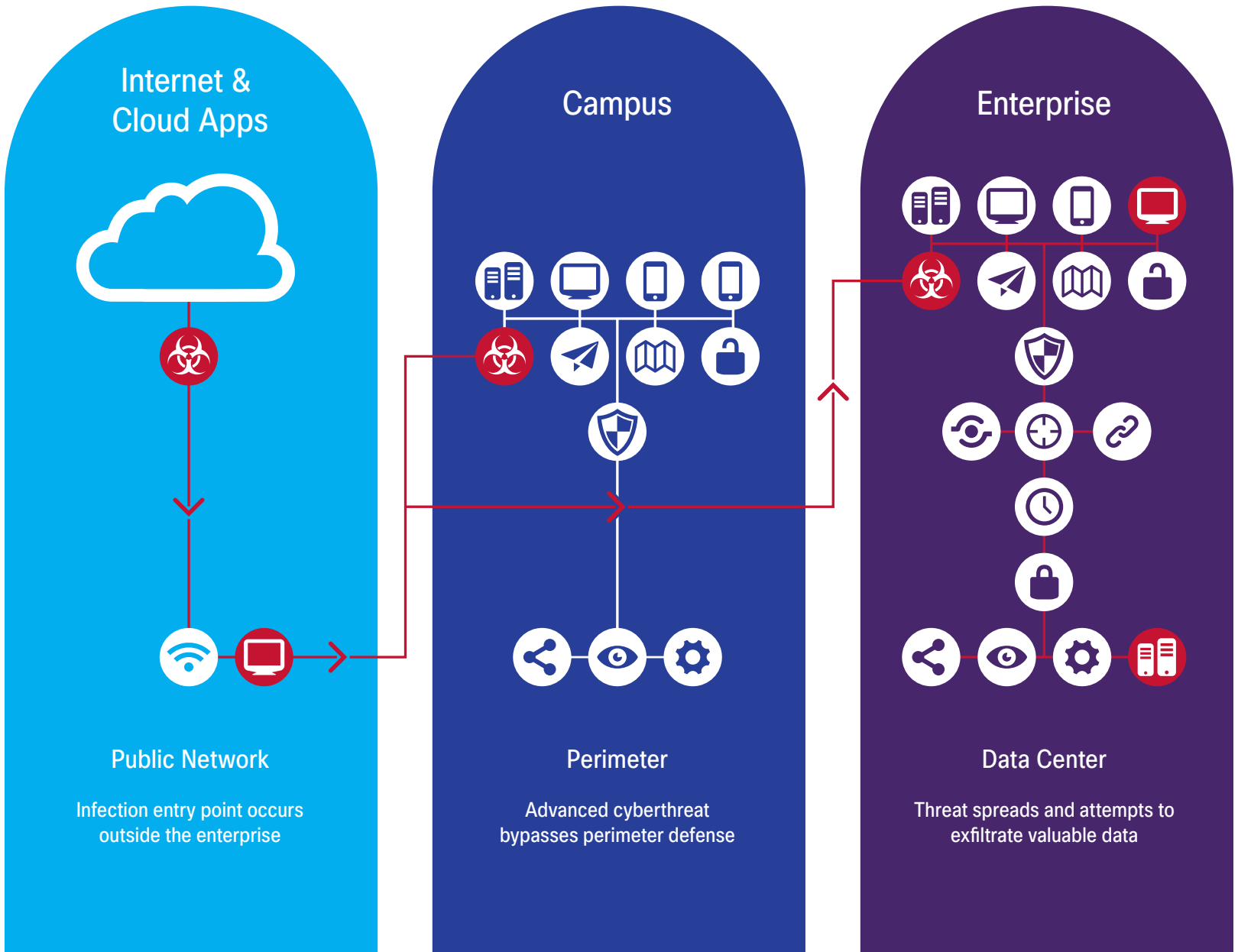
1 | Greater Attack Surface Area

Today's attack surface presents endless possibilities for malicious actors to undermine a large and fragile security ecosystem. The surface has increased exponentially and is still expanding—so many endpoints, so many inroads, so much data that's not under enterprise control.

Data is the prize most adversaries want to reach through their campaigns because it is essentially currency. If data has any "street value"—whether it's a major corporation's intellectual property or an individual's healthcare data—it is desirable and, therefore, at risk. If the value of the target is greater than the risk of compromising it, it will be hacked. Even small organizations are at risk of being hacked. And most organizations, large and small, have already been compromised and don't even know it: 100 percent of business networks analyzed by Cisco have traffic going to websites that host malware.

FIGURE 2

The Anatomy of a Modern Threat



The anatomy of a modern threat, outlined in Figure 2, underscores how the end goal of many cybercrime campaigns is to reach the data center and exfiltrate valuable data. In this example, a malicious action occurs on a device outside the corporate network. It causes an infection, which moves to a campus network. That network serves as a launchpad to the enterprise network, and then the threat makes its way to the treasure trove: the data center.

The end goal of many cybercrime campaigns is to reach the data center and exfiltrate valuable data.

In light of the expanding attack surface area and the targeting of high-value data by hackers, Cisco security experts recommend that enterprises seek to answer two important questions in 2014: "Where does our critical data reside?" and "How can we create a secure environment to protect that data, especially when new business models like cloud computing and mobility leave us with little control over it?"

2 | Proliferation and Sophistication of the Attack Model

Today's threat landscape is nothing like that of just 10 years ago. Simple attacks that caused containable damage have given way to modern cybercrime operations that are sophisticated, well-funded, and capable of causing major disruption to organizations.

Companies have become the focus of targeted attacks. These attacks are very difficult to detect, remain in networks for long periods of time, and amass network resources to launch attacks elsewhere.

To cover the entire attack continuum, organizations need to address a broad range of attack vectors with solutions that operate everywhere the threat can manifest itself: on the network, on endpoints, on mobile devices, and in virtual environments.

"Where does our critical data reside?" and "How can we create a secure environment to protect that data, especially when new business models like cloud computing and mobility leave us with little control over it?"

Cisco security experts

3 | Complexity of Threats and Solutions

Gone are the days when spam blockers and antivirus software could help guard an easily defined network perimeter from most threats. Today's networks go beyond traditional boundaries, and constantly evolve and spawn new attack vectors: mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, home computers, and even vehicles. Point-in-time solutions can't respond to the myriad technologies and strategies in use by malicious actors. This makes monitoring and managing information security even more difficult for security teams.

Organizational vulnerabilities are increasing because enterprises are working through disaggregated point solutions and multiple management platforms. The result: a set of disparate technologies across control points that were never designed to work together. This increases the potential for the compromise of customer information, intellectual property, and other sensitive information, and puts a company's reputation at risk.

A continuous capability that provides the best opportunity to meet the challenges of complex threat environments is needed. Relentless attacks do not occur at a single point in time; they are ongoing. So, too, should be a company's defenses.

With the complexity of threats and corresponding solutions at an all-time high, organizations need to rethink their security strategy. Instead of relying on point solutions, they can minimize complexity by continuously integrating security into the fabric of the network itself, so the network can:

- Continuously monitor and analyze files and identify subsequent malicious behavior whenever it may begin.
- Help organizations scale enforcement, expanding the surface on which networking devices can be placed.
- Accelerate the time to detection because it can see more traffic.
- Give organizations the ability to aggregate unique context awareness that is not possible to obtain by relying on security-specific devices alone.

The shift toward mobility and cloud services is placing a greater security burden on endpoints and mobile devices that in some cases may never even touch the corporate network. The fact is that mobile devices introduce security risk when they are used to access company resources; they easily connect with third-party cloud services and computers with security postures that are potentially unknown and outside of the enterprise's control. In addition, mobile malware is growing rapidly, which further increases risk. Given the lack of even basic visibility, most IT security teams don't have the capability to identify potential threats from these devices.

Advanced approaches such as continuous capability will play a greater role in addressing advanced malware through big data analytics that aggregate data and events across the extended network to provide greater visibility even after a file has moved into the network or between endpoints. This differs from point-in-time endpoint security that scans files at an initial point in time to determine a malware disposition. Advanced malware can evade this scan to establish itself quickly on endpoints and spread throughout networks.

Trustworthy, Transparent Systems

In light of the greater attack surface area, growing proliferation and sophistication of the attack model, and the complexity of threats and solutions, we need to trust the information we consume, along with the systems that deliver it, no matter how we access networked services.

Creating a truly secure network environment becomes even more complex as governments and businesses invest in mobility, collaboration, cloud computing, and other forms of virtualization. These capabilities help to improve resiliency, increase efficiency, and reduce costs, but also can introduce additional risks. The security of the manufacturing processes

creating IT products is also now at risk, with counterfeit and tampered products becoming a growing problem. As a result, today's government and corporate leaders overwhelmingly identify cybersecurity and associated trust issues as top concerns. The question security practitioners should ask is: What would we do differently if we knew a compromise were imminent?

Malicious actors will seek out and exploit any security weakness in the technology supply chain. Vulnerabilities and intentional backdoors in technology products can ultimately provide them with access to the "full house." Backdoors have long been a security issue and should be a concern for organizations, because they exist solely to help facilitate surreptitious or criminal activity.

Developing trustworthy systems means building in security from the ground up, from the beginning to the end of a product's life cycle. The Cisco Secure Development Life cycle (CSDL)[8] prescribes a repeatable and measurable methodology designed to build in product security at the product concept stage, minimize vulnerabilities during development, and increase resiliency of products in the face of an attack.

Malicious actors will seek out and exploit any security weakness in the technology supply chain.

Trustworthy systems provide the foundation for a continuous improvement approach to security that anticipates and preempts new threats. Such infrastructures not only protect critical information, but more importantly, help to avoid interruptions of critical services. Trustworthy products supported by trusted vendors enable their users to minimize the costs and reputation damage stemming from information misappropriation, service outages, and information breaches.

Trustworthy systems, however, should not be confused with immunity from an external attack. IT customers and users have an important role to play in maintaining the effectiveness of trustworthy systems in fending off attempts to corrupt their operations. This includes timely installation of security-focused updates and patches, constant vigilance in recognizing abnormal system behavior, and effective countermeasures against attack.

Top Concerns for 2014 from Today's CISOs

As chief information security officers (CISOs) survey today's threat landscape, they are faced with growing pressure to protect terabytes of data, meet stiff compliance regulations, and evaluate risks of working with third-party vendors—and doing it all with shrinking budgets and lean IT teams. CISOs have more tasks than ever and sophisticated, complex threats to manage. Principal security strategists for Cisco security services, who advise CISOs on security approaches for their organizations, offer this list of the most pressing concerns and challenges for 2014:

Managing Compliance

The most pervasive concern among CISOs may be the need to protect data that resides throughout an increasingly porous network, while expending precious resources on compliance. Compliance alone is not equal to being secure—it is simply a minimum baseline focusing on the needs of a special regulated environment. Security, meanwhile, is an all-encompassing approach that covers all business activities.

Trusting the Cloud

CISOs must make decisions on how to manage information safely with the finite budgets and time they are allotted. For example, the cloud

Continues on next page

Technologies do not stand still, and neither do attackers. Ensuring system trustworthiness needs to cover the full life cycle of a network, from initial design to manufacturing, system integration, daily operation, maintenance and updates, and ultimately, to decommissioning of the solution.

The need for trustworthy systems extends beyond an organization's own network to include those networks with which an organization connects. Cisco Security Research and Operations teams have observed increased use over the past year of "pivoting." The pivoting technique in cybercrime involves the use of a backdoor, vulnerability, or simple exploitation of trust at some point in the attack chain as a springboard to launch a more sophisticated campaign against much bigger targets—such as the network of a major energy firm or a financial institution's data center. Some hackers use the trust that exists between organizations as the base for a pivot, exploiting one trusted business partner to target and exploit another unsuspecting trusted business or governmental partner.

Vigilance is appropriate in the modern threat landscape. Security must adapt to all the transient states that are part of the enterprise IT environment by measurably and objectively validating system trustworthiness, based on independent confirmable data and processes. The most sustainable approach is a dynamic defense tailored to an organization's unique environment, which includes security controls that are evolved constantly so they remain relevant.[9]

Trustworthy systems can exist in this environment, and transparency is essential to building them. "A trustworthy system must be built on a strong foundation: product development practices, a trustworthy supply chain, and an architectural approach consisting of network design, implementation, and policies," says John N. Stewart,

Continued from previous page

has become a cost-effective and agile way to manage ever-growing storehouses of data, but it raises more worries for CISOs. Chief executive officers and boards of directors see the cloud as a panacea for eliminating costly hardware. They want the benefits of offloading data to the cloud, and expect the CISO to make it happen—securely and quickly.

Trusting Vendors

As with the cloud, organizations tap into vendors to provide specialized solutions. The cost model for going with third parties makes sense. However, these vendors are high-value targets for criminals, who know that third-party defenses may not be as strong.

Bouncing Back from Security Breaches

All organizations should assume they've been hacked, or at least agree that it's not a question of if they will be targeted for an attack, but when. Recent hacks such as Operation Night Dragon, the RSA breach, and the Shamoon attack against a large oil and gas company in 2012 are on the minds of many CISOs. (See Cisco's research about the prevalence of malicious activity in corporate networks on page 48.)

senior vice president and chief security officer at Cisco. "But the most important attribute is vendor transparency."

The trade-off for more transparency is less privacy, but finding the right balance can be achieved through cooperation—which leads to greater opportunities to align threat intelligence and security best practices. All organizations should be concerned about finding the right balance of trust, transparency, and privacy because much is at stake.

In the long term, better cybersecurity can be achieved for all users, and the full potential of the emerging Internet of Everything[10] economy can be realized. But meeting these goals will hinge on effective privacy policies and robust network defenses that intelligently distribute the burden of security across the endpoints and the network. In the short term, and closer to home perhaps, is the need for any modern business to use the best methods and information available to help protect its most valuable assets, and ensure it is not a direct contributor to broader cybersecurity challenges.

Today's organizations must consider what impact their security practices may have on the larger and increasingly complex and interconnected cybersecurity ecosystem. Not taking this "big picture" view could result in an organization earning a bad reputation score, which means no leading security provider will allow users to access their site. Being blacklisted is not easy for a business to come back from—and some may never fully recover.

To learn more about Cisco Trustworthy Systems practices, please visit www.cisco.com/go/trustworthy.

Threat Intelligence

Using the largest set of detection telemetry with which to work, Cisco and Sourcefire together have analyzed and assembled security insights from the past year.

Threat Alerts on the Rise

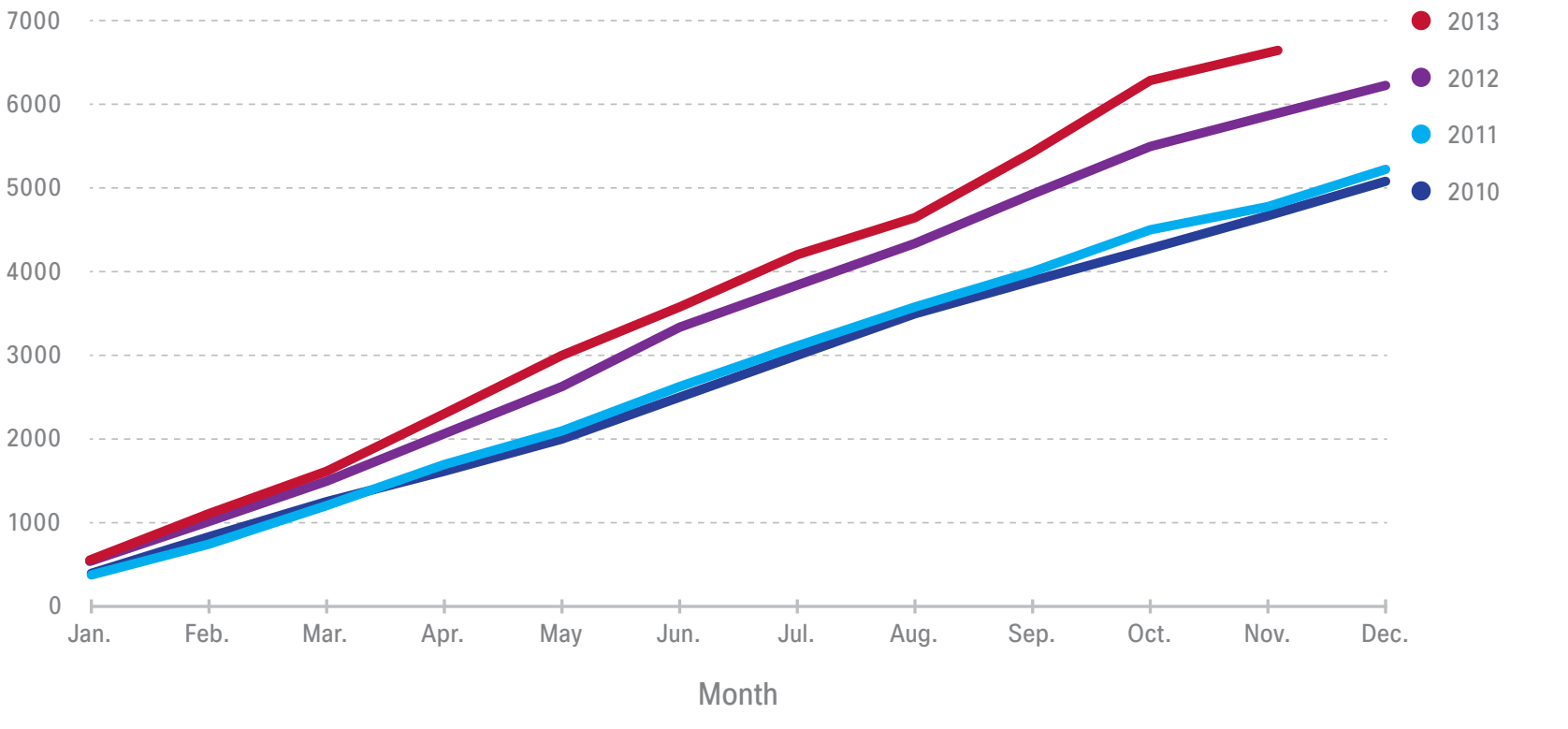
Vulnerabilities and threats reported by Cisco IntelliShield® showed steady growth in 2013: as of October 2013, cumulative annual alert totals increased 14 percent year-over-year from 2012 (Figure 3).

Alerts in October 2013 were at their highest level since IntelliShield began recording them in May 2000.

Also notable is the significant increase in new alerts as opposed to updated alerts, as tracked by IntelliShield (Figure 4). Technology vendors and researchers are finding an increasing number of new vulnerabilities (Figure 5), the discoveries being a result of the greater emphasis on highly secure development life cycle use, as well as improvements in the security of their own products. The higher number of new vulnerabilities may also be a sign that vendors are examining their product code and fixing vulnerabilities before products are released and their vulnerabilities exploited.

FIGURE 3

Cumulative Annual Alert Totals, 2010–2013



More attention to secure software development can help build trust in vendor solutions. A secure development life cycle not only mitigates the risk of vulnerabilities and allows vendors to detect potential defects early in development, but also tells purchasers that they can rely on these solutions.

FIGURE 4

New and Updated Alerts, 2013

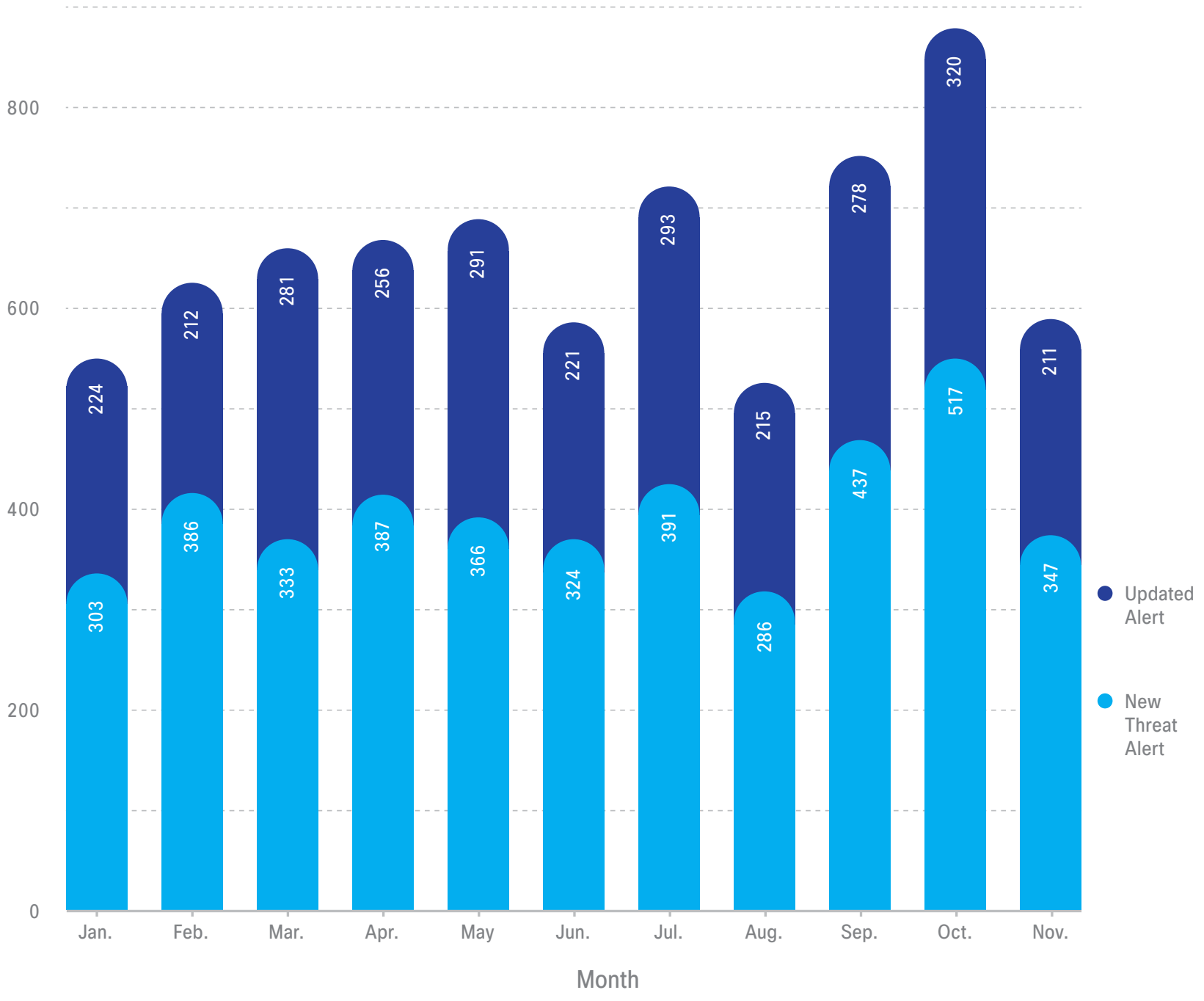


FIGURE 5

Common Threat Categories Tracked by Cisco IntelliShield

NOTE: These CWE (Common Weakness Enumeration) threat categories, as defined by the National Vulnerability Database (https://nvd.nist.gov/cwe.cfm), tie in to the methods malicious actors use to attack networks.

1 CWE-119: Buffer Errors

2 Other Intellishield Alerts (Activity, Issues, CRR, AMB)

3 CWE-399: Resource Management Errors

4 CWE-20: Input Validation

5 CWE-264: Permissions, Privileges, and Access Control

6 CWE-200: Information Leak/Disclosure

7 CWE-79: Cross-Site Scripting (XSS)

8 CWE-94: Code Injection

9 CWE: Design Error

CWE-310: Cryptographic Issues

CWE-287: Authentication Issues

CWE-352: Cross-Site Request Forgery (CSRF)

CWE-22: Path Traversal

CWE-78: OS Command Injections

CWE-89: SQL Injection

CWE-362: Race Conditions

CWE-255 Credentials Management

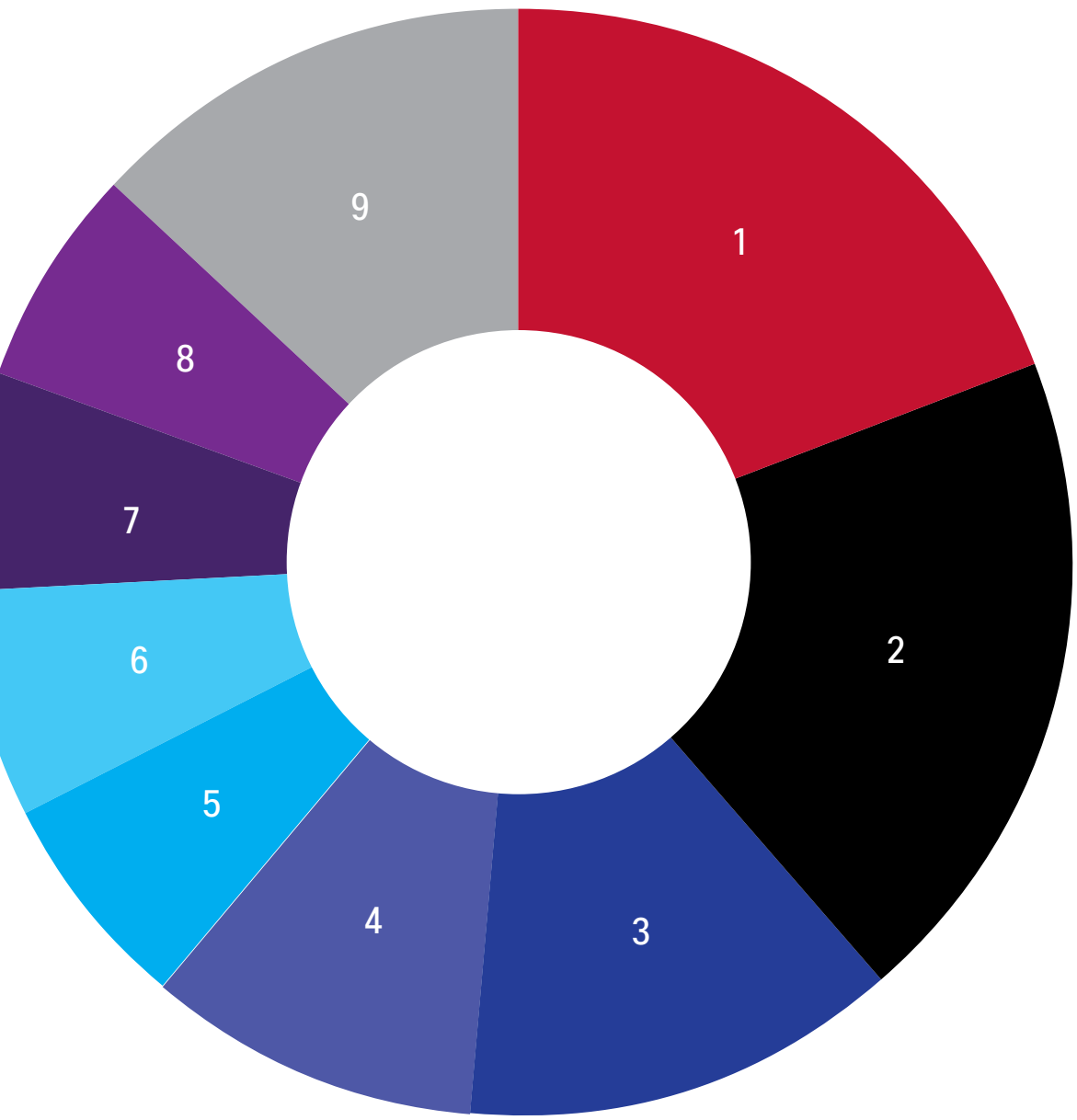
CWE-59: Link Following

CWE-16: Configuration

CWE: Insufficient Information

CWE: Other

CWE-189: Numeric Errors



Spam Volume Is Down, but Malicious Spam Is Still a Threat

Spam volume was on a downward trend worldwide in 2013. However, while the overall volume may have decreased, the proportion of maliciously intended spam remained constant.

Spammers use speed as a tool to abuse email users' trust, delivering massive amounts of spam when news events or trends lower recipients' resistance to spam scams.

In the aftermath of the Boston Marathon bombing on April 15, 2013, two large-scale spam campaigns commenced—one on April 16 and another on April 17—designed to attract email users hungry for news of the event's impact. Cisco researchers first detected the registration of hundreds of bombing-related domain names just hours after the Boston Marathon attacks occurred.[11]

Spammers prey on people's desire for more information in the wake of a major event.

Both spam campaigns carried subject lines about supposed news bulletins relating to the bombings, while the messages contained links that claimed to lead to videos of the bomb explosions or news from reputable media sources. The links directed recipients to webpages that included links to real news stories or videos—but also malicious iframes designed to infect the visitors' computers. At its peak, spam related to the Boston Marathon bombing made up 40 percent of all spam messages delivered worldwide on April 17, 2013.

Figure 6 shows one of the botnet's spam campaigns masquerading as a message from CNN.[12] Figure 7 shows the source HTML for a Boston Marathon bombing spam message. The final iframe (obfuscated) is for a malicious website.[13]

Because breaking news spam is so immediate, email users are more likely to believe the spam messages are legitimate. Spammers prey on people's desire for more information in the wake of a major event. When spammers give online users what they want, it's much easier to trick them into a desired action, such as clicking an infected link. It's also much easier to prevent them from suspecting that something is wrong with the message.

FIGURE 6

Boston Marathon Spam

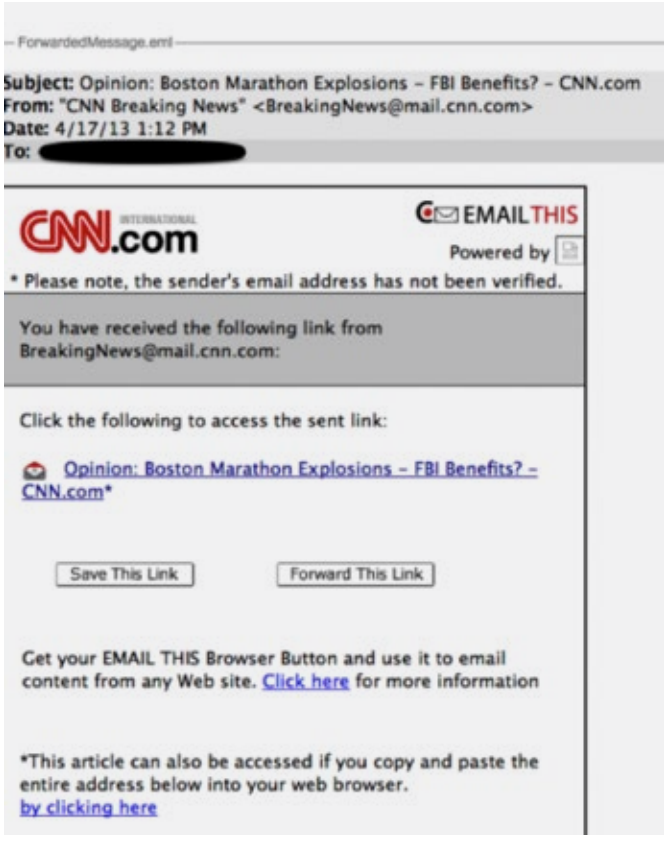
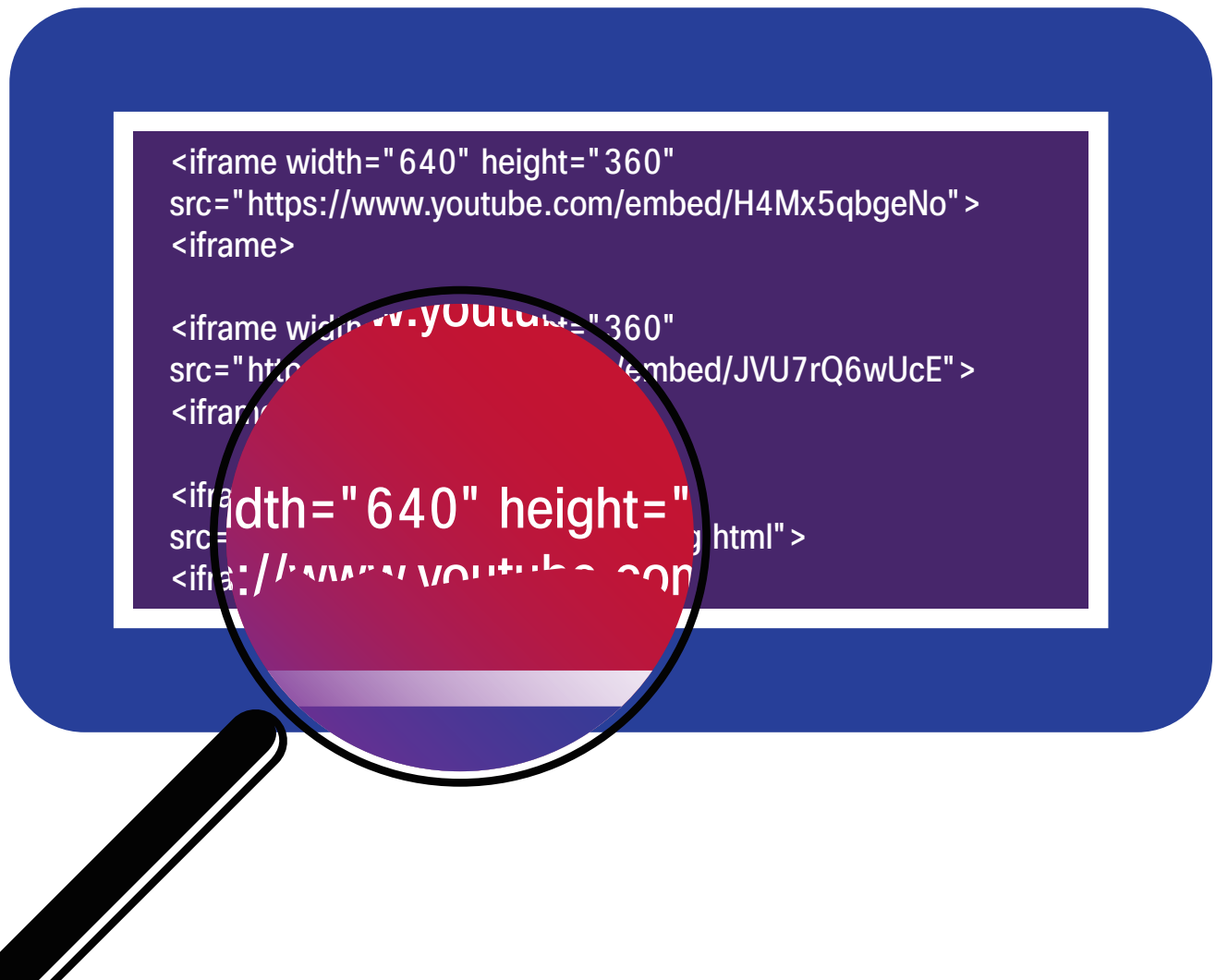


FIGURE 7

Source HTML for a Boston Marathon Bombing Spam Message



Spam by the Numbers

Global spam volume is dropping according to data collected by Cisco Threat Research Analysis and Communications (TRAC)/SIO (Figure 8), although trends vary by country (Figure 9).

FIGURE 8

Global Spam Volume, 2013

Source: Cisco TRAC/SIO

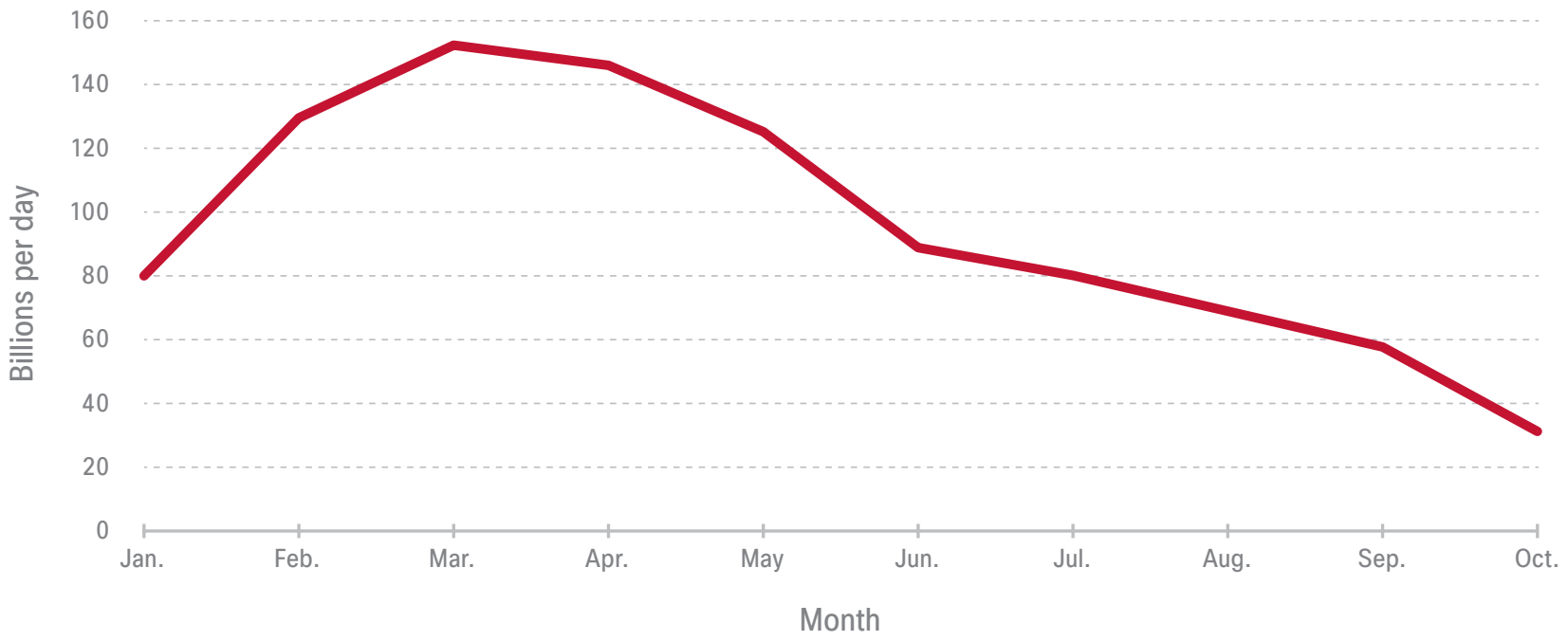


FIGURE 9

Volume Trends, 2013

Source: Cisco TRAC/SIO

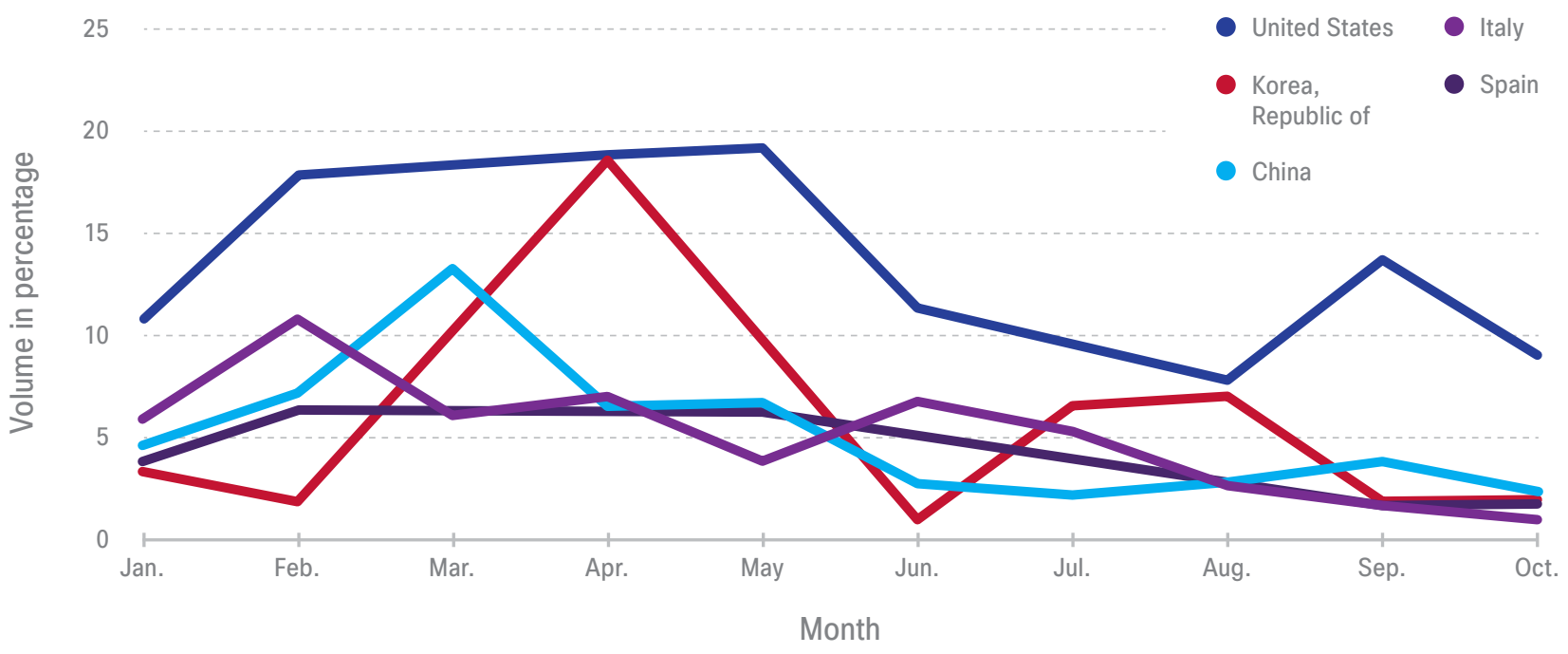


FIGURE 10

Top Themes for Spam Messages Worldwide

1.
Bank Deposit/Payment Notifications

Notifications for deposits, transfers, payments, returned check, fraud alert.

2.
Online Product Purchase

Product order confirmation, request purchase order, quote, trial.

3.
Attached Photo

Malicious attached photos.

4.
Shipping Notices

Invoices, delivery or pickup, tracking.

5.
Online Dating

Online dating sites.

6.
Taxes

Tax documents, refunds, reports, debt information, online tax filings.

7.
Facebook

Account status, updates, notifications, security software.

8.
Gift Card or Voucher

Alerts from a variety of stores (Apple was the most popular).

9.
PayPal

Account update, confirmation, payment notification, payment dispute.

Web Exploits: Java Leads the Pack

Of all the web-based threats that undermine security, vulnerabilities in the Java programming language continue to be the most frequently exploited target by online criminals, according to Cisco data.

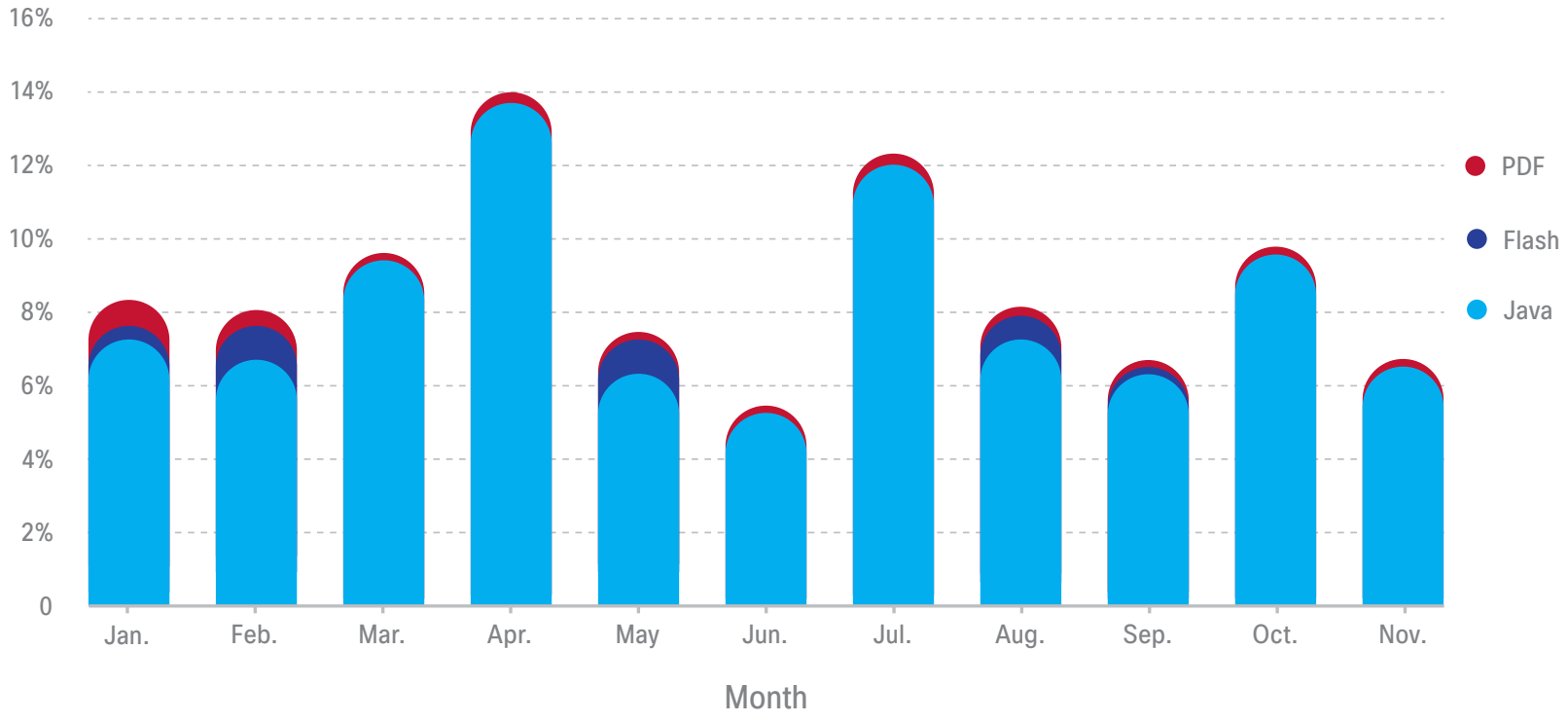
Java exploits far outstrip those detected in Flash or Adobe PDF documents, which are also popular vectors for criminal activity (Figure 11).

Data from Sourcefire, now part of Cisco, also shows that Java exploits make up the vast majority (91 percent) of indicators of compromise (IoCs) that are monitored by Sourcefire's FireAMP solution for advanced malware analysis and protection (Figure 12). FireAMP detects live compromises on endpoints, and then records the type of software that caused each compromise.

FIGURE 11

Malicious Attacks Generated through PDF, Flash, and Java 2013

Source: Cisco Cloud Web Security reports



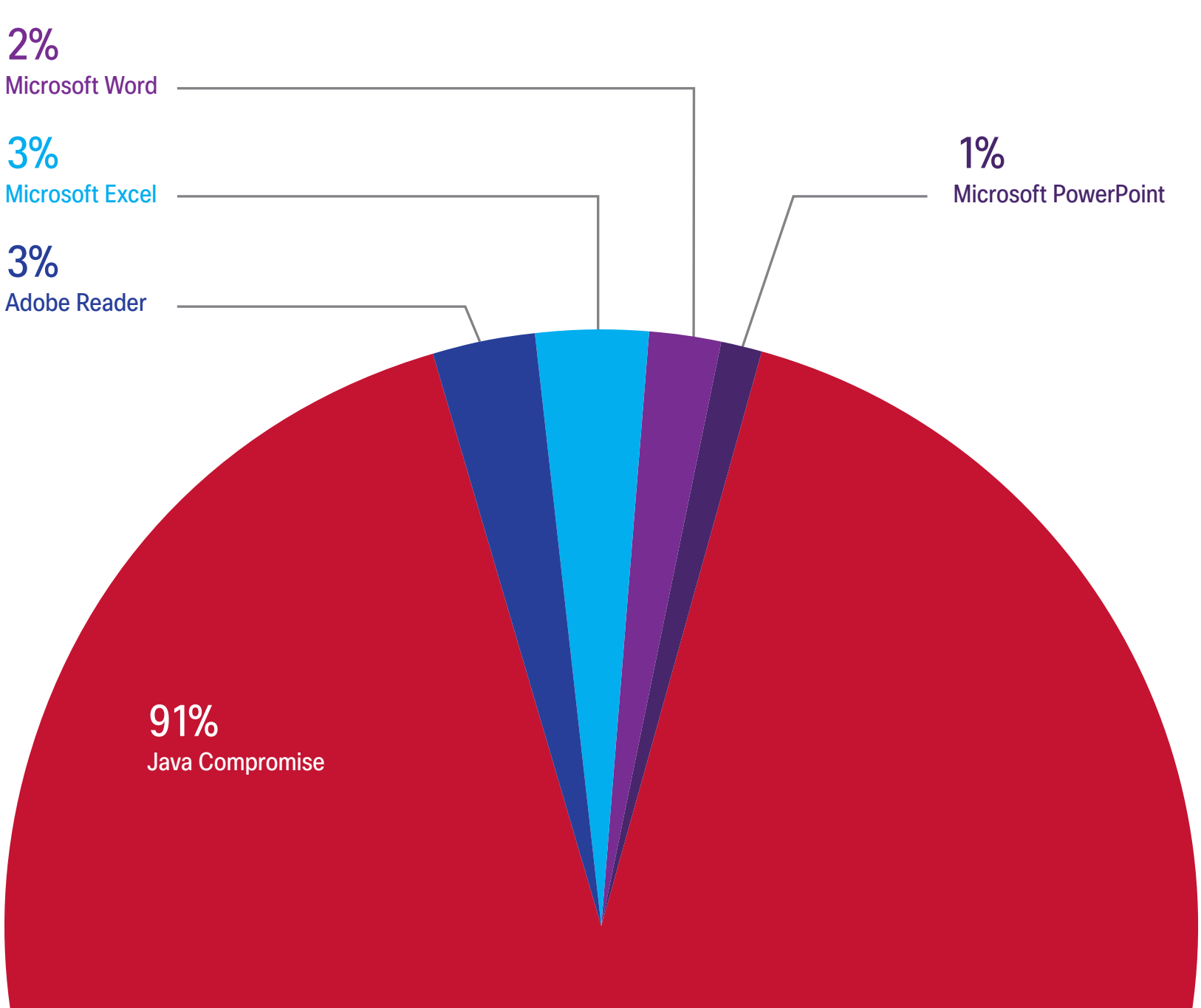
For threats such as Java exploits, the most significant issues facing security practitioners are how malware enters their network environment and where they should focus their efforts to minimize infection. Individual actions may not appear malicious, but following a chain of events can shed light on the malware story. Chaining of events is the ability to conduct a retrospective analysis on data that connects the path taken by malicious actors to bypass perimeter security and infiltrate the network.

By themselves, IoCs may demonstrate that going to a given website is safe. In turn, the launch of Java may be a safe action, as may be the launch of an executable file. However, an organization is at risk if a user visits a website with an iframe injection, which then launches Java; Java then downloads an executable file, and that file runs malicious actions.

FIGURE 12

Indicators of Compromise, by Type

Source: Sourcefire (FireAMP solution)



The ubiquity of Java keeps it high on the list of favored tools for criminals, which makes Java compromises by far the most malicious "chain of events" activity in 2013. As Java's "About" webpage explains, 97 percent of enterprise desktops run Java, as do 89 percent of desktop computers overall in the United States.[14]

Java provides an attack surface that is too big for criminals to ignore. They tend to build solutions that run exploits in order—for instance, they first attempt to breach a network or steal data using the easiest or best-known vulnerability before moving on to other methods. In most cases, Java is the exploit that criminals choose first, since it delivers the best return on investment.

Mitigating the Java Problem

Although Java-based exploits are commonplace, and vulnerabilities are difficult to eliminate, there are methods for reducing their impact:

- Where practical, disabling Java in browsers network-wide can prevent these exploits from being launched.
- Telemetry tools like Cisco NetFlow, built in to many security solutions, can monitor Java-associated traffic, giving security professionals a better understanding of the sources of threats.
- Comprehensive patch management can close many security holes.
- Endpoint monitoring and analysis tools that continue to track and analyze files after they enter the network can retrospectively detect and stop threats that pass through as safe but later exhibit malicious behavior.
- A prioritized list of potentially compromised devices can be generated by using IoCs to correlate malware intelligence (even seemingly benign events) and to identify a zero-day infection without existing antivirus signatures.

Upgrading to the latest version of Java will also help sidestep vulnerabilities. According to research from Cisco TRAC/SIO, 90 percent of Cisco customers use a version of the Java 7 Runtime Environment, the most current version of the program. This is good from a security standpoint, since this version is likely to offer greater protection against vulnerabilities.

However, Cisco TRAC/SIO research also shows that 76 percent of enterprises using Cisco solutions are also using the Java 6 Runtime Environment, in addition to Java 7. Java 6 is a previous version that has reached its end of life and is no longer supported. Enterprises often use both versions of the Java Runtime Environment because different applications may rely on different versions to execute Java code. However, with more than three-fourths of the enterprises surveyed by Cisco using an end-of-life solution with vulnerabilities that may never be patched publicly, criminals have ample opportunity to exploit weaknesses.

In 2013, Java web malware encounters peaked in April, at 14 percent of all web malware encountered. These encounters dropped to their lowest point in May and June 2013, at approximately 6 percent and 5 percent of all web malware encounters, respectively (Figure 13).

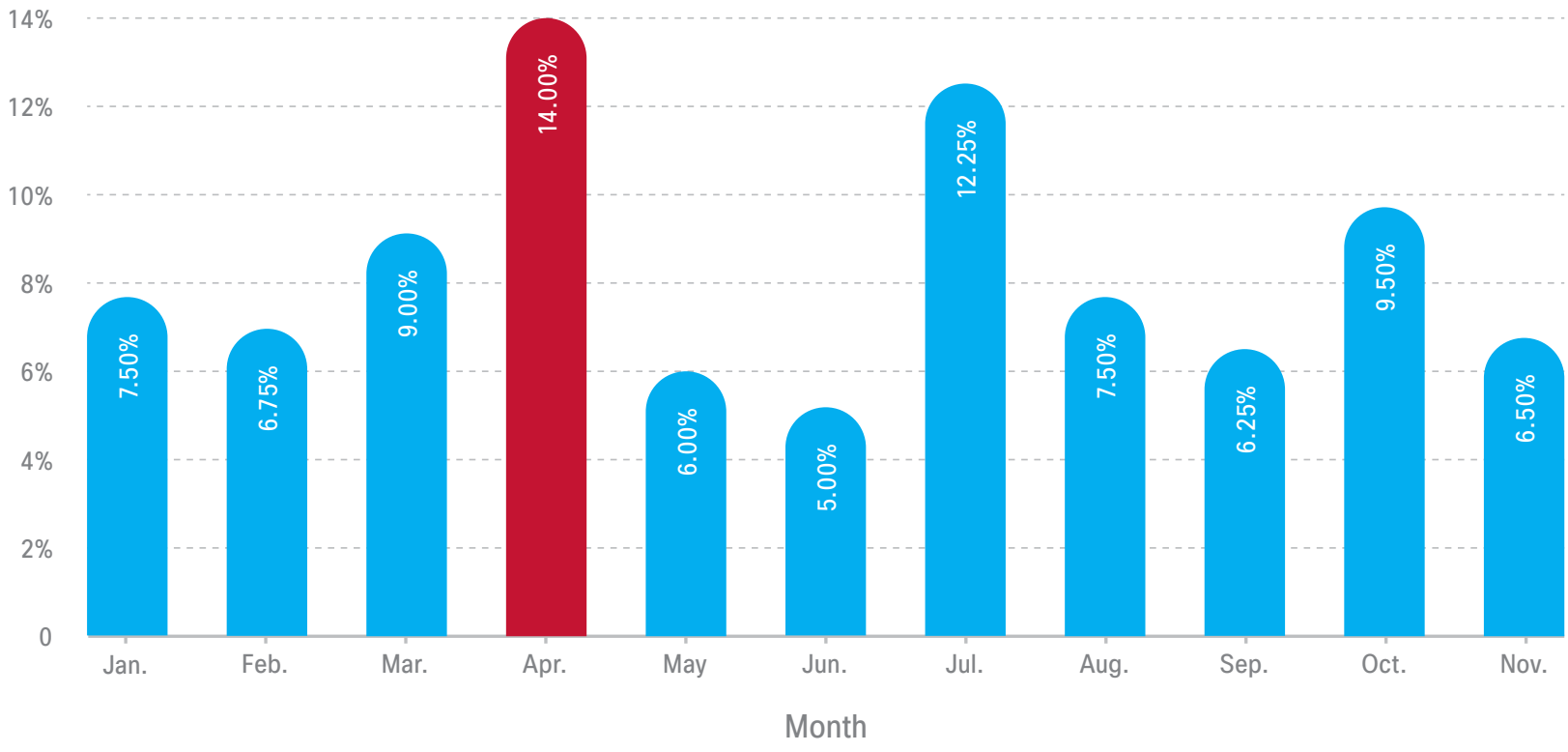
(Earlier this year, Oracle announced that it would no longer post Java SE 6 updates to its public download site, although existing Java SE 6 updates will be available in the Java Archive on the Oracle Technology Network.)

If security professionals who have limited time to fight web exploits decide to focus most of their attention on Java, they'll be putting their resources in the right place.

FIGURE 13

Java Web Malware Encounters, 2013

Source: Cisco TRAC/SIO



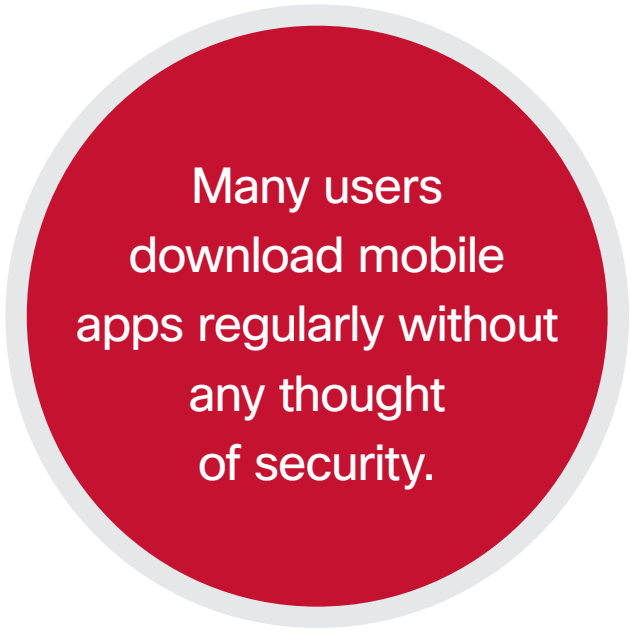
BYOD and Mobility: Device Maturation Benefitting Cybercrime

Cybercriminals and their targets share a common challenge: both are trying to figure out how best to use the bring-your-own-device (BYOD) and mobility trends for business advantage.

Two things appear to be helping criminals gain an edge. First is the maturation of mobile platforms. Cisco security experts note that the more smartphones, tablets, and other devices perform like traditional desktop and laptop computers, the easier it is to design malware for them.

Second is the growing using of mobile apps. When users download mobile apps, they're essentially putting a lightweight client on the endpoint–and downloading code. Another challenge: Many users download mobile apps regularly without any thought of security.

Meanwhile, today's security teams are grappling with the "any-to-any problem": how to secure any user, on any device, located anywhere, accessing any application or resource.[15] The BYOD trend only complicates these efforts. It's difficult to manage all of these types of equipment, especially with a limited IT budget. In a BYOD environment, the CISO needs to be especially certain that the data room is tightly controlled.



Mobility offers new ways for users and data to be compromised. Cisco researchers have observed actors using wireless channels to eavesdrop and gain access to data being exchanged through those channels. Mobility also presents a range of security issues for organizations, including the loss of intellectual property and other sensitive data if an employee's device is lost or stolen and not secured.

Instituting a formal program for managing mobile devices to help ensure that any device is secure before it can access the network is one solution to improve security for the enterprise, according to Cisco experts. At the very least, a personal identification number (PIN) lock should be required for user authentication and the security team should be able to turn off or wipe clean the device remotely if it is lost or stolen.

Mobile Malware Trends: 2013

The following research on mobile malware trends during 2013 was conducted by Cisco TRAC/SIO and by Sourcefire, now part of Cisco.

Mobile malware that targets specific devices made up just 1.2 percent of all web malware encounters in 2013. Although not a significant percentage, it is still worth noting because mobile malware is clearly an emerging—and logical—area of exploration for malware developers.

Mobile malware that targets specific devices made up just 1.2 percent of all web malware encounters in 2013.

According to Cisco TRAC/SIO researchers, when mobile malware is intended to compromise a device, 99 percent of all encounters target Android devices. Trojans targeting Java Micro Edition (J2ME)-capable devices held the second spot in 2013, with 0.84 percent of all mobile malware encounters.

Not all mobile malware is designed to target specific devices, however. Many encounters involve phishing, likejacking, or other social engineering ruses, or forcible redirects to websites other than expected. An analysis of user agents by Cisco TRAC/SIO reveals that Android users, at 71 percent, have the highest encounter rates with all forms of web-delivered malware, followed by Apple iPhone users with 14 percent of all web malware encounters (Figure 14).

Cisco TRAC/SIO researchers also reported evidence of efforts to monetize Android compromises during 2013, including launches of adware and small and medium-size enterprise (SME)-related spyware.

At 43.8 percent, Andr/Qdplugin-A was the most frequently encountered mobile malware, according to Cisco TRAC/SIO research. Typical encounters were through repackaged copies of legitimate apps distributed through unofficial marketplaces (Figure 15).

FIGURE 14

Web Malware Encounters by Mobile Device

Source: Cisco Cloud Web Security reports

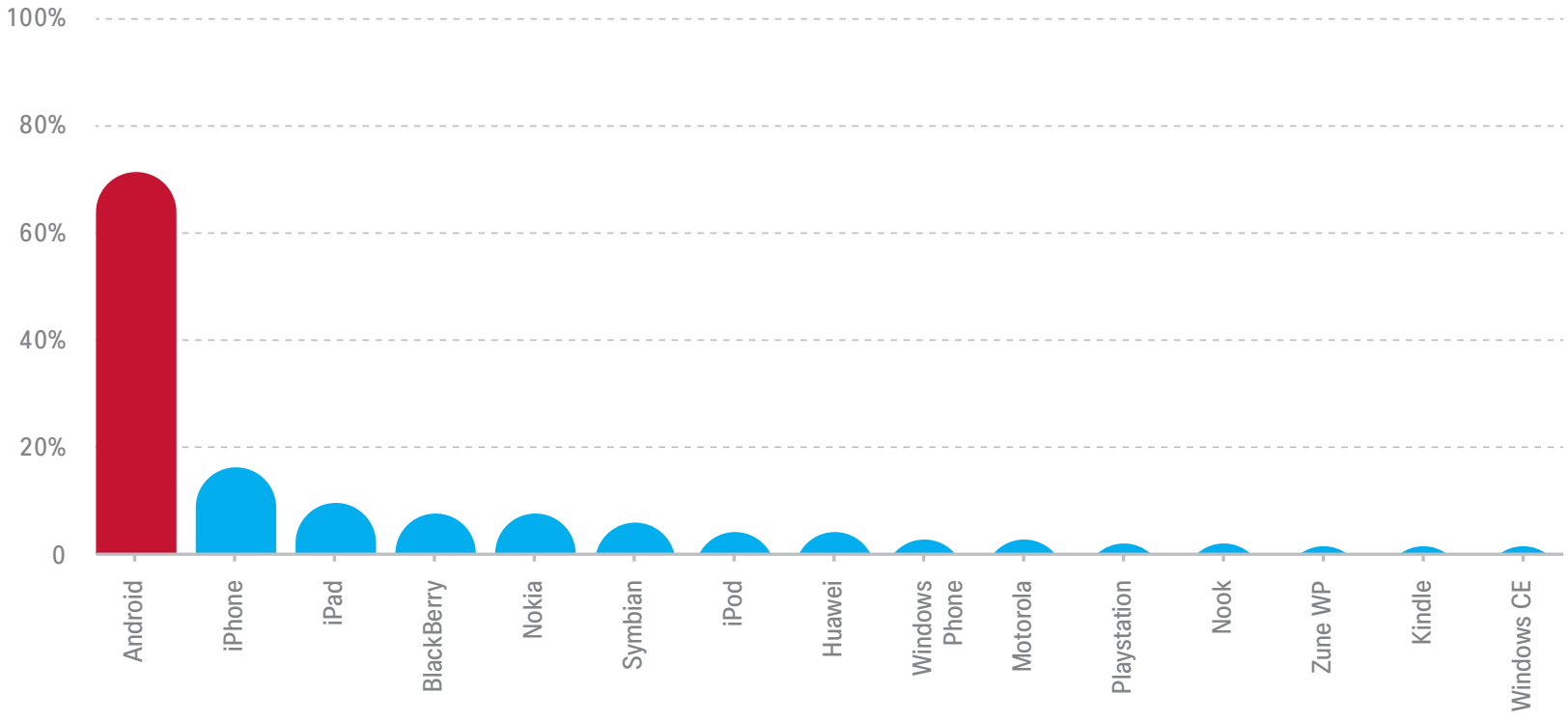


FIGURE 15

Top 10 Mobile Malware Encounters, 2013

Source: Cisco Cloud Web Security reports

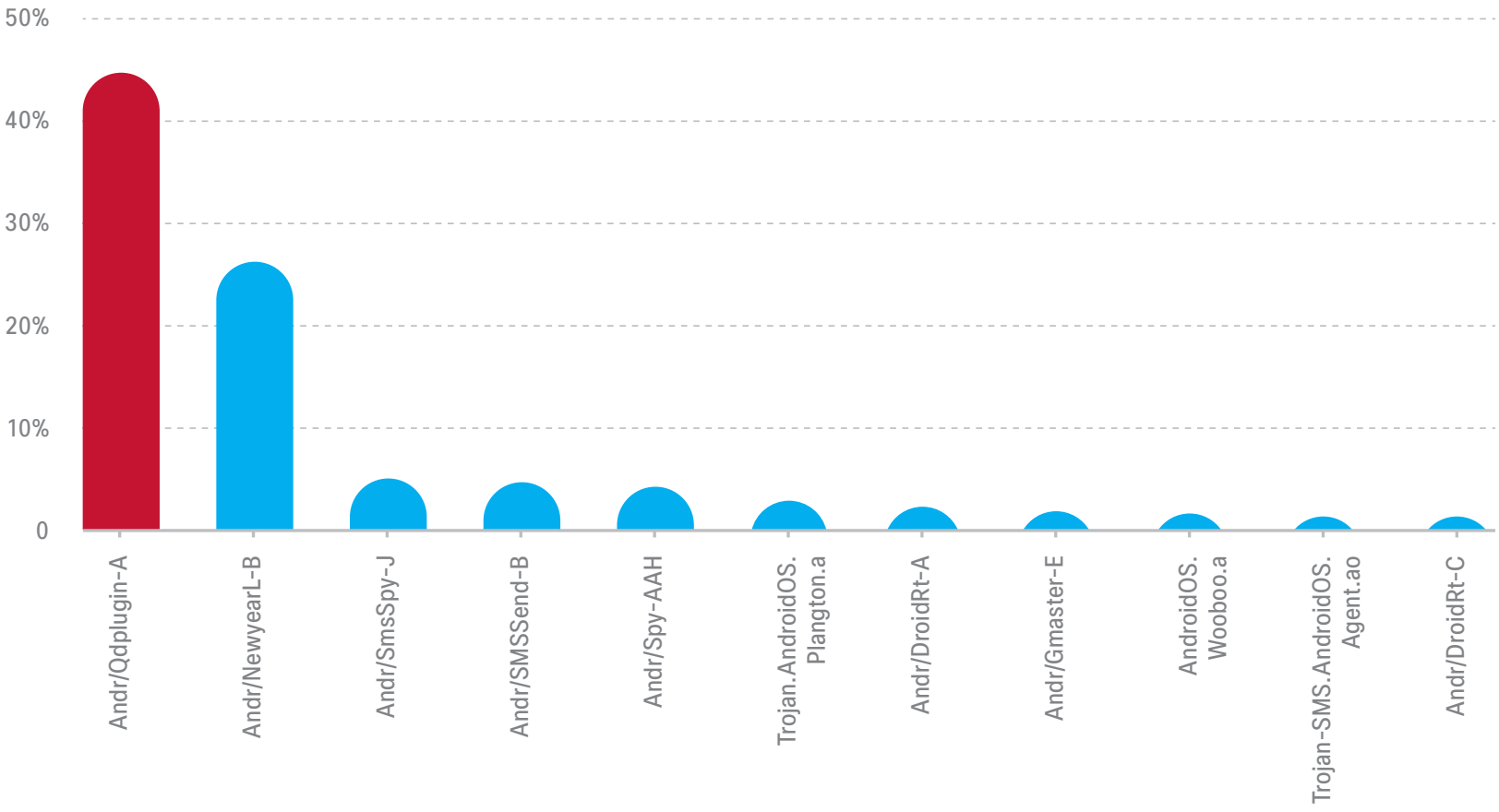
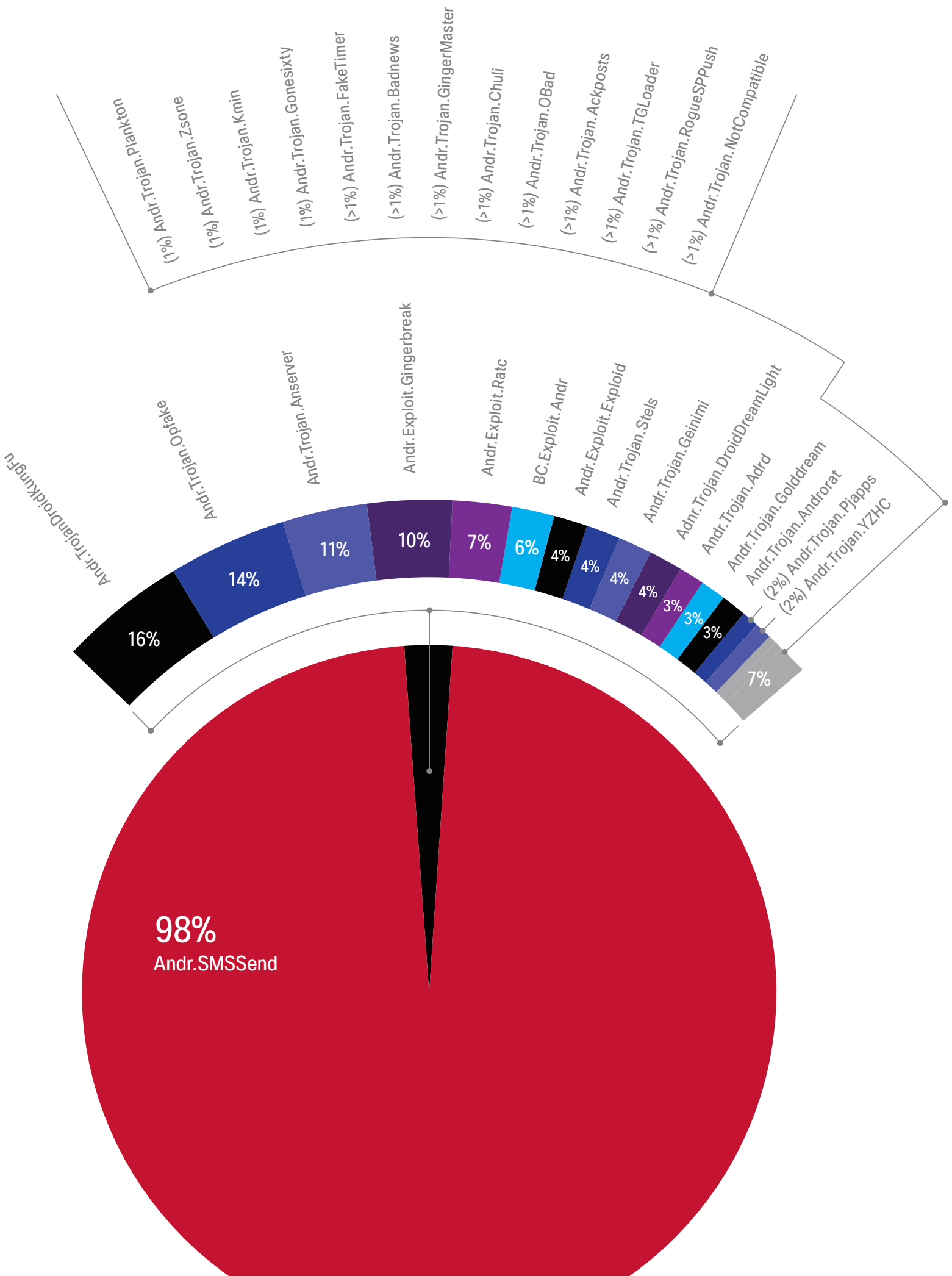


FIGURE 16

Top Android Malware Families Observed in 2013

NOTE: SMSSend accounts for 98 percent of all Android malware; the remaining 2 percent is proportionally shown.
Source: Sourcefire



Targeted Attacks: The Challenge of Dislodging Persistent and Pervasive "Visitors"

Odds are high that targeted attacks have already infiltrated your networks.

And when they do lodge themselves inside a network, they tend to stay around, stealthily stealing data or using network resources to "pivot" and then attack other entities (for more on pivoting, see page 18). The damage goes beyond the theft of data or business disruption: trust between partners and customers can evaporate if these attacks aren't dislodged from networks in a timely manner.

Targeted attacks threaten intellectual property, customer data, and sensitive government information. Their creators use sophisticated tools that circumvent an organization's security infrastructure. Criminals go to great lengths to make sure these breaches go undetected, using methods that result in nearly imperceptible "indicators of compromise" or IoCs. Their methodical approach to gain entry into networks and carry out their mission involves an "attack chain"—the chain of events that leads up to and through the phases of an attack.

Once these targeted attacks find a place in the network to hide, they efficiently carry out their tasks, and usually conduct them without being noticed.

FIGURE 17

The Attack Chain

To understand today's array of threats and effectively defend the network, IT security professionals need to think like attackers. With a deeper understanding of the methodical approach that malicious actors use to execute their mission, organizations can identify ways to strengthen their defenses. The attack chain, a simplified version of the "cyber kill chain," describes the events that lead to and through the phases of an attack.

1. Survey

Obtain a full picture of an environment: network, endpoint, mobile, and virtual, including the technologies deployed to secure the environment.

2. Write

Create targeted, context-aware malware.

3. Test

Ensure the malware works as intended, specifically so it can evade security tools in place.

4. Execute

Navigate through the extended network–being environmentally aware, evading detection, and moving laterally until reaching the target.

5. Accomplish the Mission

Gather data, create disruption, or cause destruction.

Malware Snapshot: Trends Observed in 2013

Cisco security experts perform ongoing research and analysis of malware traffic and other discovered threats, which can provide insights on possible future criminal behavior and aid in the detection of threats.

FIGURE 18

Top Malware Categories

This figure displays the top malware categories. Trojans are the most common malware, followed by adware. Source: Sourcefire (ClamAV and FireAMP solutions)

FIGURE 19

Top Windows Malware Families

This figure shows the top malware families for Windows. The largest, Trojan.Onlinegames, mainly comprises password stealers. It is detected by Sourcefire's ClamAV antivirus solution. Source: Sourcefire (ClamAV solution)

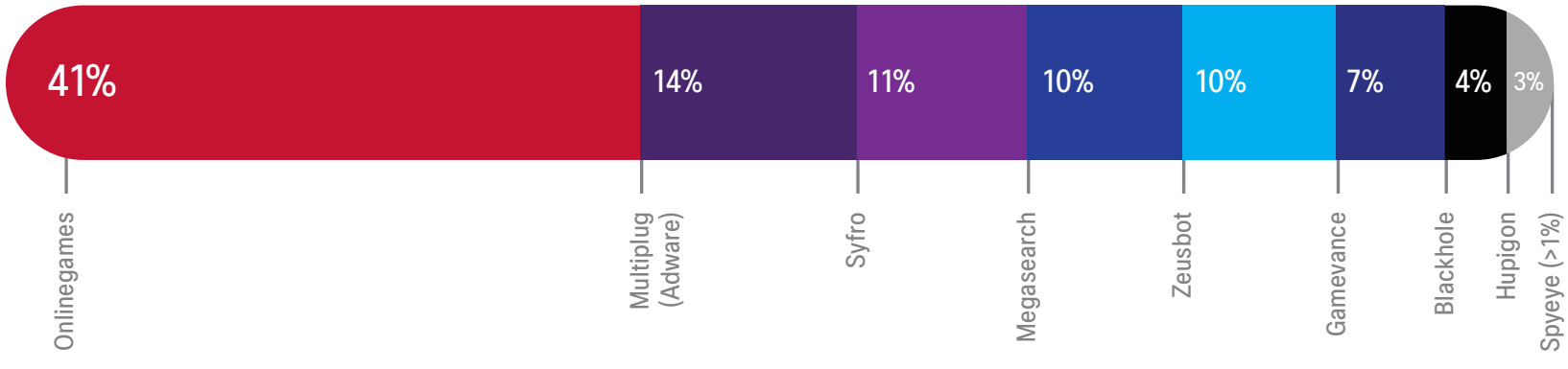


FIGURE 20

Top 10 Categories of Web Malware Hosts, 2013

This figure shows the most frequent malware hosts, according to Cisco TRAC/SIO research.
Source: Cisco Cloud Web Security reports

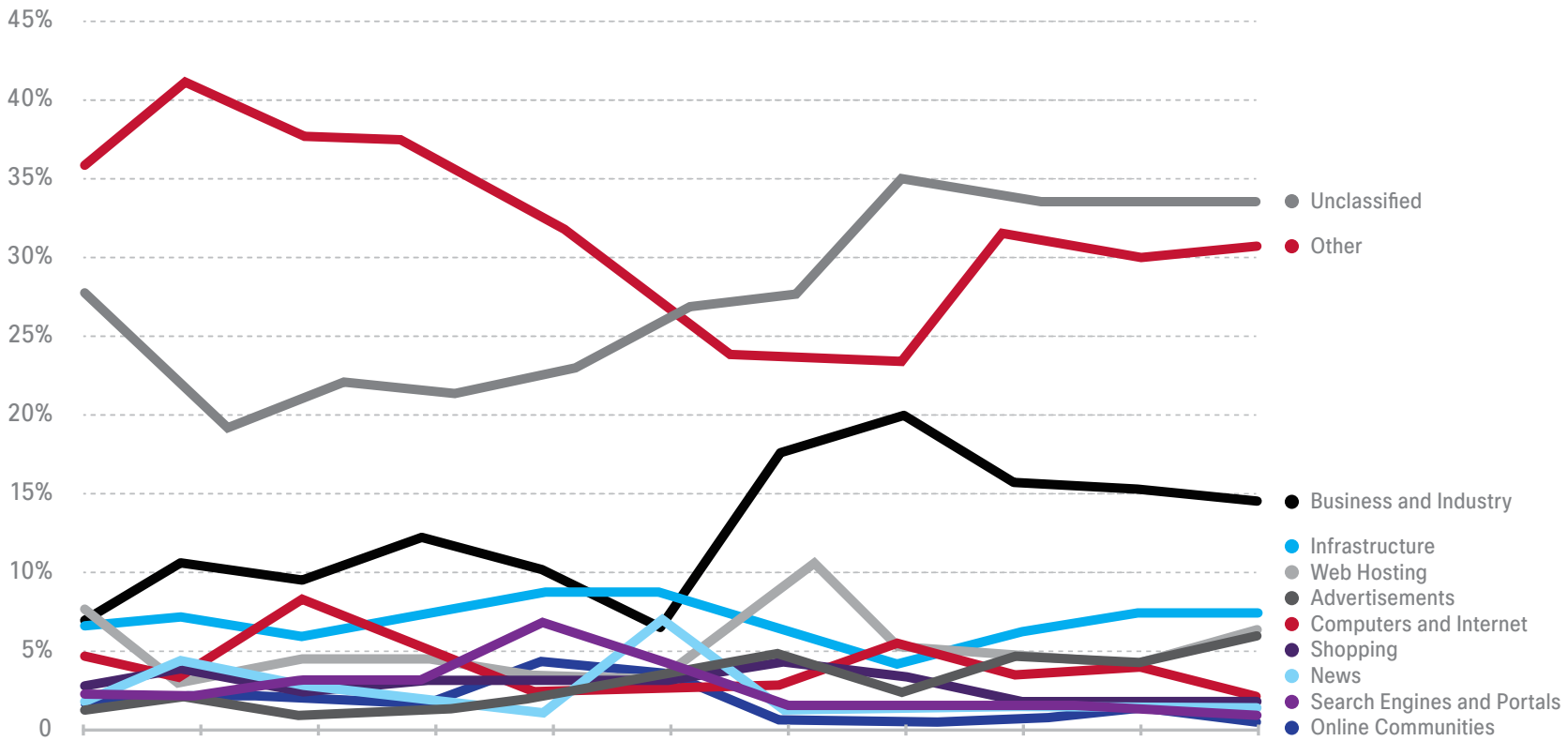
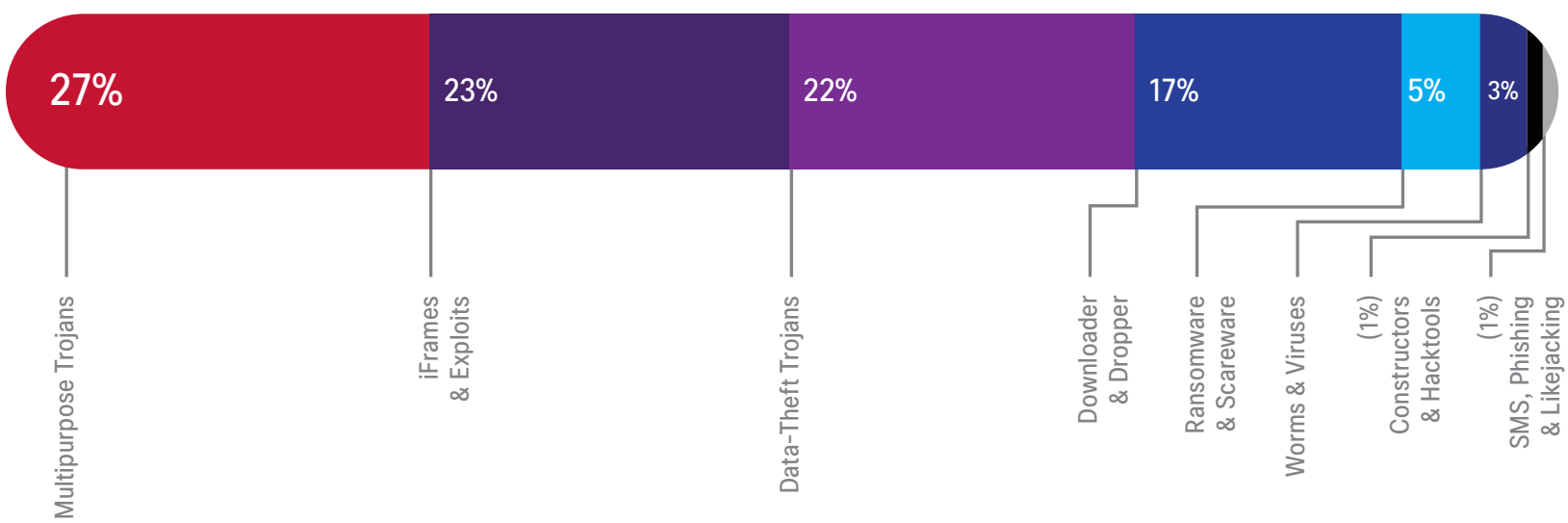


FIGURE 21

Malware Categories, by Percentage of Total Encounters, 2013

Source: Cisco TRAC/SIO



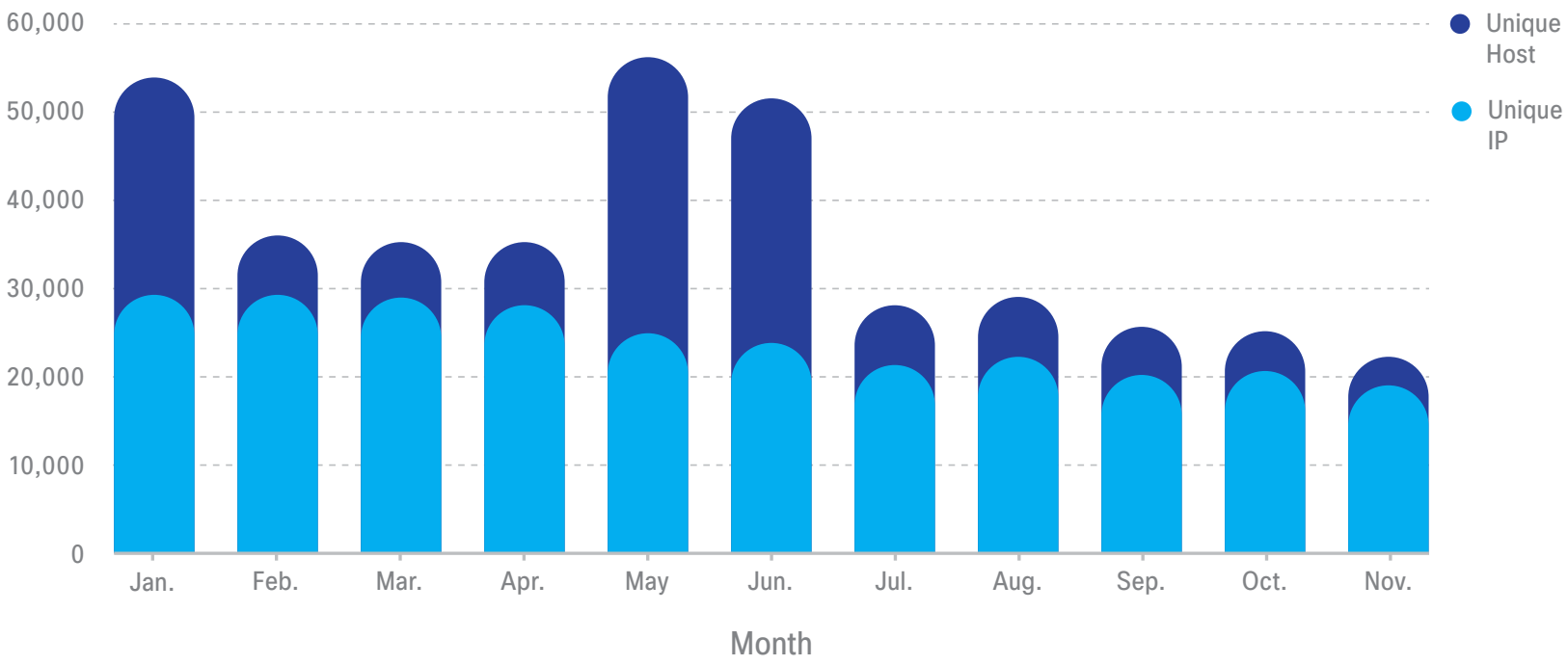
Research by Cisco TRAC/SIO during 2013 shows multipurpose trojans were the most frequently encountered web-delivered malware, at 27 percent of the total encounters. Malicious scripts, such as exploits and iframes, were the second most frequently encountered category, at 23 percent. Data-theft trojans, such as password stealers and backdoors, made up 22 percent of total web malware encounters, with downloader and dropper trojans in fourth place at 17 percent of total encounters (see Figure 21).

The steady decline in unique malware hosts and IP addresses—a 30 percent decline between January 2013 and September 2013—suggests that malware is being concentrated in fewer hosts and fewer IP addresses (Figure 22). (Note: An IP address can serve websites for multiple domains.) As the number of hosts declines—even as malware remains steady—the value and reputation of these hosts becomes more important, since good hosts help criminals accomplish their goals.

FIGURE 22

Unique Malware Hosts and IP Addresses, 2013

Source: Cisco Cloud Web Security reports



Watering Holes No Oasis for Targeted Enterprises

One way malicious actors try to deliver malware to organizations in specific industry verticals is through the use of "watering hole" attacks. Like big game watching their prey, cybercriminals looking to target a particular group (for example, people who work in the aviation industry) will monitor which websites that group frequents, infect one or more of these sites with malware, and then sit back and hope at least one user in the target group visits that site and is compromised.

A watering hole attack is essentially a trust exploit because legitimate websites are employed. It is also a form of spear phishing. However, while spear phishing is directed at select individuals, watering holes are designed to compromise groups of people with common interests. Watering hole attacks are not discerning about their targets: anyone who visits an infected site is at risk.

At the end of April, a watering hole attack was launched from specific pages hosting nuclear-related content at the U.S. Department of Labor website.[16] Then, beginning in early May 2013, Cisco TRAC/SIO researchers observed another watering hole attack emanating from several other sites centered on the energy and

Continues on next page

Prime Targets: Industry Verticals

Companies in high-profit verticals, such as the pharmaceutical and chemical industry and electronics manufacturing, have high rates of web malware encounters, according to Cisco TRAC/SIO research.

The rate goes up or down as the value of a particular vertical's goods and services rises or declines.

Cisco TRAC/SIO researchers observed remarkable growth in malware encounters for the agriculture and mining industry—formerly a relatively low-risk sector. They attribute the increase in malware encounters for this industry to cybercriminals seizing on trends such as decreasing precious metal resources and weather-related disruptions in the food supply.

Also continuing to rise are malware encounters in the electronics industry. Cisco security experts report that malware targeting this vertical typically is designed to help actors gain access to intellectual property, which they in turn use for competitive advantage or sell to the highest bidder.

To determine sector-specific malware encounter rates, Cisco TRAC/SIO researchers compare the median encounter rate for all organizations that proxy through Cisco Cloud Web Security to the median encounter rate for all companies in a specific sector that proxy through the service. An industry encounter rate above 100 percent reflects a higher-than-normal risk of web malware encounters, whereas a rate below 100 percent reflects a lower risk. For example,

Continued from previous page

oil sector. Similarities, including the specific crafting of an exploit used in both attacks, lend credence to the possibility that the two attacks were related. Cisco TRAC/SIO's research also indicated that many of the sites used the same web designer and hosting provider. This could imply that the initial compromise was due to phished or stolen credentials from that provider.[17]

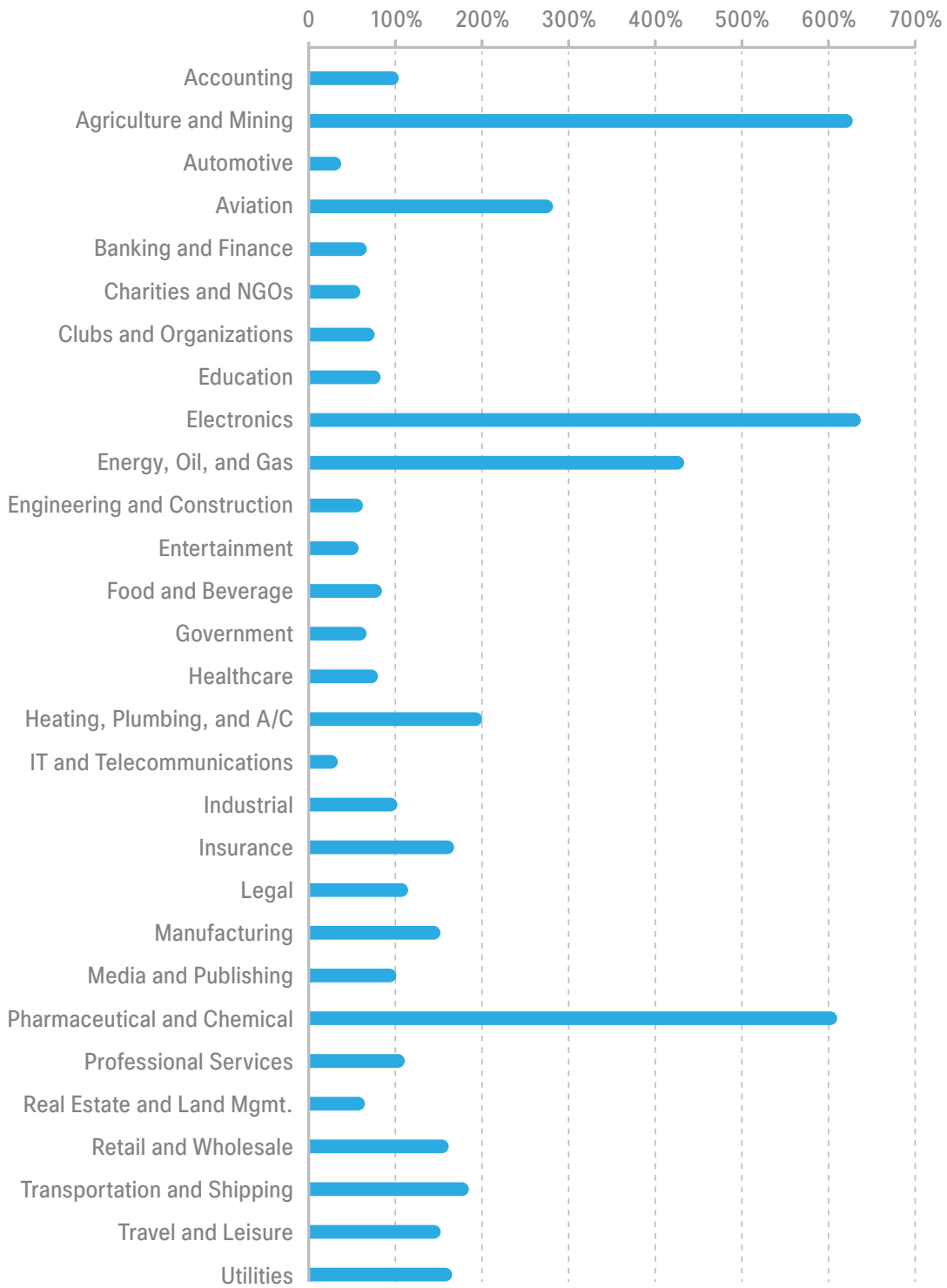
Protecting users against these attacks involves keeping machines and web browsers fully patched to minimize the number of vulnerabilities that an attacker can exploit. Ensuring web traffic is filtered and checked for malware prior to its delivery to the user's browser is also essential.

a company with a 170 percent encounter rate is at a 70 percent increased risk higher than the median. Conversely, a company with a 70 percent encounter rate is 30 percent below the median (Figure 23).

FIGURE 23

Industry Risk and Web Malware Encounters, 2013

Source: Cisco Cloud Web Security reports



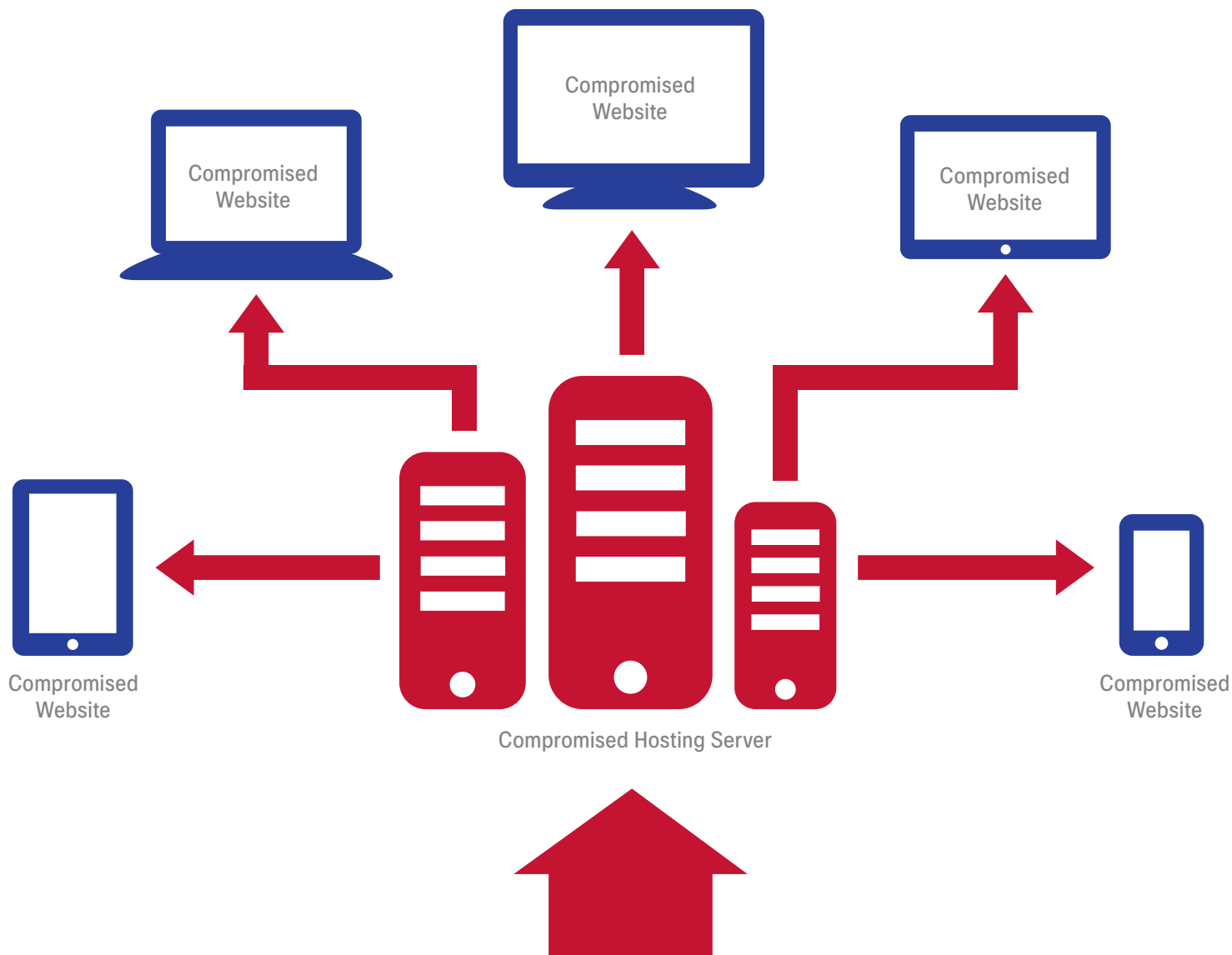
Fractures in a Fragile Ecosystem

Cybercriminals are learning that harnessing the power of the Internet's infrastructure yields far more benefits than simply gaining access to individual computers.

The newest twist in malicious exploits is to gain access to web hosting servers, nameservers, and data centers—with the goal of taking advantage of the tremendous processing power and bandwidth they provide. Through this approach, exploits can reach many more unsuspecting computer users and have a far greater impact on the organizations targeted, whether the goal is to make a political statement, undermine an adversary, or generate revenue.

FIGURE 24

High-Efficiency Infection Strategy



In essence, this trend in targeting Internet infrastructure means the foundation of the web itself cannot be trusted. Methods used to ultimately gain root access to hosting servers are varied and include tactics such as trojans on management workstations that steal server login credentials, vulnerabilities in third-party management tools used on the servers, and brute-force login attempts (see page 53). Unknown vulnerabilities in the server software itself may also provide inroads.

One compromised hosting server can infect thousands of websites and site owners around the world (Figure 24).

Websites hosted on compromised servers act as both a redirector (the intermediary in the infection chain) and a malware repository. Instead of many compromised sites loading malware from only a few malicious domains (a many-to-few relationship), the relationship has now become many-to-many, hampering takedown efforts.

Domain nameservers are prime targets in this new breed of attack, the exact methods of which are still under investigation. Indicators are that, in addition to individual websites and hosting servers, nameservers at certain hosting providers are also being compromised. Cisco security researchers say this trend toward targeting the Internet's infrastructure shifts the threat landscape, because it is giving cybercriminals control over a not-insignificant portion of the very foundation of the web.

"Cybercrime has become so lucrative and heavily commoditized that it needs a powerful infrastructure to keep it afloat," says Gavin Reid, director of threat intelligence for Cisco. "By compromising hosting servers and data centers, attackers gain not only access to large amounts of bandwidth, but also the benefit of continuous uptime for those resources."

"Cybercrime has become so lucrative and heavily commoditized that it needs a powerful infrastructure to keep it afloat."

Gavin Reid, director of threat intelligence for Cisco

Connecting the Dots: DarkLeech and Linux/CDorked

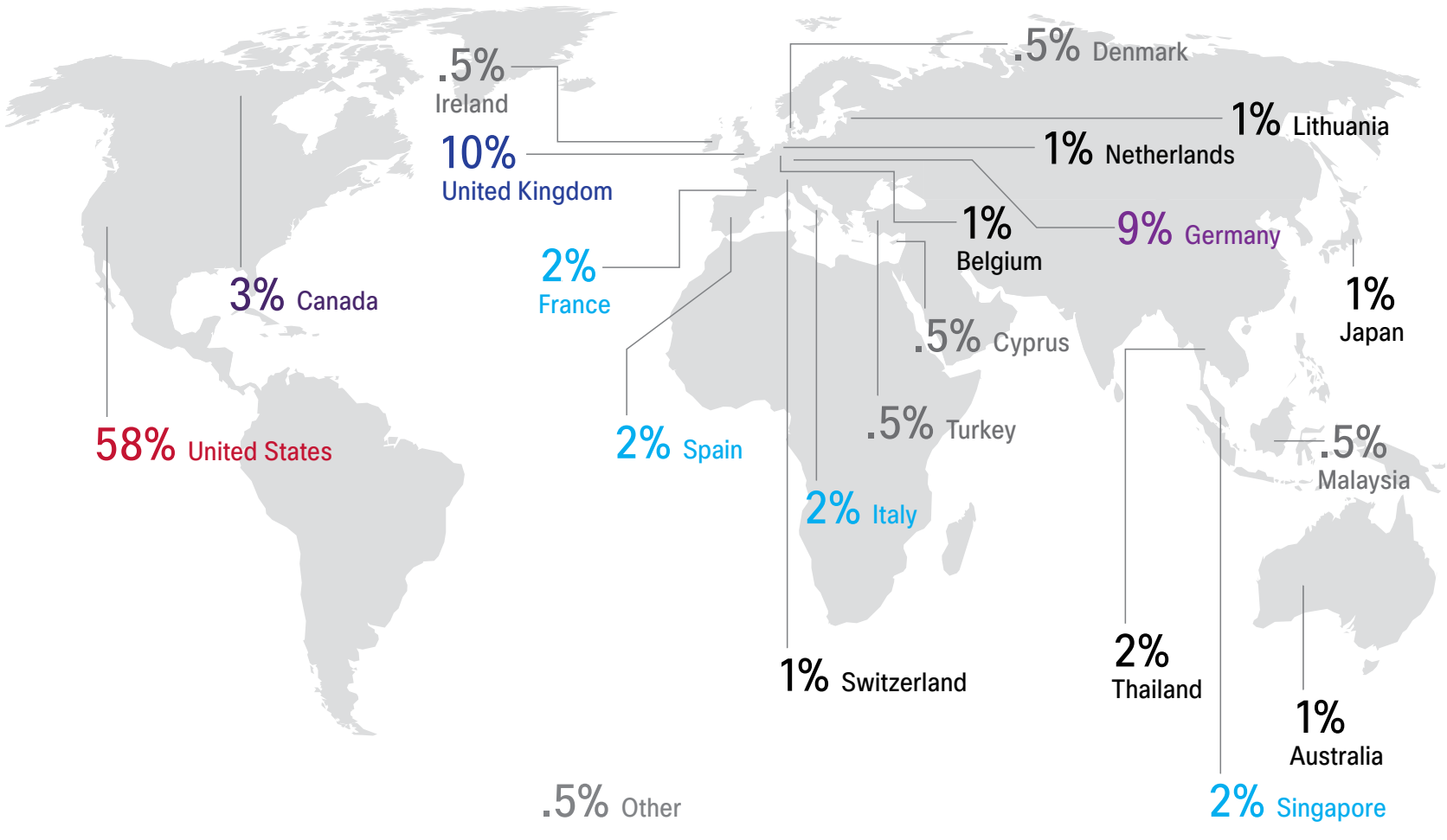
The DarkLeech attack campaign reported by Cisco in 2013[18] underscores how the compromise of hosting servers can serve as a springboard to a larger campaign. It is estimated that the DarkLeech attacks compromised, in a short time period, at least 20,000[19] legitimate websites around the world that use Apache HTTP server software. Sites were infected with a Secure Shell daemon (SSHD) backdoor that allowed remote attackers to upload and configure malicious Apache modules. The compromise enabled attackers to dynamically inject iframes (HTML elements) in real time on hosted websites, which delivered exploit code and other malicious content by means of the Blackhole exploit kit.

Because the DarkLeech iframe injections occur only at the moment of a site visit, signs of the infection may not be readily apparent. In addition, to avoid detection of the compromise, criminals use a sophisticated array of conditional criteria—for instance, injecting the iframe only

FIGURE 25

DarkLeech Server Compromises by Country, 2013

Source: Cisco TRAC/SIO



if the visitor arrives from a search engine results page, not injecting the iframe if the visitor's IP address matches that of the site owner or hosting provider, and injecting the iframe only once every 24 hours for individual visitors.

The Cisco TRAC/SIO investigation revealed that the DarkLeech compromises spanned the globe; countries with the largest number of hosting providers naturally experienced the highest rate of infection.

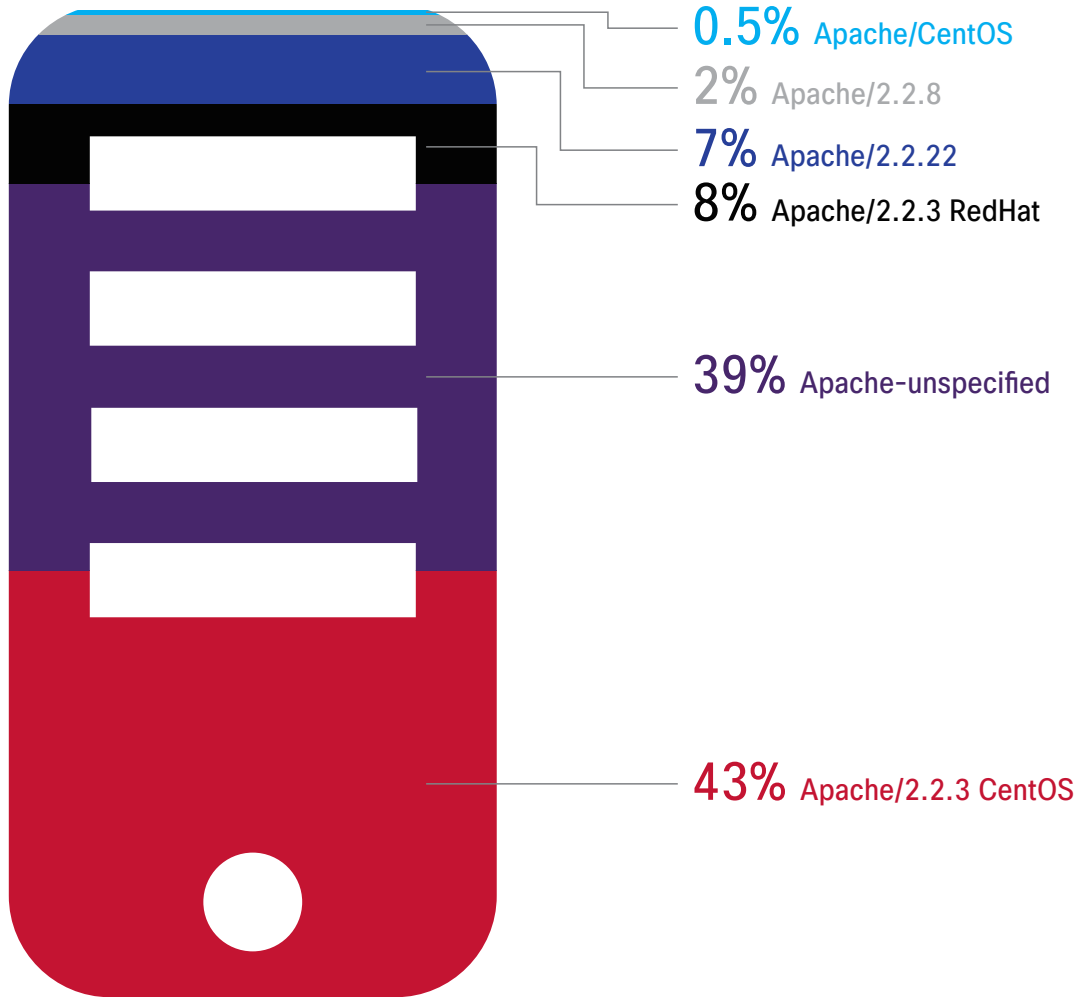
Cisco SIO/TRAC researchers queried thousands of compromised servers to ascertain the distribution of affected server software versions.

In April 2013, another malicious backdoor that had infected hundreds of servers running Apache HTTP server software was detected. Linux/CDorked[20] replaced the HTTPD binary on cPanel-installed versions of Apache. Similar backdoors targeting Nginx and Lighttpd were

FIGURE 26

DarkLeech-Compromised Server Responses

Source: Cisco TRAC/SIO



also discovered. Just as selective as DarkLeech in its attack methods, CDorked also uses conditional criteria to dynamically inject iframes on websites hosted on the affected server. Any visitor browsing an affected website then has malicious content delivered from another malicious website, where a crimeware toolkit attempts to further compromise the user's PC.[21]

A unique feature of Linux/CDorked is that it cycles through website domains in 24 hours, on average. Few compromised sites are used for longer. Thus, even if a malware domain is reported, attackers have already moved on. Also with Linux/CDorked, hosting providers are changed frequently (about every two weeks), cycling through the compromised hosts to avoid detection. Compromised nameservers at these same hosting providers enable malicious actors to move from host to host without losing control of domains during the transition. Once on a new host, the attackers begin a cycle of new domains, often using typosquatting-style[22] domain names in an attempt to appear legitimate to casual observers.

CDorked and DarkLeech appear to be part of a much greater and far more complex strategy.

Cisco TRAC/SIO analysis of traffic patterns with CDorked strongly suggests a connection with DarkLeech. The specially encoded referrer URL employed by CDorked specifically denotes traffic from DarkLeech. But that isn't the most interesting twist about the malware: both CDorked and DarkLeech appear to be part of a much greater and far more complex strategy.

"The sophistication of these compromises suggests cybercriminals have gained significant control over thousands of websites and multiple hosting servers, including nameservers employed by those hosts," says Gavin Reid, director of threat intelligence for Cisco. "Combined with the recent spate of brute-force login attacks against individual websites, we appear to be witnessing a changing tide, where the infrastructure of the web is being used to form what can only be described as a very large—and very powerful—botnet. This überbot can be used for sending spam, delivering malware, and launching DDoS attacks on a scale never before seen."

Malicious Traffic, Often a Sign of Targeted Attacks, Detected in All Corporate Networks

According to a Cisco examination of threat intelligence trends, malicious traffic is visible on 100 percent of corporate networks. This means there is evidence that sophisticated criminals or other players have penetrated these networks and may be operating undetected over long periods of time.

All organizations should assume they've been hacked, or at least agree that it's not a question of if they will be targeted for an attack, but when ... and for how long.

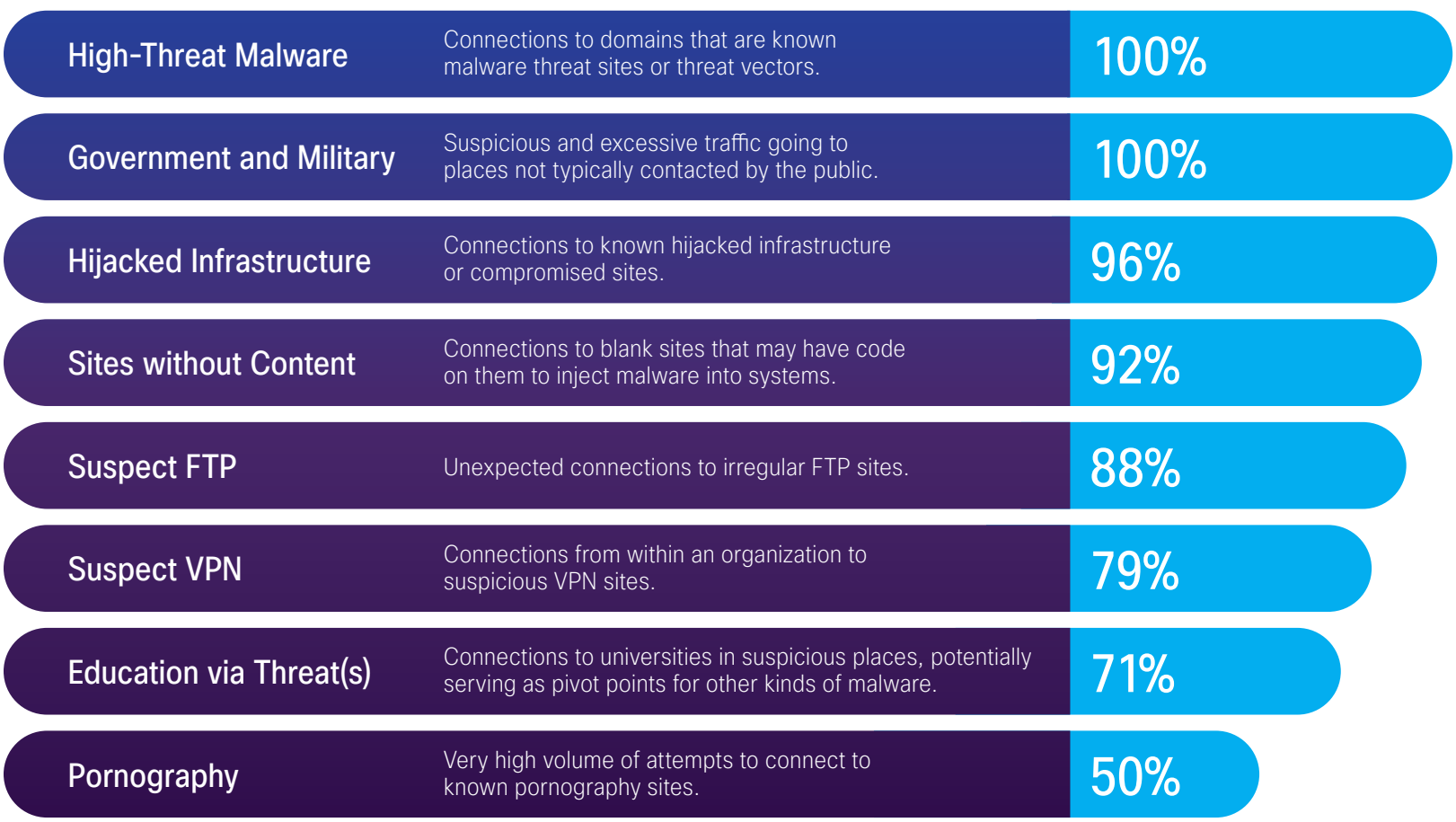
In a recent project reviewing Domain Name Service (DNS) lookups originating from inside corporate networks, Cisco threat intelligence experts found that in every case, organizations showed evidence that their networks had been misused or compromised (Figure 27). For example, 100 percent of the business networks analyzed by Cisco had traffic going to websites that host malware, while 92 percent show traffic to webpages without content, which typically host malicious activity. Ninety-six percent of the networks reviewed showed traffic to hijacked servers.

Cisco also detected traffic going to military or government websites within enterprises that do not normally do business with either, as well as to websites for high-risk geographic areas, such as countries embargoed from doing business with the United States. Cisco has observed that such sites may be used because of the generally high reputation enjoyed by public or government organizations. Traffic to these sites may not be a definitive sign of a compromise, but for organizations that do not habitually do business with the government or the military, such traffic could indicate that networks are being compromised so that criminals can use them to breach government or military websites and networks.

In spite of their best efforts to keep their networks free of malicious threats, all of the organizations Cisco examined during 2013 showed evidence of suspicious traffic. The traffic identified through DNS lookups can provide strong IoCs and are worth further investigation by organizations that want to halt these hard-to-detect threat actors in their networks. It's a method to increase visibility of criminal movement that is typically very difficult to locate.

FIGURE 27

The Pervasiveness of Malicious Traffic



SPECIAL CISCO SECURITY RESEARCH FEATURE:

New Twists on Bitsquatting—and New Ways to Halt Attacks

Cybersquatting—the practice of registering domain names that are identical or confusingly similar to a distinctive mark—has long been a tool of online criminals. Recently, "bitsquatting," the registration of domain names that are one binary digit different from the original domain, has become another way to redirect Internet traffic to sites hosting malware or scams.

Bitsquatting is a form of cybersquatting that targets bit errors in computer memory. A memory error occurs anytime one or more bits being read from memory have changed in state from what was previously written. These errors in memory can occur because of many factors, including cosmic rays (high-energy particles that strike Earth as frequently as 10,000 per square meter per second), a device being used outside its recommended environmental parameters, manufacturing defects, and even low-yield nuclear explosions.

By changing a single bit, a domain such as "twitter.com" can become the bitsquat domain "twitte2.com." An attacker can simply register a bitsquat domain, wait for a memory error to occur, and then intercept Internet traffic.

Security researchers believe bitsquatting attacks are most likely to occur against frequently resolved domain names, since these domains are most likely to appear in memory when bit errors occur. However, recent Cisco research predicts that domains previously not considered "popular" enough to attack will actually produce useful amounts of bitsquat traffic. This is because the amount of memory per device and the number of devices connected to the Internet are both increasing; according to Cisco estimates, there will be 37 billion "intelligent things" connected to the Internet by 2020.[23]

Bitsquatting Attack Vectors

Cisco TRAC/SIO has identified new bitsquatting attack vectors, including:

- Subdomain delimiter bitsquatting: According to the accepted syntax for domain name labels, the only valid characters inside a domain name are A-Z, a-z, 0-9, and the hyphen. However, when checking for bitsquat domains, limiting the search to these characters neglects an important character that is also valid inside domain names: the dot. One new bitsquatting technique relies on bit errors that result in a letter "n" (binary 01101110) becoming a dot "." (binary 00101110) and vice versa.
- Subdomain delimiters where "n" flips to ".": In a variation of the above technique, if a second-level domain name contains the letter "n" and there are two or more characters after the letter "n," then this is a potential bitsquat. For example, "windowsupdate.com" could become"dowsupdate.com."
- URL delimiter bitsquats: A popular context for domain names is within a URL. Inside a typical URL, forward-slash characters such as "/" act as delimiters, separating the scheme from the hostname from the URL path. The forward slash character (binary 00101111) can, by the flip of one bit, become the letter "o" (binary 01101111), and vice versa.

Continues on next page

Continued from previous page

Preventing Bitsquatting Attacks: Create a Bitsquat RPZ

The two mitigation techniques that have commonly been in use to prevent bitsquatting have their place in the security arsenal, but neither method is optimal:

- Use error-correcting (ECC) memory: The entire base of installed devices would have to upgrade simultaneously worldwide to make this an effective solution.
- Register the bitsquat domain so that no third party can register it: This is not always possible, as many popular bitsquat domains have already been registered. Depending on the length of the domain name, this also can be costly.

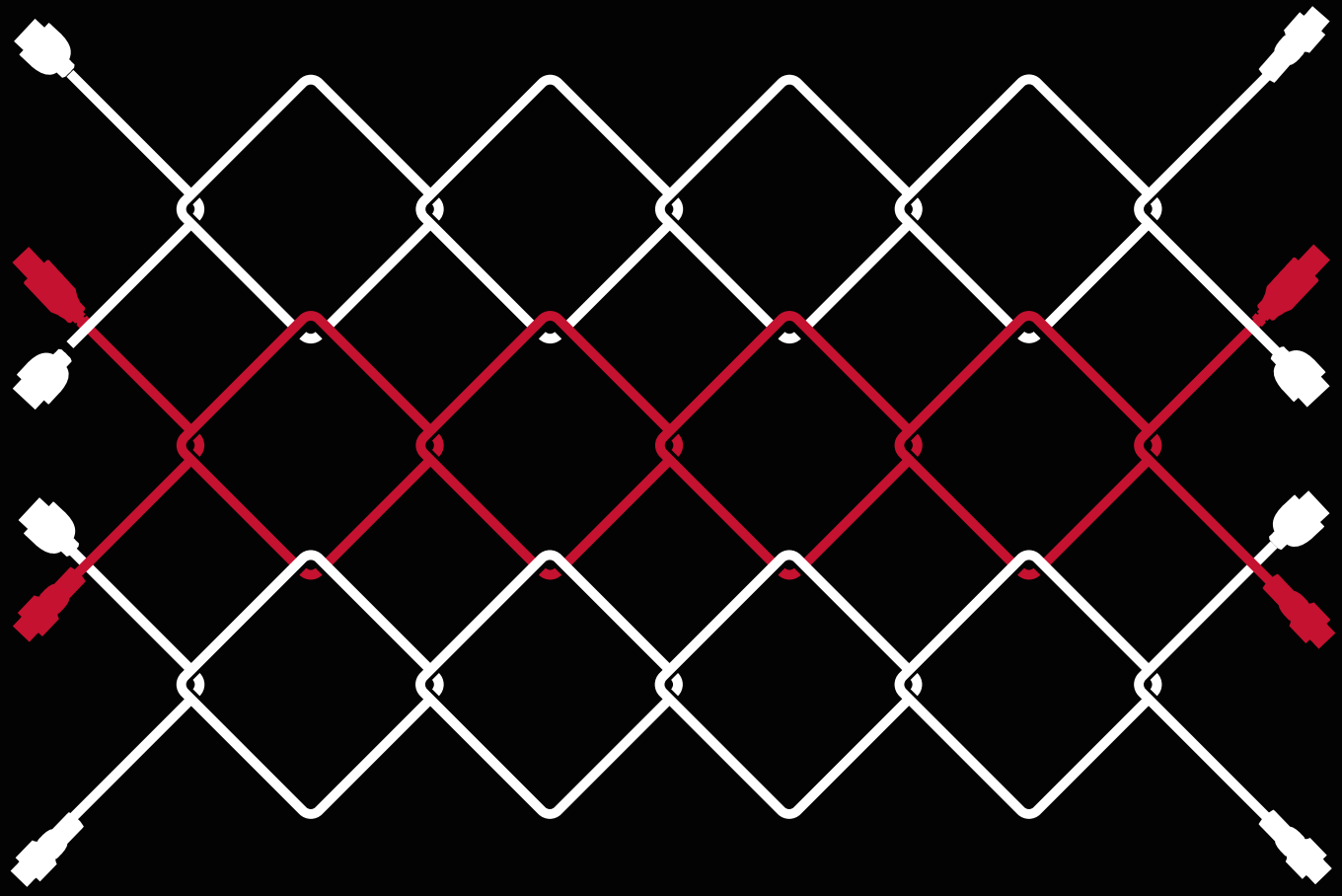
The good news is that these mitigation techniques are not the only ones a security professional can deploy to protect users from accidentally misdirecting Internet traffic. With sufficient adoption, the new mitigations could eliminate the bitsquatting problem almost completely.

For example, response policy zones (RPZs) have been a configuration option since BIND version 9.8.1, and patches exist for earlier versions of BIND. (BIND is widely used Internet DNS software.) RPZs are local zone files that allow the DNS resolver to respond to specific DNS requests by saying the domain name does not exist (NXDOMAIN), redirecting the user to a "walled garden" (a closed platform), or other possibilities.

To mitigate the effects of single bit errors for users of a DNS resolver, the resolver administrator can create an RPZ that protects against bitsquats of frequently resolved or internal-only domain names. For example, the RPZ can be set up so that any requests made to the DNS resolver for bitsquat variants of these domains will get a NXDOMAIN response, silently "correcting" bit errors without any work on the part of the client experiencing the bit error.[24]

Industry

Cisco SIO investigators elevate the discussion around industry trends that extend beyond Cisco's telemetry.



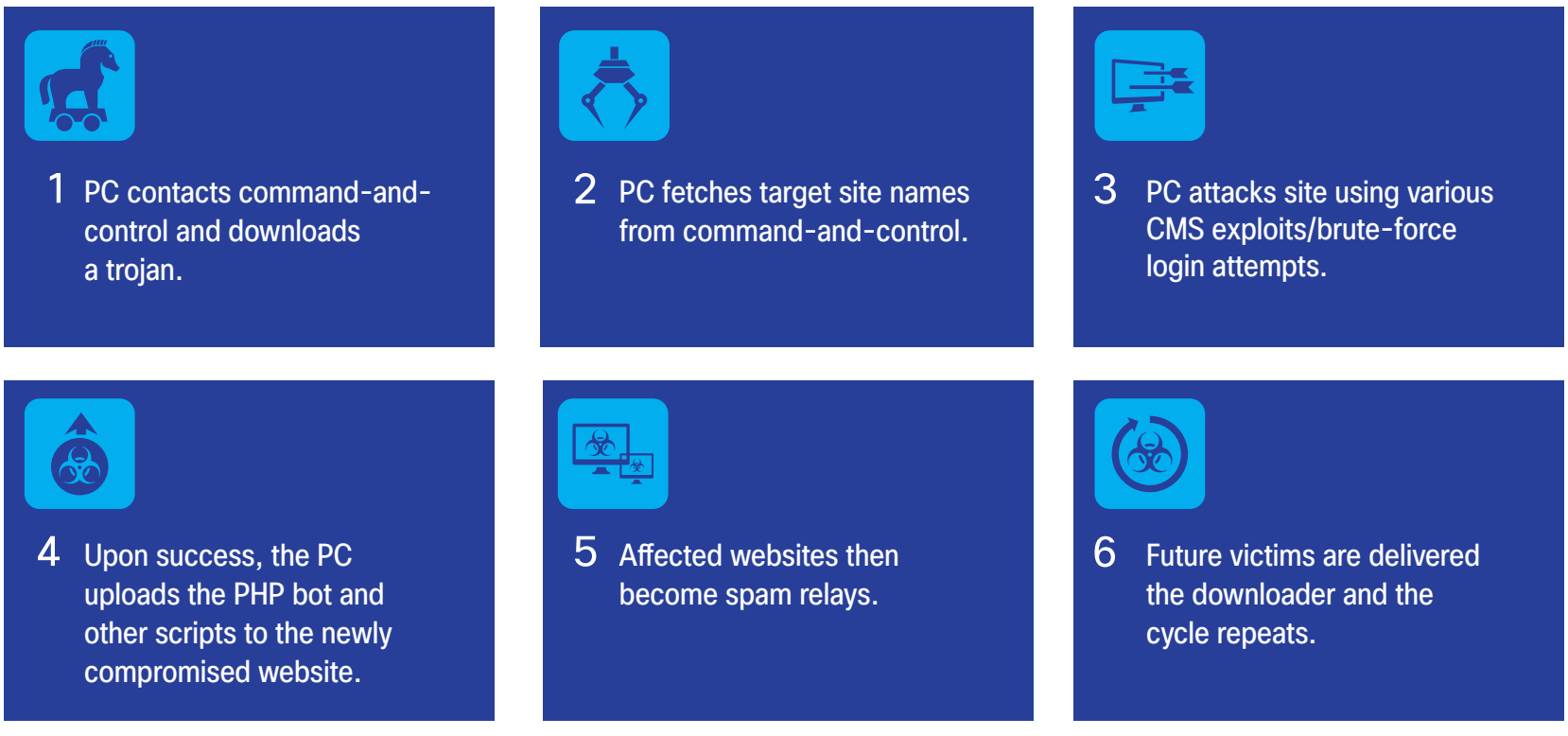
Brute-Force Login Attempts a Favored Tactic to Compromise Websites

Although brute-force login attempts are by no means a new tactic for cybercriminals, their use increased threefold in the first half of 2013.

In the course of investigation, researchers with Cisco TRAC/SIO discovered a hub of data used to feed such actions. It included 8.9 million possible username and password combinations, including strong passwords—not just the easy-to-crack "password123" variety. Stolen user credentials help to keep this list, and others like it, well stocked.

FIGURE 28

How Brute-Force Login Attempts Work



Key targets for recent brute-force login attempts are widely used content-management system (CMS) platforms such as WordPress and Joomla. Successful attempts to gain unauthorized access through a CMS give attackers the ability to upload PHP (hypertext preprocessor) backdoors and other malicious scripts to compromised websites. In some cases, the compromise can enable attackers to find a path to a hosting server, which can then be commandeered (Figure 28).

Considering that there are more than 67 million WordPress sites around the world—and that publishers are using the platform to create blogs, news sites, company sites, magazines, social networks, sports sites, and more—it's not surprising that many online criminals have their sights set on gaining access through this CMS.[25] Drupal, a rapidly growing CMS platform, has been targeted this year as well; for example, in May, users were advised to change their passwords because "unauthorized access [to Drupal] was made through third-party software installed on the Drupal.org server infrastructure."[26]

Many online criminals have their sights set on gaining access through CMS.

But it isn't just the popularity of these systems that makes them desirable targets. Many of these sites—though active—have been largely abandoned by their owners. There are likely millions of abandoned blogs and purchased domains sitting idle, and many of them are probably now owned by cybercriminals. Cisco security experts predict the problem will only worsen as more and more people in emerging Internet markets around the globe establish a blog or a website, only to let it languish later.

The widespread use of plugins, which are designed to extend the functionality of a CMS and to power videos, animations, and games, is also proving to be a boon for miscreants looking to gain unauthorized access to platforms like WordPress and Joomla. Many CMS compromises observed by Cisco researchers in 2013 can be traced back to plugins written in the PHP web scripting language that were designed poorly and without security in mind.

DNS AMPLIFICATION:
Mitigation Techniques

[Attacks launched through DNS amplification will remain a concern in 2014, according to Cisco security experts. The Open Resolver Project (openresolverproject.org) reports that as of October 2013, 28 million open resolvers on the Internet pose a "significant threat." (Consider that the Spamhaus DDoS attack of 300 Gbps used only 30,000 open resolvers.)]

If a resolver is open, that means it is not filtering where it is sending responses. DNS uses the UDP protocol, which is stateless, meaning a request can be made on behalf of another party. That party then receives an amplified amount of traffic. This is why identifying open resolvers—and taking steps to close them—is something the industry will be dealing with for some time to come.

Enterprises can reduce the chance of an attack launched by DNS amplification in several ways, including implementing the Internet Engineering Task Force's Best Current Practice (BCP) 38 to avoid being the source of attacks. This BCP recommends that upstream providers of IP connectivity filter packets entering their networks from downstream customers, and to discard any packets that have

Continues on next page

DDoS Attacks: What's Old Is New Again

Distributed denial of service (DDoS) attacks—which disrupt traffic to and from targeted websites and can paralyze ISPs (Internet service providers)—have been increasing in both volume and severity.

Because DDoS attacks had long been considered "old news" in terms of cybercrime techniques, many enterprises were confident the security measures they had in place could provide adequate protection. But that confidence has been shaken by large-scale DDoS attacks in 2012 and 2013, including Operation Ababil, which was directed at several financial institutions and likely politically motivated.[27]

"DDoS attacks should be a top security concern for organizations in the public and private sector in 2014," says John N. Stewart, senior vice president and chief security officer at Cisco. "Expect future campaigns to be even more extensive and to last for extended periods. Organizations, particularly those that operate or have interests in industries that are already prime targets, such as financial services and energy, need to ask themselves, 'Can we be resilient against a DDoS attack?'"

A new twist: Some DDoS attacks are probably being used to conceal other nefarious activity, such as wire fraud before, during, or after a campaign. (See "DarkSeoul," page 57.)

Continued from previous page

a source address not allocated to that customer.[30] The BCP was co-authored by Cisco, which offers guidelines on deploying uRPF, its implementation.[31]

Another mitigation technique is to configure all authoritative DNS servers to use rate limiting. The authoritative nameserver, which serves an enterprise's domain, is generally open to all requests. DNS response rate limiting (DNS RRL) is a feature that can be turned on to prevent a DNS server from answering the same question from the same entity too many times—thus protecting the enterprise from being used as an intermediary in DDoS attacks. DNS RRL is enabled on DNS servers and it is one way for a server administrator to limit how effectively a server can be used by attackers in amplification attacks. DNS response rate limiting is a newer feature, and it is not supported by all DNS servers; however, it is supported by ISC BIND, a popular DNS server.

In addition, all recursive DNS servers need to be configured with an access control list (ACL) so they will respond only to queries from hosts on their own network. A poorly managed ACL can be a primary factor in DNS attacks, especially on large servers with large amounts of available bandwidth. This technique also helps

Continues on next page

These attacks can overwhelm bank personnel, prevent transfer notifications to customers, and prevent customers from reporting fraud. And by the time an institution recovers from such an event, it is unable to recoup its financial losses. One such attack that took place on December 24, 2012, targeted the website of a regional California financial institution and "helped to distract bank officials from an online account takeover against one of its clients, netting thieves more than $900,000."[28]

Rapidly deepening expertise in compromising hosting servers will only make it easier for cybercriminals to launch DDoS attacks and steal from targeted organizations (see "Fractures in a Fragile Ecosystem," page 43). By commandeering a portion of the Internet's infrastructure, malicious actors can take advantage of large amounts of bandwidth, positioning them to launch any number of powerful campaigns. It's already happening: In August 2013, the Chinese government reported that the largest DDoS attack it had ever faced shut down the Chinese Internet for about four hours.[29]

Even spammers are using DDoS attacks to strike back at organizations they believe are standing in the way of their revenue generation. In March 2013, the nonprofit Spamhaus—which tracks spammers and created the Spamhaus Block List, a directory of suspect IP addresses—was the target of a DDoS attack that temporarily shut down its website and slowed Internet traffic worldwide. The attackers were allegedly affiliated with the Netherlands-based CyberBunker, a hosting provider with permissive terms of use, and STOPhaus, which has publicly expressed its dislike for Spamhaus's activities. The DDoS attack came after the widely used Spamhaus service included CyberBunker on its blacklist. In apparent retaliation, suspected spammers attempted to take Spamhaus offline via a DDoS attack.

Continued from previous page

reduce the chances of becoming an intermediary in a DDoS attack.

"Since there is discussion in the security industry around allowing authoritative nameservers to disable service to entities that end up becoming intermediaries in DDoS attacks, enterprises should employ the simple mitigation techniques described above," says Gavin Reid, director of threat intelligence for Cisco.

For more on DNS best practices, refer to "DNS Best Practices, Network Protections, and Attack Identification": http://www.cisco.com/web/about/security/intelligence/dns-bcp.html.

This DDoS incident employed a DNS amplification attack, which exploits open DNS resolvers that respond even to queries outside its IP range. By sending an open resolver a very small, deliberately formed query with a spoofed source address of the target, attackers can evoke a significantly larger response to the intended target. After initial attempts to take Spamhaus offline failed, the attackers employed a DNS amplification attack targeting Tier 1 and other upstream providers for Spamhaus.

DarkSeoul

As noted in "DDoS Attacks: What's Old Is New Again," cybercriminals' new focus and fast-growing expertise in compromising hosting servers is only making it easier to launch DDoS attacks and steal from organizations.

Cisco security researchers warn that future DDoS campaigns are likely to be capable of creating both significant disruption and damage—including financial loss due to theft.

The DarkSeoul targeted attacks of March 2013 involved "wiper" malware designed to destroy data in the hard drives of tens of thousands of PCs and servers. The attacks targeted financial institutions and media firms in South Korea, with the payload set to activate at the same time. The wiper malware appears to be only one facet of the attack, however. At the same time the malware was triggered, the website of the Korean network provider LG U+ was defaced and the networks of other targeted organizations started going down—capabilities not reproducible in the wiper malware.[32]

Some believe the attacks were a result of cyberwarfare instituted by North Korea to disrupt South Korea economically or an act of sabotage by another nation-state. But the possibility exists that the DarkSeoul attacks were meant to conceal financial gain.[33]

Security researchers are still trying to understand these attacks—and discover who was responsible for them—but evidence indicates that plans for DarkSeoul may have been put in motion as far back as 2011. In that year, the U.S. Federal Bureau of Investigation (FBI) first warned of the emergence of banking trojans designed to conceal the wiring of fraudulent funds from victims' accounts.[34] Then, in 2012, the RSA security firm reported on a new breed of cybercriminals constructing a sophisticated trojan campaign that would launch an attack on a scheduled day and attempt to "to cash out as many compromised accounts as possible before its operations are ground to a halt by security systems."[35] And on Christmas Eve 2012, online thieves used a DDoS attack as a cover while they stole from a regional California financial institution.[36]

One malware binary identified in the DarkSeoul attacks that targeted media organizations and financial institutions is a banking trojan that specifically targeted customers of those same Korean banks, according to Cisco TRAC/SIO investigators. That fact, along with the timeline of cybercrime trends leading up to DarkSeoul, indicates the campaign could have been theft made to look like something else.

Ransomware

Throughout 2013, attackers have increasingly moved away from traditional botnet-driven infections on PCs. Part of this shift included the increased use of ransomware as the final malware payload from compromised websites, malicious email, and downloader trojans. Ransomware is a category of malware that prevents the normal operation of infected systems until a prescribed fee is paid.

Throughout 2013, attackers have increasingly moved away from traditional botnet-driven infections on PCs.

Ransomware provides a difficult to track, yet straightforward, direct revenue stream for attackers without requiring the use of intermediary leased services such as those provided by traditional botnets. Attackers mimic legitimate local economies that have seen a significant increase in sole proprietorship as a result of job losses

and economic downturns, but the motivation for cybercriminals is the loss of botnet availability and accessible exploit kits due to takedowns.

In the fall of 2013, a new type of ransomware, dubbed CryptoLocker, began encrypting victims' files with a combination of RSA 2048-bit key pairs and AES-256, considered unfeasible to break. In action, CryptoLocker move files beyond the local machine to include matching file types on any writeable mapped drive. Upon completion of the encryption routine, victims are presented with a series of dialog boxes that provide detailed instructions for payment of the ransom (Figure 29). A timer is also presented instructing the victim to pay within a specific time (ranging from 30 to 100 hours). The dialog further warns that if the ransom is not paid in the allotted time, the private key will be deleted from the command-and-control server, after which the chance to decrypt the files will be lost.

CryptoLocker surged in mid-October, possibly in response to the loss of the Blackhole and Cool exploit kits following the arrest of the alleged author of those frameworks.

FIGURE 29

Ransom Instructions from CryptoLocker

The Security Talent Shortage and Solutions Gap

[The sophistication of the technology and tactics used by online criminals—and their nonstop attempts to breach network security and steal data—have outstripped the ability of IT and security professionals to address threats. Most organizations do not have the people or the systems to monitor their networks consistently and to determine how they are being infiltrated.]

The security talent shortage makes this problem worse: even when budgets are generous, CISOs struggle to hire people with up-to-date security skills. It's estimated that by 2014, the industry will still be short more than a million security professionals across the globe. Also in short supply are security professionals with data science skills—understanding and analyzing security data can help improve alignment with business objectives. (See the appendix on page 68, "Security Organizations Need Data Scientists: Introductory Data Analysis Tools for Security Practitioners.")

CISOs struggle to hire people with up-to-date security skills.

Cloud as a New Perimeter

As CISOs tell Cisco security experts (see page 18), moving ever-increasing amounts of critical business data to the cloud is a growing security concern.

The cloud revolution, says Michael Fuhrman, Cisco vice president of engineering, is comparable to the rise in web-based solutions in the late 1990s.

"This was a radical shift in business use of new technology—and at that same time, we saw a rise in online attacks from criminals," says Fuhrman. "Today, the radical shift comes from the cloud. Not only do businesses host many of their critical applications in the cloud, but they are also using the cloud to consume and analyze critical business information."

The rise in cloud computing is undeniable and unstoppable. Cisco has projected that cloud network traffic will grow more than threefold by 2017.[37]

In 2014 and onward, security professionals can expect to see entire corporate perimeters move to the cloud. These network edges have been in the process of becoming far less well-defined in recent years. But with so many applications and so much data in the cloud, organizations are rapidly losing the ability to see who and what is moving in and out of corporate boundaries, and what actions users are taking.

This transition to the cloud changes the game because it redefines where data is stored, moved, and accessed—and creates greater opportunities for attackers.

Adding to fears about ceding the control of data to the cloud is lack of information about how cloud vendors defend their products against security breaches. Organizations often don't ask enough questions about what is contained in their vendors' service-level agreements, or how often vendors upgrade their security software or patch vulnerabilities.

Organizations need reassurance that a cloud provider is using the most sophisticated tools and strategies available to thwart attacks, or to detect and stop them while in progress. For information security teams, the decision to move forward often comes down to one question: "What controls should I look for in a provider to trust it to manage and protect my data?"

On the other side of the fence, cloud providers struggle with identifying and implementing a manageable set of controls mapped to an increasing number of international regulations, which are needed to address an increasingly hostile threat environment.

"When we choose vendors for security and critical infrastructure, we often buy based on technical qualifications and reputation," says John N. Stewart, senior vice president and chief security officer at Cisco. "Lately, the vendor's process and evolving security approach have also become increasingly important factors."

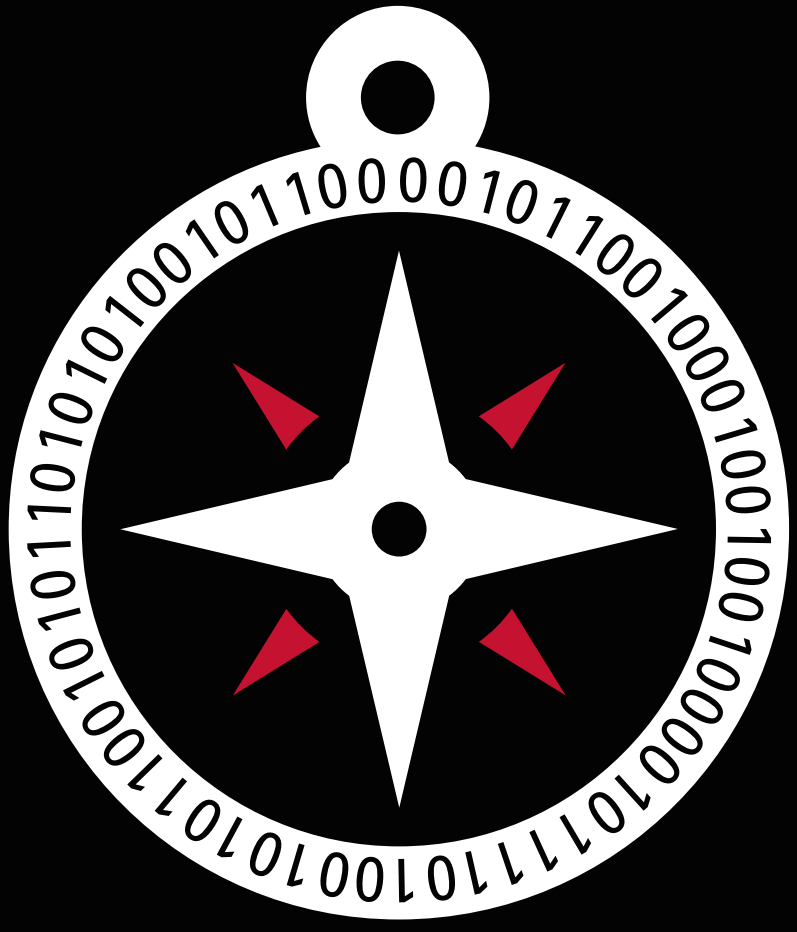
Coincidentally, the very things that make the cloud a threat—such as the location outside the network perimeter and the increasing use of the cloud for business-critical data—can enable organizations to make more accurate and near-real-time security decision making. With more traffic going through the cloud, security solutions that also rely on the cloud can quickly and easily analyze this traffic and gain from this supplemental information. In addition, for smaller organizations or those with budget constraints, a well-protected and well-managed cloud service can offer more security safeguards than a business's own servers and firewalls.

"When we choose vendors for security and critical infrastructure, we often buy based on technical qualifications and reputation. Lately, the vendor's process and evolving security approach have also become increasingly important factors."

John N. Stewart, senior vice president and chief security officer at Cisco

Recommendations

More organizations are struggling to solidify a security vision supported by an effective strategy that uses new technologies, simplifies their architecture and operations, and strengthens their security teams.



Objectives for 2014: Verifying Trustworthiness and Improving Visibility

Today, in an environment where the level of trust associated with a network or device must be dynamically evaluated, organizations are faced with fragmented security models that provide inconsistent enforcement, isolated threat intelligence, and a proliferation of vendors and products to manage.

The connections among organizations, data, and the advanced attacks launched by malicious actors are simply too complex for a single appliance to address. And most organizations lack security personnel with the expertise and experience to help them adapt their security models to the challenges—and opportunities—presented by cloud computing, mobility, and other new ways of doing business that are driven by technology advancements.

The past year has seen organizations of all types struggling to understand how to embrace innovation without creating new security gaps or widening known ones. 2013 also brought the issue of trust to the forefront. Users of all types are now even more likely to question the trustworthiness of the technology they rely on every day whether at work or in their personal lives. It is therefore more important than ever for technology vendors to help assure customers that security is a priority in their manufacturing processes—and to be prepared to back up those assurances.

"We are in a market transition where trust matters, and process and technology must be integral features of product design for a vendor to meet the needs of today's threats," says Cisco chief security officer John N. Stewart. "A company's promise is insufficient. Firms need verification through certified products, integrated development processes, innovative technology, and respected standing in the industry. Organizations also must make it an ongoing priority to verify the trustworthiness of the technology products they use and the vendors that supply them."

Improving the alignment between security operations and business objectives is also an important measure for strengthening enterprise security. In a climate of limited resources and anemic budgets, this alignment can help CISOs and other security executives in the organization to identify key risks and appropriate mitigation approaches. Part of this process is the acceptance of the fact that not all corporate resources can be completely protected at all times. "Come to an agreement as to what is most important from a cybersecurity perspective," says Gavin Reid, director of threat intelligence for Cisco. "This is a more productive approach than hoping to find a magic pill that can fix everything."

To meet today's security challenges head on, organizations need to examine their security model holistically and gain visibility across the entire attack continuum:

- **Before an attack:** To defend their network, organizations must be aware of what's on it: devices, operating systems, services, applications, users, and more. Additionally, they must implement access controls, enforce security policies, and block applications and overall access to critical assets. However, policies and controls are only a small piece of a bigger picture. These measures can help to reduce the surface area of attack, but there will always be gaps that attackers will find and exploit to achieve their objectives.
- **During an attack:** Organizations must address a broad range of attack vectors with solutions that operate everywhere that a threat can manifest itself—on the network, on endpoints, from mobile devices, and in virtual environments. With effective solutions in place, security professionals will be better positioned to block threats and help to defend the environment.
- **After an attack:** Invariably, many attacks will be successful. This means organizations need to have a formal plan in place that will allow them to determine the scope of the damage, contain the event, remediate, and bring operations back to normal as quickly as possible.

> "Attackers and their tools have advanced to evade traditional defenses. The reality is that it's no longer a matter of if attackers get in, but when," says Marty Roesch, chief security architect for the Security Group at Cisco. "A visibility-driven and threat-focused approach to security is needed to protect users across the attack continuum—before, during, and after an attack."

How Services Help Meet Security Challenges

With a greater attack surface, the increasing proliferation and sophistication of attack models, and the growing complexity within the network, more organizations are struggling to solidify a security vision that uses new technologies, simplifies their architecture and operations, and strengthens their team.

Lack of security talent, as discussed on page 60, complicates these issues. In addition, the security industry is innovating faster than organizations can adopt and operationalize these new tools.

Finding the right talent to address the evolving security landscape effectively can be a challenge. Bringing in complementary outside resources can not only help to reduce costs, but also allow the business to free up resources to focus on higher priorities.

Strengthening the Chain Where It Weakens

Preventing threats is of course paramount to maintaining cybersecurity. This is why, with more online criminals shifting their focus toward compromising the Internet's infrastructure instead of individual computers, Cisco security experts recommend that ISPs and hosting companies take a more active role in helping to protect the integrity of the Internet.

Identifying difficult-to-detect threats like DarkLeech and Linux/CDorked (see page 45) requires much more "human responsiveness" on the part of hosting providers. Such responsiveness includes fully investigating reports from users and taking them seriously. Providers also need to establish better controls to make sure they can verify the integrity of their server operating system installations. Cisco investigators say that with stealthy malware like CDorked, security teams would have had no way of knowing that the binary had been replaced if a control had not already been in place to verify the integrity of the installation.

Systems of individual users are susceptible to compromise, of course, but the weakening in the chain often begins long before a threat reaches them. More often now, the attack happens in the middle of the chain, which is why providers need to have better awareness about potential threats that target the Internet's infrastructure.

Appendix

Security Organizations Need Data Scientists

Introductory Data Analysis Tools for Security Practitioners

Chief security officer (CSO) teams are collecting an unprecedented amount of data, and the intelligence captured in that data is much too valuable to go unused. Analyzing security-relevant data provides clues into attackers' activities and gives actionable insight into how to thwart attacks.

Data analysis is not new to the security practitioner. There is also an expectation among security practitioners that records will be generated and labeled. Pen-testers create a record of investigation after an assessment. Operating system designers implement auditing subsystems. Application developers design applications that generate logs.

Regardless of what the records are called, one thing is certain: Security practitioners have a great deal of data—and analyzing that data can lead to important discoveries.

Security practitioners have a great deal of data—and analyzing that data can lead to important discoveries.

While data analysis itself is not new, the evolution of the security landscape has had an impact on the process of data analysis:

- The sheer volume of data generated is staggering.
- The frequency with which ad hoc data analysis is needed is increasing.
- Standardized reports, while helpful, are insufficient.

Fortunately, the barrier to entry for security practitioners to do data analysis, even in this more complex environment, is low—and the data analysis tools ecosystem is rich. Following is an overview of just some of the freely available tools that practitioners can use to start analyzing data.

Analyzing Traffic with Wireshark and Scapy

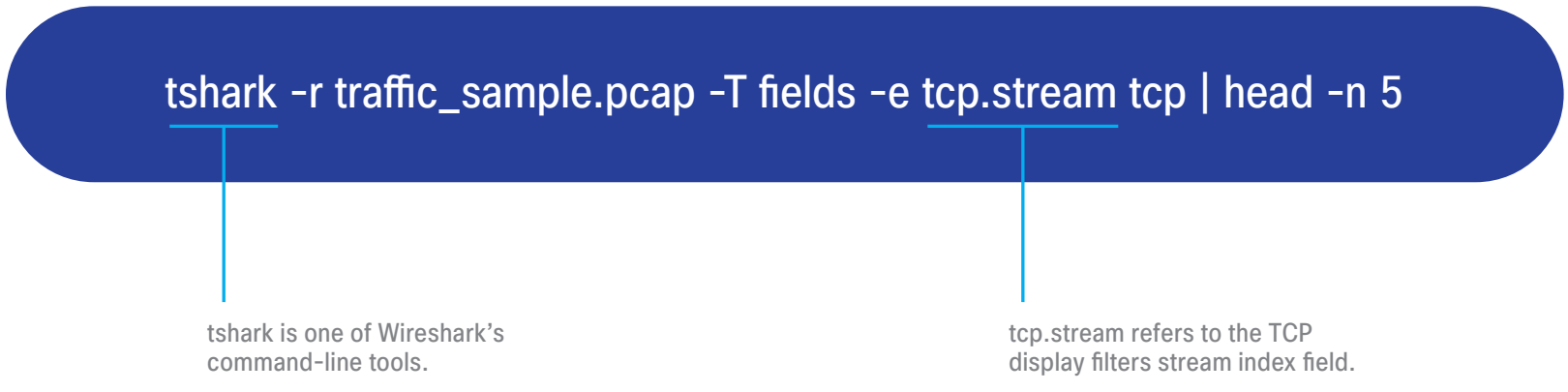
Two tools that excel in doing traffic analysis are Wireshark and Scapy. Wireshark needs no introduction. Scapy is a Python-based tool that can be used, either as a Python module or interactively, for crafting or inspecting traffic.

Wireshark's rich set of command-line tools and protocol dissectors make it indispensable. For example, with the use of Wireshark's tcp.stream display filter field, a pcap file containing multiple TCP streams can be broken into smaller files that each contain all the packets belonging to a single TCP stream.

Figure A1 shows this command that prints the TCP stream index of the first five TCP packets in traffic_sample.pcap.

FIGURE A1

The tshark Command to Extract the tcp.stream Index



With that knowledge, one can write a script that will split traffic_sample.pcap into individual pcap files:

```
$ cat ~/bin/uniq_stream.sh
#!/bin/bash

function getfile_name() {

                orig_name=$1
                stream=$2
                file_name="$(echo $orig_name | cut -d'.' -f1)"
                file_name+="-${stream}.pcap"

                echo "${file_name}"

                return 0
}

streams=$(tshark -r ${1} -T fields -e tcp.stream | sort -un | tr '\n' ' ')

for x in ${streams}
do
                file_name=$(getfile_name ${1} ${x})
                echo "Creating ${file_name}..."
                tshark -r ${1} -w $file_name tcp.stream eq ${x}
done
$
```

The script creates a single pcap file for each of the 147 TCP streams in traffic_sample.pcap. It is now easier to do further analysis on each TCP stream. Note that non-TCP packets from traffic_sample.pcap will not be in any of the new pcap files:

```
$ /bin/uniq_stream.sh traffic_sample.pcap
Creating traffic_sample-1.pcap...
Creating traffic_sample-2.pcap...
...
...
Creating traffic_sample-146.pcap...
Creating traffic_sample-147.pcap...
```

Scapy has its own strengths. Since it is developed in Python, all the features of the Python language and other Python tools can be used. The following snippet demonstrates how Scapy makes use of operator overloading so that crafting traffic can be done rapidly and intuitively:

```
# scapy
>>> dns_query = IP()/UDP()/DNS()
>>> from socket import gethostbyname,gethostname
>>> dns_query[IP].src = gethostbyname(gethostname())
>>> dns_query[IP].dst = “8.8.8.8”
>>> import random
>>> random.seed()
>>> dns_query[UDP].sport = random.randint(0, 2**16)
>>> dns_query[DNS].id = random.randint(0, 2**16)
>>> dns_query[DNS].qdcount = 1
>>> dns_query[DNS].qd = DNSQR(qname=“www.cisco.com”)
>>> scapy.sendrecv.sr1(dns_query)
>>> response = scapy.sendrecv.sr1(dns_query)
Begin emission:
.....Finished to send 1 packets.
.*
Received 14 packets, got 1 answers, remaining 0 packets
>>> response[DNS].ar[DNSRR].rdata
‘64.102.255.44’
>>>
```

This example shows how packets can be constructed and how live traffic can be analyzed. However, Scapy can be used to analyze pcap files just as easily.

Analyzing CSV Data

Comma-separated values (CSV) is a popular format for exchanging data. Many tools (including tshark) allow the user to export data in CSV format. Typically, security practitioners use spreadsheet programs like Excel to analyze CSV data. It is also often possible to use command-line tools like grep, cut, sed, awk, uniq, and sort.

Consider using csvkit as an alternative. Csvkit provides several utilities that make it easier to process CSV data from the command line. Examine the following CSV file and notice how easy it is to find all lines that have the tty.example.org host in the src column:

```
$ head -n 3 tcp_data.csv
src,srcport,dst,dstport
“tty.example.org”,“51816”,”vex.example.org”,”443”
“vex.example.org”,”443”,”tty.example.org”,”51816”

$ csvgrep -n tcp_data.csv
                1: src
                2: srcport
                3: dst
                4: dstport

$ csvgrep -c 1 -r ‘tty\.example\.org’ tcp_data.csv | head -n 5
src,srcport,dst,dstport
tty.example.org,51816,vex.example.org,443
tty.example.org,51816,vex.example.org,443
tty.example.org,51427,paz.example.org,5222
tty.example.org,51767,bid.example.org,80
```

Csvkit includes a host of utilities. Csvstat is particularly useful as it automatically computes various statistics. For example, it is easy to compute the frequency of the top five src hosts:

```
$ csvstat -c 1 tcp_data.csv
  1. src
  <type 'unicode'>
  Nulls: False
  Unique values: 55
  5 most frequent values:
                tty.example.org:        2866
                lad.example.org:        1242
                bin.example.org:        531
                trw.example.org:        443
                met.example.org:        363
Max length: 15

Row count: 6896
```

Matplotlib, Pandas, IPython, and Others

A rich set of Python-based data analysis and visualization tools is available. A great place to discover these tools is the SciPy site (http://www.scipy.org). Of particular interest are the Matplotlib, pandas, and IPython packages:

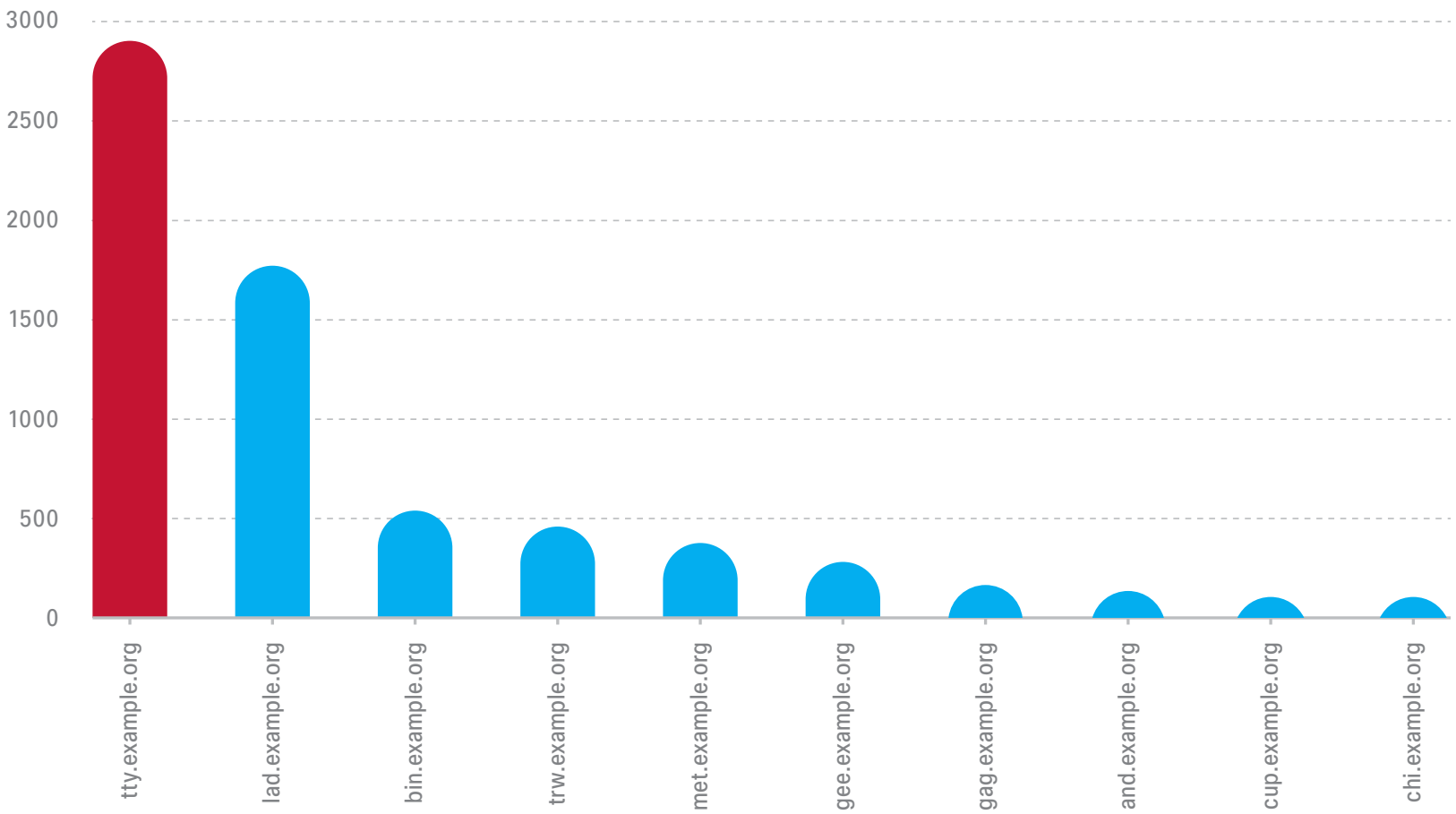
- Matplotlib allows for easy, flexible and visualization.
- Pandas provides tools to manipulate and examine raw data.
- IPython brings features to the Python interpreter that facilitate interactive data analysis.

The following demonstrates how security practitioners can use these three tools to graph the top src hosts in tcp_data.csv:

```
In [3]: df = read_csv("/Users/shiva/tmp/data_analysis/tcp_data.csv")
In [4]: df
Out[4]:
<class 'pandas.core.frame.DataFrame'>
Int64Index: 6896 entries, 0 to 6895
Data columns (total 4 columns):
src 6896 non-null values
srcport 6896 non-null values
dst 6896 non-null values
dstport 6896 non-null values
dtypes: int64(2), object(2)
In [5]: df['src'].value_counts()[0:10]
Out[5]:
tty.example.org 2866
lad.example.org 1242
bin.example.org 531
trw.example.org 443
met.example.org 363
gee.example.org 240
gag.example.org 126
and.example.org 107
cup.example.org 95
chi.example.org 93
dtype: int64
In [6]: df['src'].value_counts()[0:10].plot(kind="bar")
Out[6]: <matplotlib.axes.AxesSubplot at 0x8479c30>
```

FIGURE A2

Chart Generated Using Plot ()



The beauty of pandas is in how it allows users to explore data. For example, it takes little effort to find the number of unique srcports that tty.example.org connects from for each unique dst and dstport combination it communicates with:

```
In [229]: tty_df = df[df.src == “tty.example.org”]
In [230]: num_ports = lambda x: len(set(x))
In [231]: pivot_table(tty_df, rows=[‘dst’,‘dstport’], values=‘srcport’, aggfunc=num_ports)
Out[231]:
dst dstport
add.example.org 80 2
ala.example.org 80 3
and.example.org 80 1
auk.example.org 80 2
bid.example.org 80 1
…
```

Start Analyzing Data

The examples on the previous pages are barely a drop in the ocean and do not do justice to the tools referenced. However, they are enough for security practitioners to start performing meaningful data analysis.

CSOs need to have their security practitioners wear data scientist hats. Diving into available data will yield insights that are not otherwise possible. Over time, intuition about what parts of the data to explore will develop. Some organizations may even find they can benefit from having dedicated data scientists on their teams.

About Cisco SIO

Cisco SIO

It has become an increasingly difficult challenge to manage and secure today's distributed and agile networks.

Online criminals are continuing to exploit users' trust in consumer applications and devices, increasing the risk to organizations and employees. Traditional security, which relies on the layering of products and the use of multiple filters, is not enough to defend against the latest generation of malware, which spreads quickly, has global targets, and uses multiple vectors to propagate.

Cisco stays ahead of the latest threats by using real-time threat intelligence from Cisco Security Intelligence Operations (SIO). Cisco SIO is the world's largest cloud-based security ecosystem, using more than 75 terabits of live data feeds from deployed Cisco email, web, firewall, and intrusion prevention system (IPS) solutions.

Cisco SIO weighs and processes the data, automatically categorizing threats and creating rules using more than 200 parameters. Security researchers also collect and supply information about security events that have the potential for widespread impact on networks, applications, and devices. Rules are dynamically delivered to deployed Cisco security devices every three to five minutes.

Traditional security is not enough to defend against the latest generation of malware.

The Cisco SIO team also publishes security best practice recommendations and tactical guidance for thwarting threats. Cisco is committed to providing complete security solutions that are integrated, timely, comprehensive, and effective—enabling holistic security for organizations worldwide. With Cisco, organizations can save time researching threats and vulnerabilities and focus more on taking a proactive approach to security.

For early warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions, please visit www.cisco.com/go/sio.

Endnotes

1 For more on the any-to-any evolution, see "The Nexus of Devices, Clouds, and Applications" in the *Cisco 2013 Annual Security Report*: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

2 Ibid.

3 *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*, by John Kindervag, Forrester, Nov. 12, 2012.

4 "Timeline of Edward Snowden's Revelations," *Al Jazeera America*: http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html.

5 "NSA collecting phone records of millions of Verizon customers daily," by Glenn Greenwald, *The Guardian*, Jun. 5, 2013: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

6 GCHQ: Government Communications Headquarters, a British intelligence agency.

7 "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," by Barton Gellman and Ashkan Soltani, Oct. 30, 2013, *The Washington Post*: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

8 For more information, see "Cisco Secure Development Life cycle (CSDL)": http://www.cisco.com/web/about/security/cspo/csdl/index.html.

9 Ibid.

10 Cisco defines the Internet of Everything as "the next wave of dramatic Internet growth that will come through the confluence of people, process, data and things."

11 "Massive Spam and Malware Campaign Following the Boston Tragedy," *Cisco Security Blog*, Apr. 17, 2013: http://blogs.cisco.com/security/massive-spam-and-malware-campaign-following-the-boston-tragedy/.

12 Ibid.

13 Ibid.

14 Java website "About" page: http://www.java.com/en/about/.

15 To learn more about the "any-to-any evolution," see the *Cisco 2013 Annual Security Report*: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

16 "Department of Labor Watering Hole Attack Confirmed to be 0-Day with Possible Advanced Reconnaissance Capabilities," by Craig Williams, *Cisco Security Blog*, May 4, 2013: http://blogs.cisco.com/security/department-of-labor-watering-hole-attack-confirmed-to-be-0-day-with-possible-advanced-reconnaissance-capabilities/.

17 "Watering-Hole Attacks Target Energy Sector," by Emmanuel Tacheau, *Cisco Security Blog*, Sept. 18, 2013: http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/.

18 "Apache DarkLeech Compromises," by Mary Landesman, *Cisco Security Blog*, Apr. 2, 2013: http://blogs.cisco.com/security/apache-DarkLeech-compromises/.

19 "Ongoing malware attack targeting Apache hijacks 20,000 sites," by Dan Goodin, *Ars Technica*, Apr. 2, 2013: http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/.

20 "Linux/CDorked FAQS," by Mary Landesman, *Cisco Security Blog*, May 1, 2013: http://blogs.cisco.com/security/linuxcdorked-faqs/.

21 "DarkLeech Apache Attacks Intensify," by Matthew J. Schwartz, *InformationWeek*, Apr. 30, 2013: http://www.informationweek.com/security/attacks/DarkLeech-apache-attacks-intensify/240153922.

22 Typosquatting is the practice of registering domain names that are one character different from a popular domain name.

23 "Thanks to IoE, the next decade looks positively 'nutty,'" by Dave Evans, *Cisco Platform Blog*, Feb. 12, 2013: http://blogs.cisco.com/news/thanks-to-ioe-the-next-decade-looks-positively-nutty/.

[24] For more information about mitigation strategies for bitsquatting, read the Cisco white paper, *Examining the Bitsquatting Attack Surface*, 2013: http://blogs.cisco.com/wp-content/uploads/Schultz-Examining_the_Bitsquatting_Attack_Surface-whitepaper.pdf.

[25] "WordPress Sites in the World" and "A Look at Activity Across WordPress.com," WordPress.com: http://en.wordpress.com/stats/.

[26] "Important Security Update: Reset Your Drupal.org Password," Drupal.org, May 29, 2013: https://drupal.org/news/130529SecurityUpdate.

[27] A detailed report of the patterns and payloads of the Operation Ababil campaign can be found in "Cisco Event Response: Distributed Denial of Service Attacks on Financial Institutions": http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[28] "DDoS Attack on Bank Hid $900,000 Cyberheist," by Brian Krebs, *KrebsonSecurity* blog, Feb. 19, 2013: http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[29] "Chinese Internet Hit by Attack Over Weekend," by Paul Mozer, *China Real Time Report*, WSJ.com, Aug. 26, 2013: http://blogs.wsj.com/chinarealtime/2013/08/26/chinese-internet-hit-by-attack-over-weekend/.

[30] Source: Wikipedia: "Ingress Filtering": http://en.wikipedia.org/wiki/Ingress_filtering.

[31] "Understanding Unicast Reverse Path Forwarding," Cisco website: http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html.

[32] "Your Hard Drive Will Self-Destruct at 2 p.m.: Inside the South Korean Cyberattack," by Sean Gallagher, *Ars Technica*, Mar. 20, 2013: http://arstechnica.com/security/2013/03/your-hard-drive-will-self-destruct-at-2pm-inside-the-south-korean-cyber-attack/.

[33] "Thoughts on DarkSeoul: Data Sharing and Targeted Attackers," by Seth Hanford, *Cisco Security Blog*, Mar. 27, 2013: http://blogs.cisco.com/tag/darkseoul/.

[34] Ibid.

[35] "Cyber Gang Seeks Botmasters to Wage Massive Wave of Trojan Attacks Against U.S. Banks," by Mor Ahuvia, RSA, Oct. 4, 2012: https://blogs.rsa.com/cyber-gang-seeks-botmasters-to-wage-massive-wave-of-trojan-attacks-against-u-s-banks/.

[36] "DDoS Attack on Bank Hid $900,000 Cyberheist," by Brian Krebs, *KrebsonSecurity* blog, Feb. 19, 2013: http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[37] "Cisco projects data center-cloud traffic to triple by 2017," ZDNet, Oct. 15, 2013: http://www.zdnet.com/cisco-projects-data-center-cloud-traffic-to-triple-by-2017-7000021985/.

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**.