



Cisco 2014 Midyear
Security Report



Executive Summary

Any cyberattack, large or small, is born from a weak link in the security chain. Weak links can take many forms: outdated software, poorly written code, an abandoned website, developer errors, a user who blindly trusts. Adversaries are committed to finding these weak links, one and all, and using them to their full advantage.

Unfortunately, for the organizations and users targeted, malicious actors do not have to look long or hard for those weaknesses. In the rapidly emerging Internet of Everything, which ultimately builds on the foundation of the connectivity within the Internet of Things, their work will be made even easier, as anything connected to a network, from automobiles to home automation systems, presents an attack surface to exploit.

The effects of cyberattacks are sobering, in terms of both costs and losses in productivity and reputation. According to the Ponemon Institute, the average cost of an organizational data breach was US\$5.4 million in 2014, up from US\$4.5 million in 2013. In addition, the Center for Strategic and International Studies' *Estimating the Cost of Cyber Crime and Cyber Espionage* report estimates that US\$100 billion is lost annually to the U.S. economy, and as many as 508,000 U.S. jobs are lost, because of malicious online activity.¹





Threat Intelligence

[Go to Threat Intelligence](#)

The **Cisco 2014 Midyear Security Report** examines threat intelligence and cybersecurity trends for the first half of 2014. Cisco's research helps to underscore just how many different types of weak links exist in the systems we use, including the Internet itself, and what can be done to reduce their number and effects. Key findings include:

As part of Cisco's ongoing "Inside Out" project examining Domain Name System (DNS) queries—or the process of looking up the Internet Protocol (IP) address associated with a domain name—originating from inside the corporate networks of select Cisco customers, researchers observing the networks of 16 large multinational organizations found that:

Nearly 70 percent of select customer networks observed by Cisco researchers have been identified as issuing DNS queries for Dynamic DNS (DDNS).

More than 90 percent of select customer networks have been identified as issuing DNS requests for hostnames associated with the distribution of malware.

More than 40 percent of select customer networks have been identified as issuing DNS requests for sites and domains associated with devices that provide services such as IP Security (IPsec) VPN, Secure Sockets Layer (SSL) VPN, Secure Shell (SSH) Protocol, Simple File Transfer Protocol (SFTP), FTP, and FTP Secure (FTPS).

Of the 2528 vulnerability alerts published from January to June 2014, 28 were identified as being actively exploited. These are the high-priority or urgency vulnerabilities that need to be patched using an accelerated response.

After an overall decline in 2013, global spam volume has been on the rise since last October, but not all countries are seeing an increase.



Industry Trends

[Go to Industry Trends](#)

For the first half of 2014, the pharmaceutical and chemical industry, a high-profit vertical, once again places in the top three high-risk verticals for web malware encounters.

The media and publishing industry has experienced a significantly higher than normal rate of web malware encounters than previously observed.

2014 appears to be an active year for Network Time Protocol (NTP) distributed denial of service (DDoS) attacks. One of the most significant NTP amplification attacks observed in the first six months of 2014 targeted a customer of global DNS provider, CloudFlare. At its peak, the February attack reached nearly 400 Gbps of User Datagram Protocol (UDP) traffic.

The number of exploit kits has dropped by 87 percent since the coder, Paunch, the alleged creator of the widely popular Blackhole exploit kit, was arrested last year, according to Cisco security researchers.

Several exploit kits observed in the first half of 2014 were trying to move in on territory once dominated by the Blackhole exploit kit, but a clear leader has yet to emerge.

Point-of-sale (POS) exploits are gaining favor with criminals in 2014 for several reasons:

The increasing likelihood that POS systems are connected to the Internet, providing criminals with a point of entry to corporate networks.

Lack of understanding that payment card information should be considered critical data, which means it is less protected.

Organizations' growing use of third-party vendors for all or part of their POS solutions, providing more access points for criminals.



A Look Forward

[Go to A Look Forward](#)

Security risks the Internet of Things is likely to create and why organizations should take a proactive approach to address them.

The value of using predictive analytics and machine learning to help identify hard-to-detect threats on the network.

A trend among organizations toward viewing cybersecurity as both a strategic risk and a business process.

The need for visibility-driven, threat-focused, and platform-based security solutions that cover the entire attack continuum before, during, and after an attack and help to close security gaps and reduce complexity caused by disparate products.



Table of Contents

Introduction	7
The Internet of Things: New Opportunities, New Risks	7
Threat Intelligence	9
A Paradigm Shift in Compromise: Looking Inside Out	10
Geopolitical Trends to Watch	14
Web Exploits: Java Exploits Continue to Dominate	15
Vulnerabilities Update: Focusing on the Most Common Exploits	17
Heartbleed: Not the Only Cause for Worry	20
Industry Vertical Risk Report: Unusual Upticks for Some Sectors	21
Malware Encounters by Region	23
Top 5 Risk Verticals by Region	25
Spam Update: "Life Event" Spam Becomes More Prevalent	26
Spammers Become More Agile, Change Approaches to Improve Success	26
Global Spam Volume Up by Twice the Normal Rate, But Some Countries See Sharp Decline	27
Industry Trends	28
Compromised Secure Encrypted Connections	29
Amplification Attacks: Adversaries Clocking in with NTP	31
Exploit Kits: The Field Opens Up to Competition	33
Malvertising: A Disruptor for the Internet Economy	35
Really Bad Ads: Malvertising's Role in Ransomware	36
WordPress Vulnerabilities: Who Is Minding the Store?	37
POS Attacks: Popular Threat Vector for Criminals Seeking Payment Card Data	38
More Critical Monitoring of Payment Card Data	39
Social Engineering: Finding the Weak Links in Person	40
A Look Forward	42
Intelligent Cybersecurity for the Real World	43
Operationalizing Security: Making Security a Business Process	45
Understanding Cyber Risk in Business Terms	47
Predictive Analytics: A Detective That Enables Better Security	49
About Cisco	50
Endnotes	51

This document contains searchable and shareable content



Click to open Find feature in Adobe Acrobat



Share content through email and social media

Recommended software:

Adobe Acrobat Version 7.0 and above



The Internet of Things: New Opportunities, New Risks

The Internet of Things “is the network of physical objects accessed through the Internet, as defined by technology analysts and visionaries. These objects contain embedded technology to interact with internal states or the external environment. In other words, when objects can sense and communicate, it changes how and where decisions are made, and who makes them.”²

The Internet of Things is expected to grow to approximately 50 billion things by 2020, according to Cisco.³ It is already changing the security landscape, exponentially expanding the attack surface. The Internet of Things magnifies the importance of continuous and pervasive detection and protection as people, processes, and data all become increasingly connected.

In this rapidly evolving world of pervasive computing and extreme interconnectedness, anything connected to a network presents an attack surface for adversaries to exploit. Much of what attackers *could* do is still hypothetical, but they are already making plans, testing ideas, and finding some success.

Cars, medical devices, and even baby monitors have all been recent targets for Internet of Things “research and development” by hackers.⁴⁻⁶

The ultimate goal of the Internet of Things is to increase operational efficiency, power new business models, and improve quality of life. By connecting everyday objects and networking them together, we benefit from their ability to combine simple data to produce usable intelligence. But that also means there is greater potential that more personal information and business data will exist in the cloud and be passed back and forth. With that come significant implications for applying proper security to protect data and for establishing privacy policies to address how data is used.

Privacy is a significant concern in the Internet of Things. Even when users take precautions to secure their information and refrain from being too trusting, they are still at risk because of weak links in the security chain that are beyond their control (see [Compromised Secure Encrypted Connections](#), page 29). When adversaries reach a point where they can begin correlating information from different sources—a car, a smartphone, a home automation system—they will be able to gain a much bigger picture about a user than if they were looking at information from only one device, system, or application. These details about users, from their shopping habits to their physical location, will allow actors to launch well-crafted, highly targeted campaigns at a level of sophistication never before seen.





To some, it might seem far-fetched to think something as mundane as a wearable device for tracking fitness or a digital video recorder (DVR) could pose a significant security risk or would be of any interest to a hacker. But as cars and other nontraditional computing devices start to resemble standard computing platforms more and more, they could be vulnerable to the same threats⁷ that target traditional computing devices.

Leading vendors are aware of security issues in Internet of Things devices and have the background and experience to make sure security is architected into their products. Emerging companies can use lessons learned by the cybersecurity industry over the past 20 years and try to avoid making similar mistakes as they innovate. Many of the same best practices that apply to general purpose computers do and will apply to Internet of Things devices: installing the latest software, for example. But in the Internet of Everything world to which the Internet of Things is leading us, security will be managed largely by systems, not users, so industry will also need to take that into consideration when designing secure technology for this emerging environment. This includes ensuring transparency for users so they can be assured that Internet of Things devices are maintaining their security automatically or will know when manual action might be required.

There will always be one more new thing being added to the Internet ecosystem. At the same time, the population of abandoned and unmanaged Internet-connected devices will grow as well. Like the countless long-forgotten or neglected websites on the Internet today (see [WordPress Vulnerabilities: Who Is Minding the Store?](#), page 37), these devices, from kitchen appliances to surveillance cameras to personal printers, will be weak links in the security chain, providing enterprising hackers with almost limitless doorways that can be unlocked and potentially lead to the data center.

Cybercriminals' capabilities and motivations are understood; their growing focus on the Internet of Things is a natural progression. Unlike the global community's first foray into an Internet-connected world, we all have the benefit of foresight: We know from experience that the Internet of Things environment presents risk and that organizations and users will be targeted. A greater risk, now, is underestimating the industriousness of adversaries and just how quickly the Internet of Things—and Internet of Everything—are beginning to take shape.



The background of the slide is a dark blue gradient with a complex, abstract network diagram. It consists of numerous small, light blue circular nodes connected by thin, white lines, creating a web-like structure that spans the entire frame. The lines and nodes vary in opacity and brightness, giving a sense of depth and connectivity.

Threat Intelligence

Cisco security researchers have assembled and analyzed security insights for the first half of 2014 based on the largest set of telemetry data available. Cisco security experts perform ongoing research and analysis of discovered threats, such as malware traffic, which can provide insights on possible future criminal behavior and aid in the detection of threats.



A Paradigm Shift in Compromise: Looking Inside Out

Threat intelligence presented in the *Cisco 2014 Annual Security Report* included a key finding from a recent “Inside Out” project in which Cisco security researchers reviewed DNS lookups originating from inside corporate networks.⁸

Cisco security researchers found that malicious traffic was visible on 100 percent of the networks sampled.⁹

Based on the activity they observed, Cisco researchers also determined that this particular group of corporate networks reviewed likely had been penetrated for some time and that the core infiltration had not been detected.

Cisco presents some additional findings in this report from the ongoing Inside Out project. The information is based on Cisco threat researchers’ review of data analytics collected from select customer networks since the beginning of 2014. The researchers closely examined 16 large multinational organizations that collectively controlled more than US\$4 trillion in assets with revenues in excess of US\$300 billion in 2013. This analysis yielded three compelling security insights tying those enterprises to malicious traffic.



Requests for DDNS

Threat Description

DDNS is a system normally used for legitimate purposes, namely, home users who need the ability to map a static fully qualified domain name (FQDN)—for example, homeserver.isp.com—to a number or pool of IP addresses dynamically assigned by their Internet service provider (ISP).

Unfortunately, DDNS, like many technologies and features developed for legitimate use, has become popular with adversaries because it allows botnets and other attack infrastructure to be resilient against detection and subsequent destruction. Unusually large volumes of requests for domains using

DDNS service providers, such as name-services.com, might indicate potential compromise on an organization's network. Although many, and sometimes all, of an organization's queries for DDNS providers are legitimate, these requests always should be vetted to make sure that they are, in fact, legitimate.

Findings

Nearly **70 percent** (66.67 percent) of customer network sample queries observed in 2014 as part of this “Inside Out” project have been identified as issuing DNS queries for DDNS. (Note: Cisco security researchers expect to see this percentage increase over time as the sample size of customer

networks analyzed increases. Cisco has only started tracking this new category as a potential indicator of compromise [IOC]; an IOC is an event or artifact observed on a system, often subtle, that, when correlated with other IOCs for a system, points to a likely compromise.) As indicated earlier, this does

not by any means translate to each of these customers being compromised by malware that is using DDNS providers; however, Cisco has advised that these customers look more closely at these DDNS requests to make sure they are being performed for business-legitimate reasons.





Requests for Sites Associated with Malware That Incorporates MiTB Functionality

Threat Description

Palevo, SpyEye, and Zeus are malware families that incorporate man-in-the-browser (MiTB) functionality. DNS lookups for hosts compromised by Palevo, Zeus, and SpyEye are considered a very high threat. These botnets spread through

instant messaging, peer-to-peer (P2P) networks, and removable drives. They are used to perform distributed denial of service (DDoS) attacks and steal information entered into fields created in real time and added to an

existing form. Palevo, Zeus, and SpyEye are highlighted because they represent a specific class of malware that targets financial and other information entered into online forms in browsers using the Windows operating system.

Findings

More than **90 percent** (93.75 percent) of customer networks observed in 2014 have been identified as having traffic going to websites that host malware. Specifically, the networks have been identified

as issuing DNS requests for hostnames where the IP address to which the hostname resolves is reported to be associated with the distribution of, or is infected by, Palevo, Zeus, or SpyEye malware.



SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT



DNS Requests for FQDNs, Sites, and Hosts Associated with Administrative Protocols

Threat Description

Malicious entities might use secure, encrypted communication channels or data transfer protocols to cover their tracks when stealing information; some examples are IP Security (IPsec) VPN, Secure Sockets Layer (SSL) VPN, Secure Shell (SSH) Protocol, Simple File Transfer

Protocol (SFTP), FTP, and FTP Secure (FTPS). Organizations should regularly monitor and validate these communications. These types of sites can be used to exfiltrate data using encrypted channels to avoid detection.

Findings

More than **40 percent** (43.75 percent) of customer networks observed in 2014 have been identified as issuing DNS requests for sites and domains associated with devices that provide services such as IPsec VPN, SSL VPN, SSH, SFTP, FTP, and FTPS.



Cisco researchers used DNS lookups emanating from enterprise networks to create a snapshot of possible data compromises and vulnerabilities. Cisco security experts analyzed the information based on blocklists and observed trends in cyber compromises, unique vulnerabilities facing specific verticals, and geopolitical factors that might affect actors and targeted information. Cisco customers that take part in the Inside Out project receive an *External Cyber Threat Report* prepared and delivered by Cisco.



Geopolitical Trends to Watch

Geopolitical events in Eastern Europe and the Middle East are creating new trends in the cyber realm that are expanding the risk landscape for businesses, governments, and other organizations and individual users around the globe, according to Cisco cybersecurity experts:



Political instability in Ukraine ushered in a series of DDoS attacks and website defacements apparently calculated to complement actions on the ground. The disruptions in Crimea and Kiev led to the discovery of sophisticated espionage malware on Ukrainian networks (dubbed Ouroboros, or Snake), which had gone undiscovered for months or years.

In the Middle East, the overrunning of entire sections of northern and western Iraq by the Islamic State of Iraq and the Levant (ISIL, or ISIS) is being accompanied by a social media campaign for sabotage and psychological warfare.

Looking forward, long-standing ethnic and religious divisions are deepening in a part of the world that is already leading the way in the use of cyber tactics by both state and nonstate actors. In the second half of 2014, contentious presidential elections in Turkey and midterm elections in the United States, and the drawdown of Western military operations in Afghanistan are likely to create new ripple effects across the global cyber landscape.



**SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT**



Web Exploits: Java Exploits Continue to Dominate

Java programming language exploits remain the leader among IOCs monitored by the Cisco® FireAMP advanced malware detection platform. These exploits have extended their seemingly uncatchable lead in the first half of 2014.



SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT

FIGURE 1

2014 Midyear Application Compromise Share

SOURCE: Cisco® FireAMP¹⁰

Java exploits represented 91 percent of IOCs in November 2013, according to the *Cisco 2014 Annual Security Report*; that figure rose slightly to **93 percent** as of May 2014. Java's extensive attack surface and high return on investment are what make it a favorite for adversaries to exploit. (For more insight on the Java problem and tips for mitigating it, see the *Cisco 2014 Annual Security Report*¹¹).

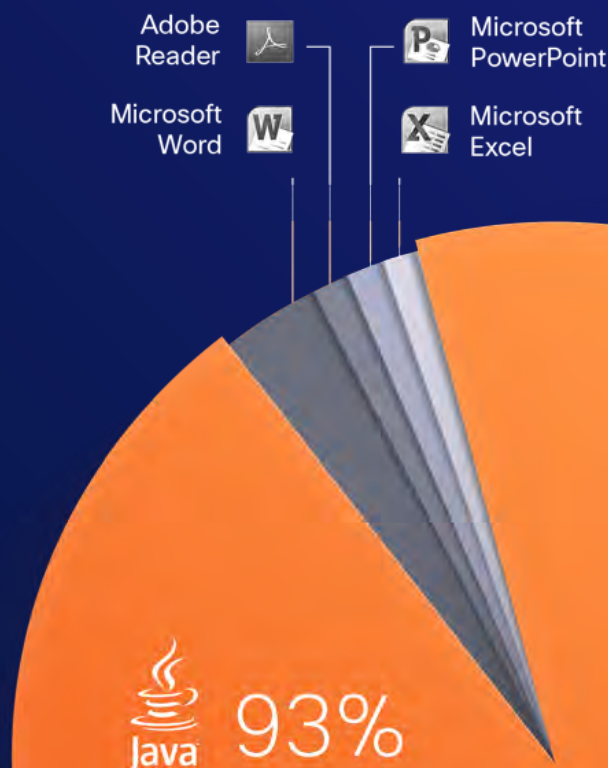




FIGURE 2

Java Web Malware Encounters (January–May 2014)

SOURCE: Cisco Cloud Web Security

Java web malware encounters peaked in March 2014, at nearly 10 percent of all web malware encountered.

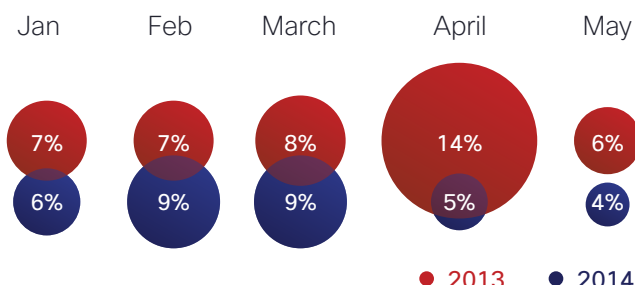


FIGURE 3

Java, PDF, and Flash Encounters (January–May 2014)

SOURCE: Cisco Cloud Web Security

Java, Flash, and Adobe PDF are all popular vectors for criminal activity.

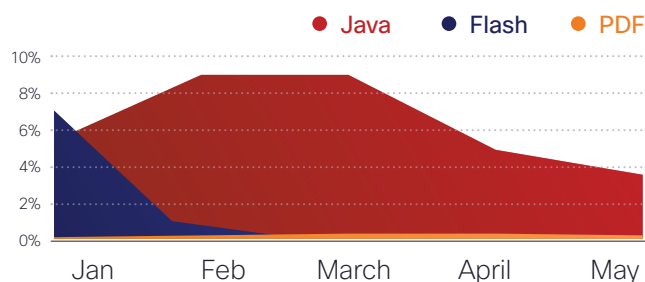
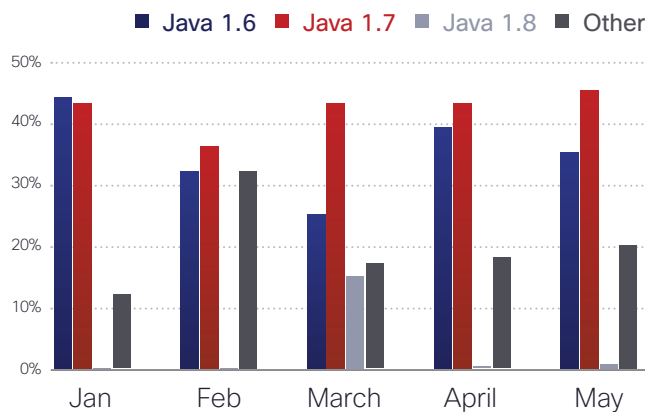


FIGURE 4

Java Encounters by Version (January–May 2014)

SOURCE: Cisco Cloud Web Security

Adversaries continue to excel at exploiting older versions of Java, particularly Java 6 and 7. There was a surge in web malware encounters with Java 8 in March, the month the new version was released. However, encounters for Java 8 dropped off significantly by April and remained very low through May. With increases in exploit kits that rely first and foremost on non-Java vectors, such as Microsoft Silverlight, we might be seeing a shift away from Java 8 (which has stronger security controls) to other software that is more conducive to attacks.





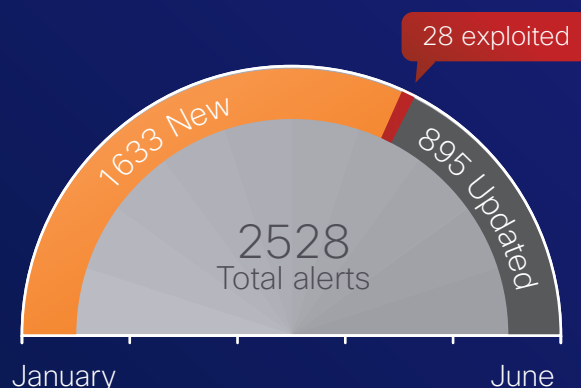
Vulnerabilities Update: Focusing on the Most Common Exploits

FIGURE 5

Alert Metrics (January–June 2014)

SOURCE: Cisco Intellishield®

From January 1, 2014, to June 30, 2014, Cisco published thousands of multivendor alerts about known security vulnerabilities. Although that number might sound intimidating, the extremely critical vulnerabilities number about 1 percent of that total. Of the 2528 new vulnerability alerts published during that time period, only 28 were being actively exploited soon after published reports, according to Cisco's research.



Adversaries cluster around common vulnerabilities or “weak links” that they prove easy to exploit through their “research and development” efforts; successful exploits are then incorporated into exploit kits sold in the underground economy. Java and Silverlight programming languages are examples of vulnerabilities that can be found in a number of popular exploit kits. (See [Web Exploits: Java Exploits Continue to Dominate](#) on page 15 and [Exploit Kits: The Field Opens Up to Competition](#) on page 33.)

As vulnerability reports are published, security practitioners and the media tend to focus on zero-day vulnerabilities because there is a seemingly urgent need to react to such high-profile news. However, organizations should prioritize their investments of time and money into patching the small number of vulnerabilities that criminals are most actively exploiting. Other vulnerabilities can be managed by more routine processes.



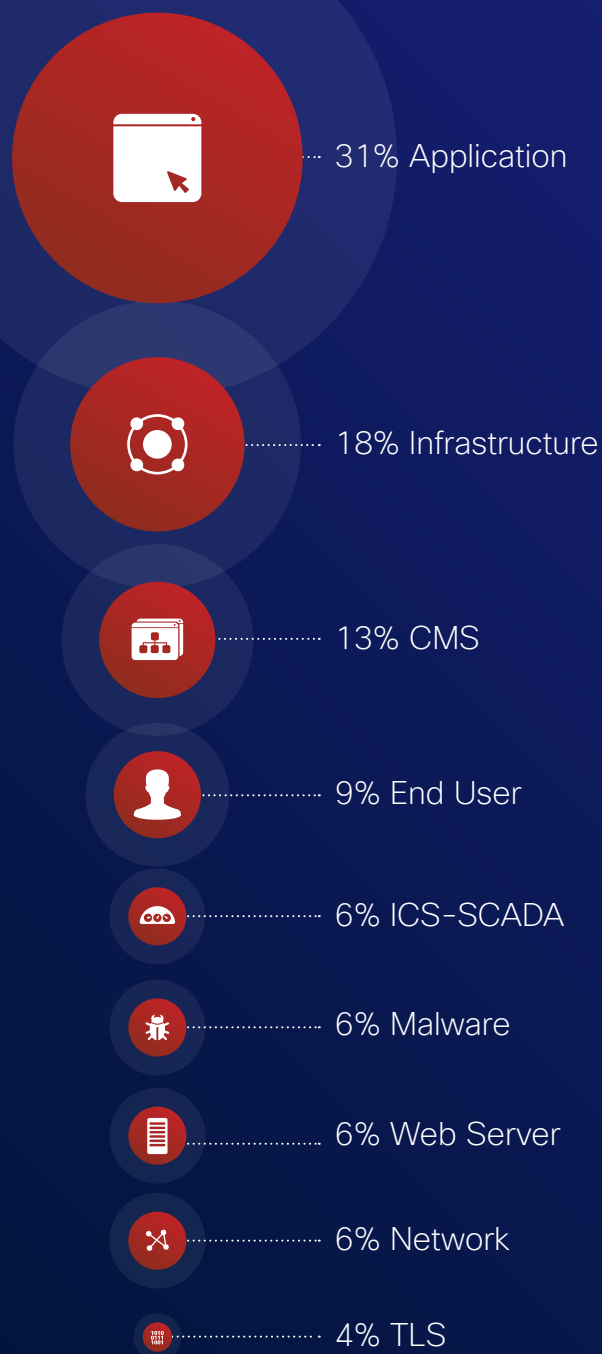
SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT



FIGURE 6

Top Products Being Exploited

SOURCE: Cisco IntelliShield®



It is good practice for organizations to have a “high-urgency patching process” that would run in tandem with their standard patching processes. By addressing targeted priority vulnerabilities quickly, other, less-urgent vulnerabilities can be integrated into the regularly scheduled maintenance and patching process. The result is more accurate risk management: better than trying to install all patches or not installing them until regularly scheduled maintenance periods. Strong security intelligence to identify high-urgency vulnerabilities is necessary to maintain a high-urgency patching process effectively.

Figure 6 shows the top products that attackers were exploiting in the first quarter of 2014. [Figure 7](#) illustrates some of the most commonly exploited vulnerabilities, according to the Common Vulnerability Scoring System (CVSS).

The “Urgency” score in the CVSS chart is useful because it indicates that these vulnerabilities are being actively exploited, which corresponds to the “Temporal” scores indicating active exploits. In addition, by scanning the list of products being exploited, enterprises can determine which of these products are in use and therefore need to be monitored and patched.

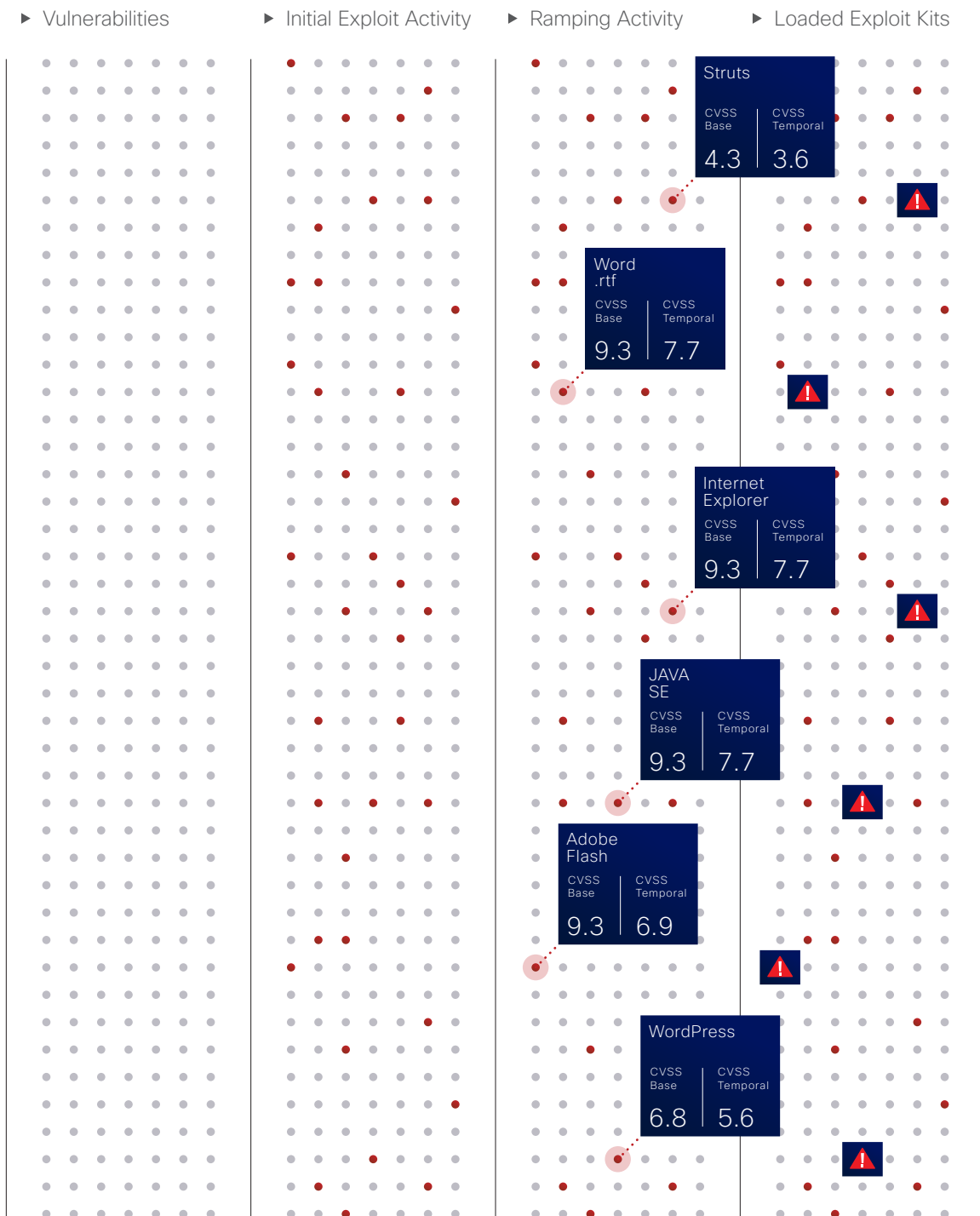
It is important to understand that the vulnerabilities in [Figure 7](#) were those showing initial signs of exploit activity during the period observed. The majority of these vulnerabilities had not yet gone “mainstream,” meaning they had not made their way into exploit kits for sale.



FIGURE 7

Most Commonly Exploited Vulnerabilities

SOURCE: Cisco IntelliShield®





Heartbleed: Not the Only Cause for Worry

Some organizations were not exposed to the “Heartbleed bug”—a security vulnerability in the OpenSSL cryptography library—because they were using an older version of OpenSSL that did not include that vulnerability.¹² The vulnerability involves the implementation of the Transport Layer Security (TLS) heartbeat extension (RFC6520) and could allow secret key or private information leakage in TLS encrypted communications.¹³

However, it is important for these organizations to note that from January to April 2014, there were 16 TLS and certificate validation vulnerabilities *not* related to Heartbleed.

These vulnerabilities might put them at risk. Cisco security experts also recommend that all users consider that they have likely been exposed to risks as a result of Heartbleed and should therefore take appropriate action, such as changing passwords or closing web accounts.¹⁴

Since Heartbleed was discovered, the OpenSSL project (OpenSSL.org) has reported several other discovered defects in OpenSSL software, some of which “can allow an attacker to create a denial of service condition, or in certain situations, remote code execution.”¹⁵ Some of these defects are long-overlooked weaknesses: for example, the CCS injection vulnerability, discovered by a security researcher in Japan, is a 16-year-old security flaw in OpenSSL software that allows an adversary to intercept and decrypt encrypted data traveling across the Internet.¹⁶





Industry Vertical Risk Report: Unusual Upticks for Some Sectors

For the first half of 2014, the pharmaceutical and chemical industry, a high-profit vertical, once again places in the top three high-risk verticals for web malware encounters; it topped the list of verticals in 2013.¹⁷ The aviation industry also appears again in the top five, this time assuming third place on the list.¹⁸ This is not surprising given the value of the intellectual property that companies in the aviation industry hold.

Meanwhile, the media and publishing industry, which currently ranks first, is experiencing significantly higher than normal rates of web malware encounters than previously observed by Cisco security researchers, who have been compiling this data since 2008.

Adversaries launching exploits and other scams around high-profile events, such as the 2014 Winter Olympic Games and the Academy Awards, and big news stories, such as the Malaysia Airlines Flight 370 mystery and the South Korean ferry disaster, are likely reasons for the increase in encounters for the media and publishing industry. Their scams are designed to prey on the human “weak link”: that is, users induced to click through to sites that host malware because they are tempted by attention-getting headlines.

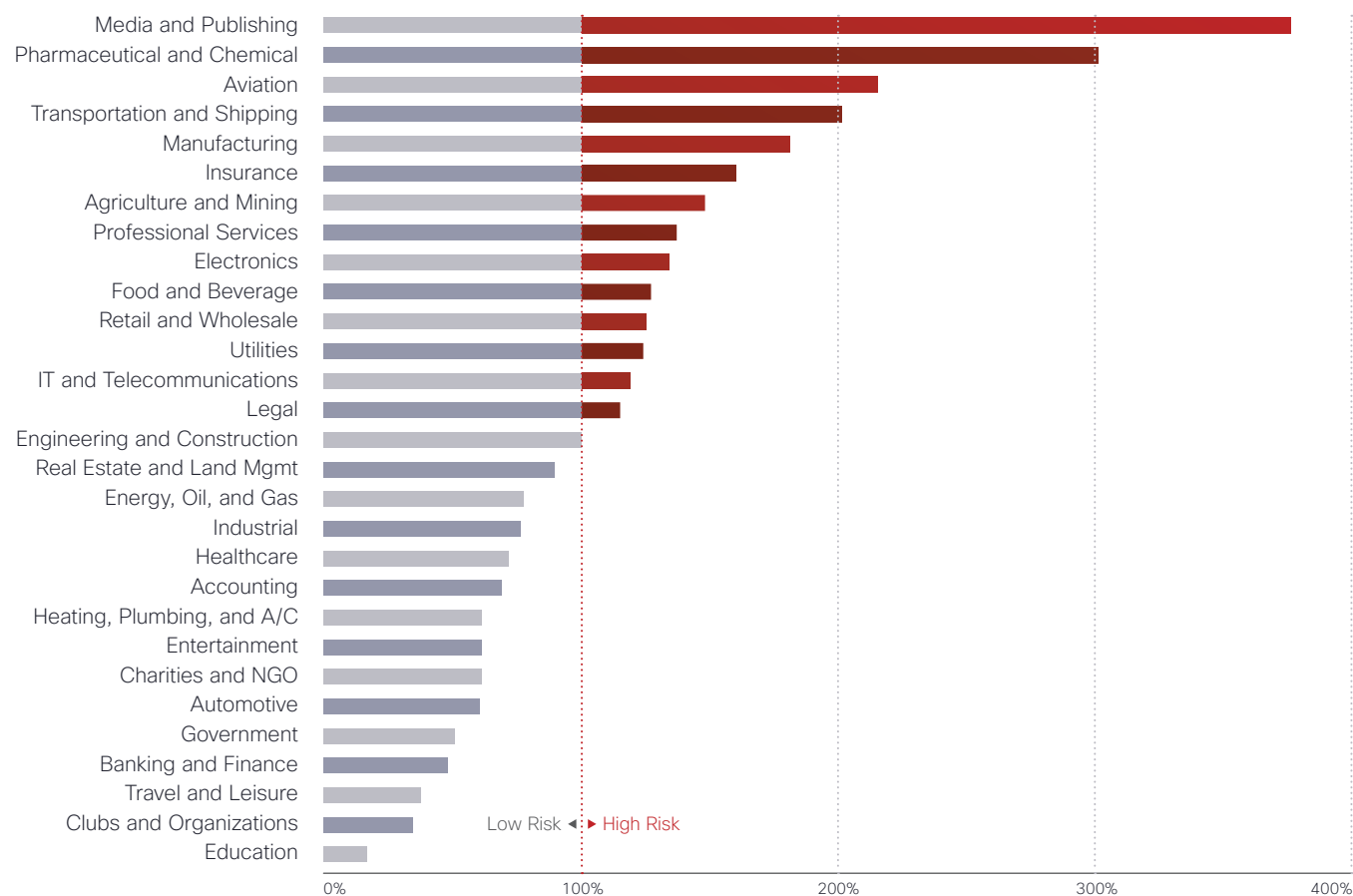
Media and publishing sites, large and small, can attract a wide range of traffic from individual consumers and organizations across the globe. They also rely largely on advertising for revenue. For that reason in particular, it is likely that growth in malvertising is partly responsible for the surge in web malware encounters for the media and publishing industry in the first half of 2014. (See [Malvertising: A Disruptor for the Internet Economy](#), page 35.)



FIGURE 8

Vertical Risk of Web Malware Encounters, 1H14

SOURCE: Cisco Cloud Web Security



To determine sector-specific malware encounter rates, Cisco security 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, 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.



Malware Encounters by Region

For the first time, Cisco security researchers are presenting web malware encounter risk data for industry verticals according to region. The three regions are defined as **AMER (North America, Central America, and Latin America)**, **APJC (Asia-Pacific, China, Japan, and India)** and **EMEAR (Africa, Europe, and the Middle East)**.

In the AMER region, as [Figure 9](#) shows, aviation outpaces other industries encountering web malware by a significant margin.

Vertical risk in a particular region will be influenced by that region's gross domestic product. Typically, the higher value of the goods and services, or intellectual property, of a particular vertical, the greater the risk of malware encounters for that industry.

A particular vertical also might be underrepresented in a region that does not typically produce in that particular sector. This is a reason for "farm-to-table" risk typically experienced by companies in the agriculture, food and beverage, and transportation industries. It is also likely why the retail food and beverage industry saw the highest number of web malware encounters in EMEAR. Recent drought, floods, and unrest in that region have all had an effect on the availability of basic supplies and infrastructure for people living in that region.

Encounter vs. Compromise

An "encounter" is an instance when malware is blocked. Unlike a "compromise," a user is not infected during an encounter because a binary is not downloaded.

In APJC, the highest risk vertical was insurance, followed by the pharmaceutical and chemical, and the electronics verticals. Recent disruptive events in the APJC region, such as the devastating earthquake, tsunami, and nuclear disaster in Japan in 2011, and subsequent tightening of the insurance market, are likely factors for the insurance industry becoming a key target for adversaries. Additionally, given the fact that the insurance industry is a supplier of services to major corporations and other entities, malicious actors might be looking to compromise insurance firms as a way to siphon sensitive information about clients or find a path to their networks and data centers.



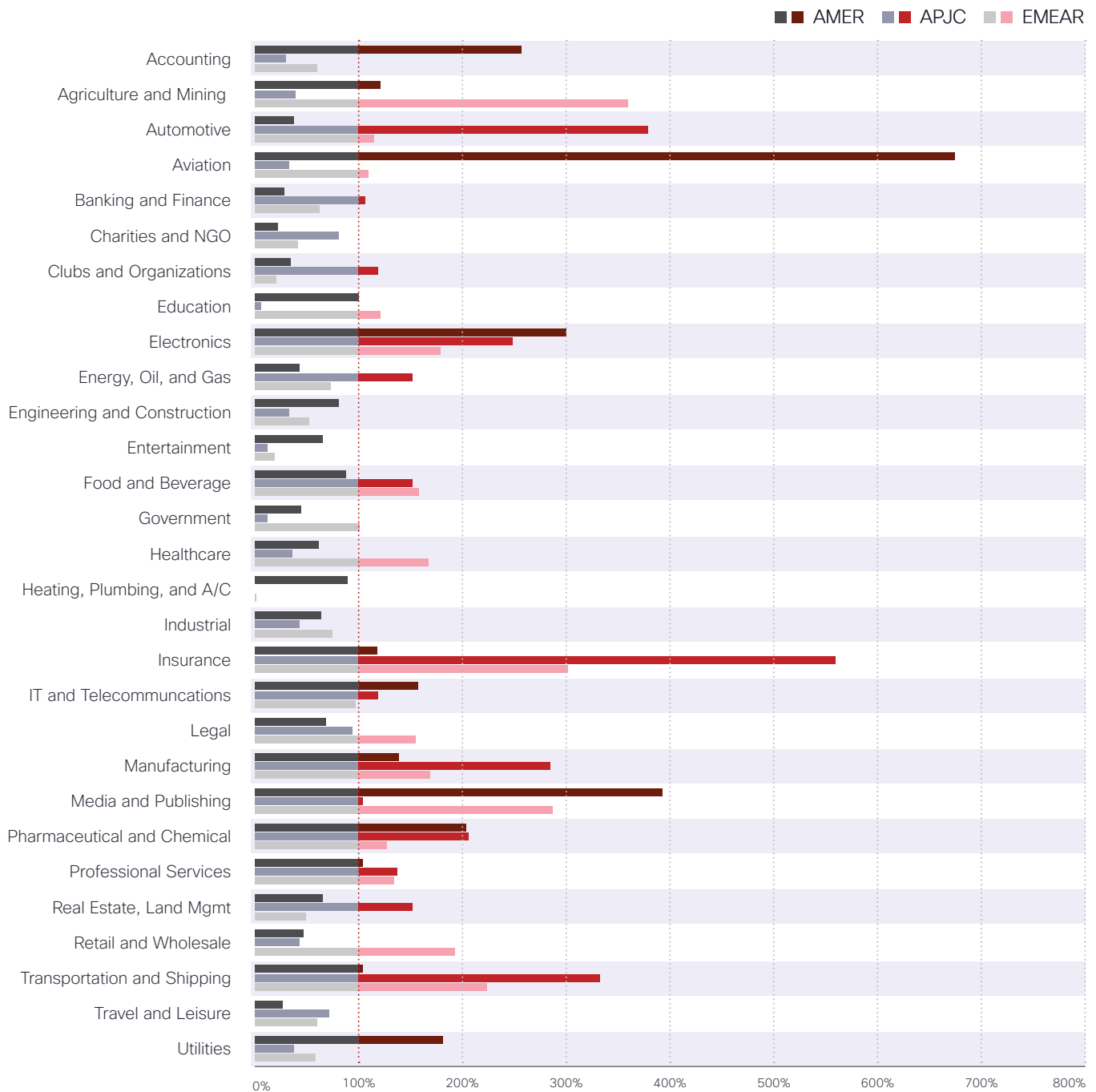
SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT



FIGURE 9

Vertical Risk of Web Malware Encounters by Region

SOURCE: Cisco Cloud Web Security





Top Five Risk Verticals by Region

Figure 10 provides a breakdown of the top five risk verticals for each region: AMER, APJC, and EMEAR. iFrames and malicious scripts dominate for all industries represented, although malicious actors in all three regions appear to be relying heavily on exploits to target specific industries. In APJC, scams, phishing, and clickfraud are used frequently to compromise the trust of users in the transportation and shipping industries.

It appears few adversaries are even attempting to target the top five risk verticals in any of the three regions with techniques such as ransomware and scareware or viruses and worms. Mobile web malware encounters are also quite low for all regions.

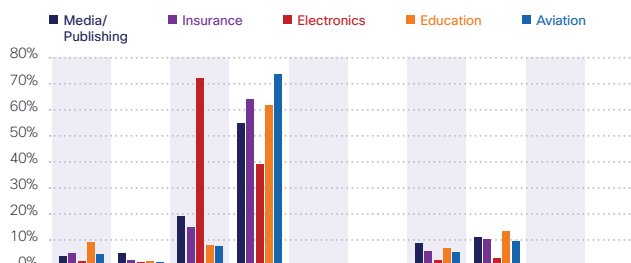
The findings in these charts are based primarily on where blocks of web malware occurred (that is, encounters), according to Cisco Cloud Web Security data, versus types of threats on the web.

FIGURE 10

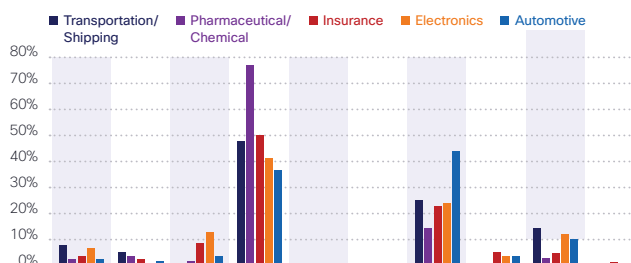
Vertical Risk of Web Malware

SOURCE: Cisco Cloud Web Security

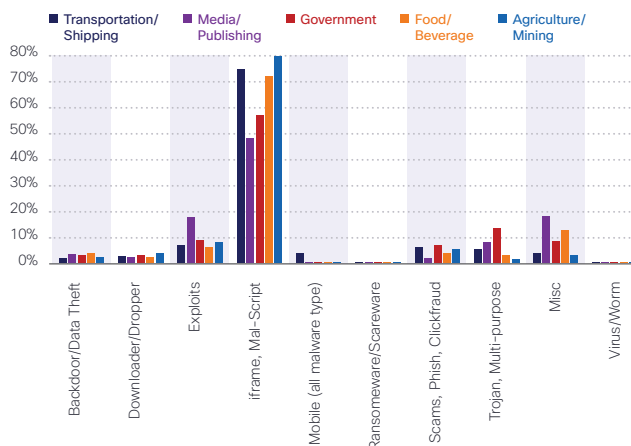
AMER



APJC



EMEAR



SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT



Spam Update: “Life Event” Spam Becomes More Prevalent

Spam creators have traditionally relied on social engineering trickery to convince recipients to open their messages and click through on links, usually leading to malware or compromised websites. Fake package deliveries or spurious urgent tax matters are common ploys, but security professionals now see a trend toward “life event” or “misfortune” spam, which uses emotion to obtain results.

For example, “life event” spam might highlight treatment or recovery from a life-threatening illness, and “misfortune” spam might mention eviction or bankruptcy. Both can exert a powerful pull on a recipient to click the message, much more so than a message about an express parcel delivery.

“Life event” and “misfortune” spam preys on a common weak link in security protections: the user, who, even with training on social engineering, is inclined to respond to a pitch about easing personal misfortunes.

As with combating any spam campaign, the key to mitigating life event spam is through the use of spam-blocking technology that can be updated dynamically.

Spammers Become More Agile, Change Approaches to Improve Success

Spammers are quick to react to technology advances that block their messages. They will adjust text, images, and domain names to dodge spam filters. And when efficacy of the message drops, they will make changes all over again.

Cisco security researchers monitor types of spam and how messages evolve in order to inform customers of new tactics by spammers looking to gain entry into networks or steal information. In some cases, coverage notes for a specific type of spam—such as a fake notice about an electronic payment—might be updated dozens of times by Cisco researchers as spammers change tactics.



Global Spam Volume Up by Twice the Normal Rate, But Some Countries See Sharp Decline

FIGURE 11

Global Spam Volume (January 2014–May 2014)

SOURCE: Cisco Threat Intelligence Platform

After an overall decline in 2013, global spam volume has been on the rise since last October. According to Cisco research, spam volumes have increased to the point that spam is now at its highest level since late 2010. From June 2013 to January 2014, spam was averaging from 50 billion to 100 billion messages per month. However, as of March 2014, volumes were peaking above 200 billion messages per month, two times above normal rates.¹⁹

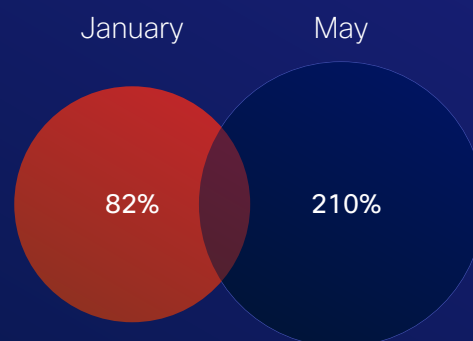
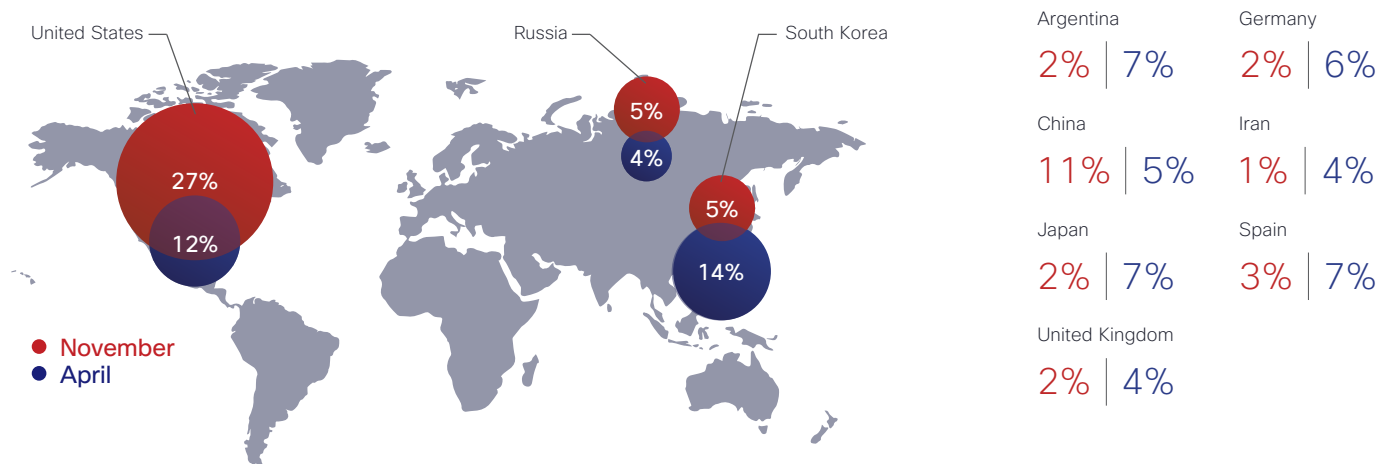


FIGURE 12

Volume Trends by Country, (November 2013–April 2014)

SOURCE: Cisco Threat Intelligence Platform

Also, although global spam volume is up, not all countries are seeing an increase. In fact, both Russia and the United States have experienced sharp declines in spam volume since November 2013. Meanwhile, South Korea has seen a significant spike in spam volume, compared to the other top 10 countries monitored by Cisco security researchers.



The background of the slide is a dark blue field filled with a complex, abstract network diagram. This diagram consists of numerous small, light-colored circular nodes connected by thin, white lines. The connections form a dense, interconnected web that spans the entire frame, with some lines appearing more prominent than others, creating a sense of depth and complexity. The overall aesthetic is technical and futuristic, typical of cybersecurity or data science presentations.

Industry Trends

Cisco security experts offer insight and analysis on threats and security trends observed during the first half of 2014, as well as projections for what to expect in the months ahead.



Compromised Secure Encrypted Connections

Recent high-profile attacks that exploited encryption and security certificates, such as Heartbleed and Apple “goto fail,”²⁰ have revealed that many popular implementations of TLS represent the weakest link for all users. That security measures such as encryption and cryptography have become weak links is ironic. For years, consumers have been urged to look for the padlock symbol online as a way to confirm they are about to complete a “safe” transaction. Many users also have trusted that their information is being well protected at the point of sale (POS) offline, believing that end-to-end encryption is taking place, if they even thought about it at all.

What the past six months have shown, however, is that no matter how vigilant or cautious users are, or how many security safeguards they put in place, weak links far beyond their control can still leave them at great risk.

Addressing the problem of compromised secure encrypted connections is obviously an imperative for any business that accepts payments. This requires closer examination of the industry processes that help bring encryption and other security products to market.



SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT



Heartbleed and similar events underscore that many organizations using secure encrypted connections and related technology assume the following:

Cryptographic protocols that are based on standards and popular open-source code provide robust security.

All embedded source code in security products and services, including code that has been provided by third parties, has been fully vetted by security experts.

Neither assumption is true, but both are factors in the successful implementation of attacks such as Heartbleed that take advantage of vulnerabilities and other security flaws and exploit users' trust.



Improving industry processes will not be easy. In its current state, according to Cisco security experts, OpenSSL is complex and difficult to implement correctly and test for vulnerabilities. The current vetting process of open-source and proprietary code needs a more robust approach, but who should develop and maintain that approach remains a question. Meanwhile, the security community is debating whether the broken certificate authority system can even be fixed.



In the security world, simplicity is paramount; minimizing the amount of code that needs to be trusted is an important step toward making secure implementations. Cisco security experts expect that improving open-source SSL/TLS security libraries will require, at minimum:

Reducing the complexity of the protocols and their implementations

Validating that the code has been implemented correctly, is free of vulnerabilities, and does not contain hidden flaws

Making sure that those who test and validate the code are qualified

One positive outcome of recent events like Heartbleed: Many in the developer community are now proactively looking through their code to find and fix flaws. The Linux Foundation also recently announced the formation of the Core Infrastructure Initiative, which “enables technology companies to collaboratively identify and fund open source projects that are in need of assistance, while allowing the developers to continue their work under the community norms that have made open source so successful.”²¹ OpenSSL was one of the first projects under consideration to receive funds from the Core Infrastructure Initiative. Cisco is one of the founding backers of the Initiative.



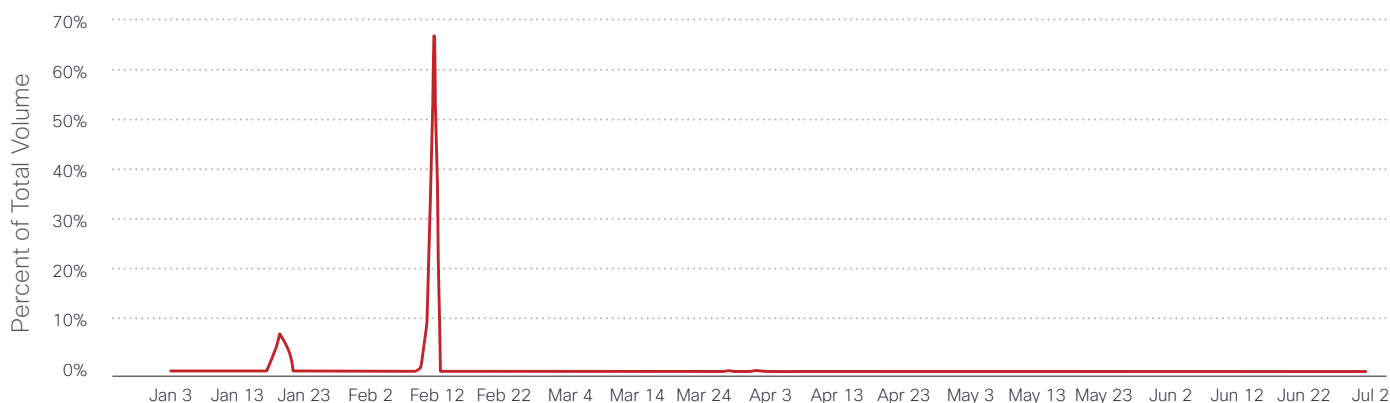
Amplification Attacks: Adversaries Clocking in with NTP

Cisco security experts warned in the *Cisco 2014 Annual Security Report* that DDoS attacks, namely, those launched through DNS amplification, would remain a top security concern for organizations in 2014.²² But even before that, Cisco researchers asserted that the NTP, which is designed to synchronize the clocks of computers over a network, was a weak link and poised to become a vector for amplified DDoS attacks. They based their projection on their observation that attack tools designed to utilize the increasing number of vulnerable NTP servers were starting to be distributed among the hacker community.²³

FIGURE 13

CloudFlare NTP DDoS Attack, 2014

SOURCE: Cisco Threat Intelligence Platform

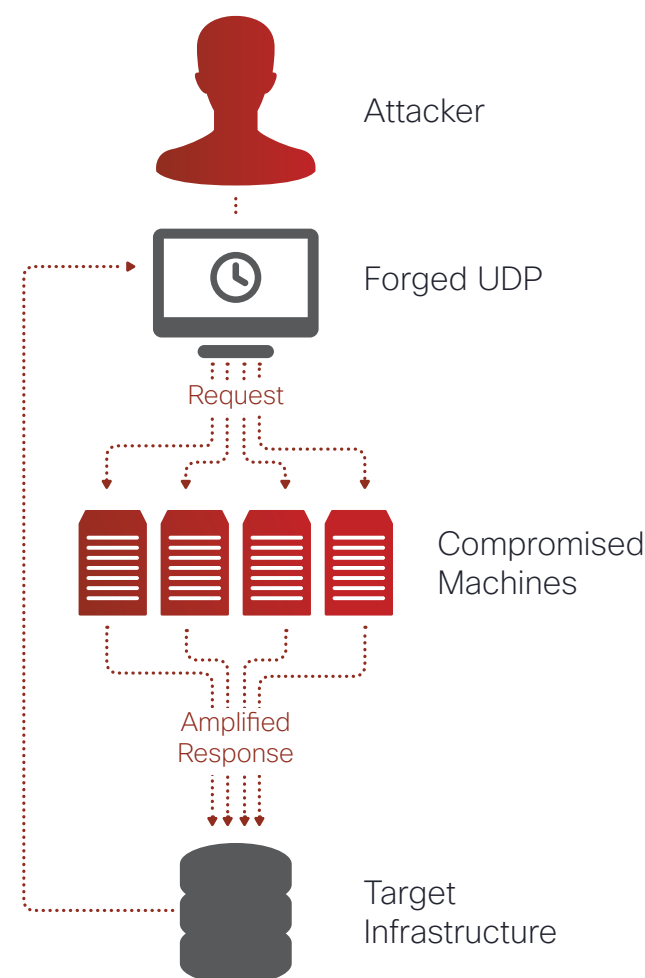


One of the most significant NTP amplification attacks observed in the first six months of 2014 targeted a customer of global DNS provider, CloudFlare (see Figure 13). At its peak, the February attack reached nearly 400 Gbps of UDP traffic, surpassing the March 2013 Spamhaus DDoS attack of 300 Gbps that involved 30,000 open DNS resolvers.²⁴

It is easy to understand why some actors are experimenting with NTP as a tool for their DDoS attacks: OpenNTPProject.org, an NTP scanning project designed to increase awareness about the NTP problem, has identified more than 1 million vulnerable NTP servers.²⁵ Combined, the bandwidth of these servers is likely larger than any DDoS attack seen to date.

FIGURE 14

Execution of an NTP Attack



To execute an NTP amplification attack, the adversary sends out small requests to vulnerable NTP machines, forging the address of the UDP packet so that the requests appear to be coming from the target the attacker is trying to take offline. The UDP is stateless; the ability to spoof the UDP address is a necessary component of both DNS and NTP amplification attacks. The NTP servers involved in the attack return a very large response to the small requests, sending all of the information back to the target whose machine is inundated and taken offline. (There are industry efforts under way to prevent UDP spoofing, which need to continue.)

Upgrading public-facing NTP servers to the latest version of NTP is necessary to prevent a potential NTP amplification attack. At the time of this writing, that version is 4.2.7. This update eliminates support for the `MON_GETLIST` or “monlist” command, which is a remote command that returns the addresses of the last 600 machines with which an NTP server interacted. If upgrading is not possible, using the `noquery` option in the NTP configuration also will prevent monlist queries.

Although NTP amplification attacks might be a new type of DDoS attack, expect DNS amplification to remain a go-to technique for many adversaries. According to the Open Resolver Project, as of October 2013, 28 million open resolvers pose a significant threat.²⁶



Exploit Kits: The Field Opens Up to Competition

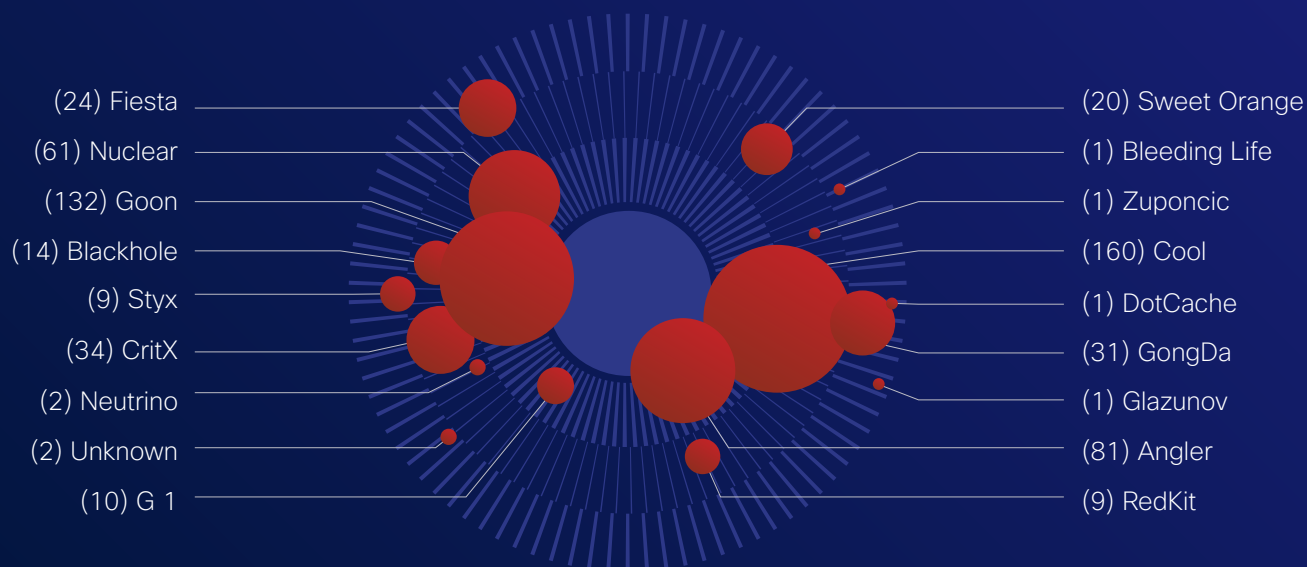
When the “malware kingpin known as ‘Paunch,’ the alleged creator and distributor of the Blackhole exploit kit,” was arrested in Russia in October 2013,²⁷ it did not take long for exploit kit authors to start staking their claim in territory his kit once dominated.

Blackhole was hands down the most widely used and well-maintained exploit kit. When Paunch and Blackhole were put out of commission by the authorities, adversaries turned their attention to new exploit kits. There were many contenders in the first half of 2014 vying for the top spot, according to Cisco security researchers; however, a clear leader has yet to emerge.

FIGURE 15

Exploit Kits Observed Since January 2014

SOURCE: Cisco Threat Intelligence Platform



(# of attacks) Exploit Kit Name

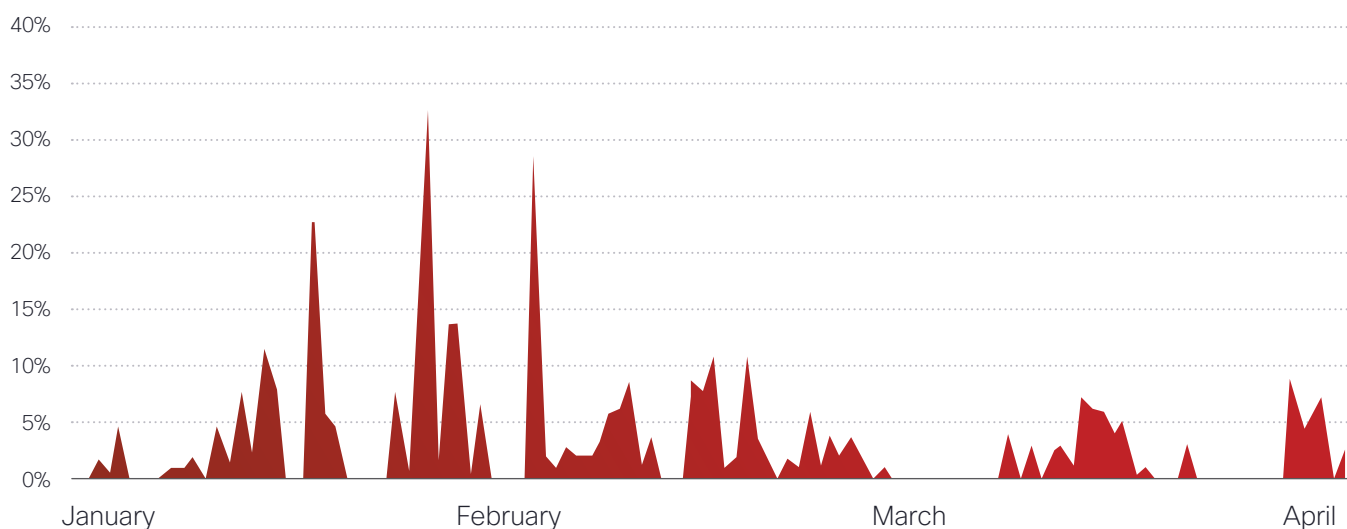


Despite the heightened competition, the number of exploit kits has dropped by 87 percent since Paunch was arrested last year, according to Cisco security researchers (see Figure 16).

FIGURE 16

Decline in Number of Exploit Kits (January–April 2014)

SOURCE: Cisco Threat Intelligence Platform



Attackers are also using exploit kits for more targeted and sophisticated campaigns, setting their sights on compromising specific users with the goal of uncovering vulnerabilities in applications, programs, and systems that will give them a direct path to infrastructure. For instance, the “LightsOut” or “Hello” exploit kits specifically target the energy industry.



Malvertising: A Disruptor for the Internet Economy

Internet advertising spend now outpaces all other forms of media.²⁸ Considering Internet advertising's humble beginnings—a simple banner ad from Hotwired in 1994—that is a pretty impressive climb over two decades. Internet advertising, annoying as it can be for users, is important because it allows people to freely consume the vast majority of the web. If that model were to change or people were to stop trusting Internet advertising altogether, the repercussions for the Internet would be monumental.

“Malvertising,” online advertising used to spread malware, is a threat to that model, and users’ trust. It affects all Internet users and is a disruptor for the Internet economy. According to Cisco security experts, malvertising underscores the sophistication of the modern cybercriminal economy in terms of the division of labor, cooperation, and specialization across the attack chain.

Malvertising is becoming more prevalent, and adversaries are able to launch highly targeted campaigns. A malvertiser who wants to target a specific population at a certain time—for example, soccer fans in Germany watching a World Cup match—can turn to a legitimate ad exchange to meet their objective. Just like legitimate advertisers, they contact companies that are gatekeepers for the ad exchanges. They will pay up front for the advertising, perhaps US\$2000 or more per ad run, and instruct the companies to tell the ad exchanges to serve the ads as quickly as possible, leaving little or no time for the ad content to be inspected.



Malvertising victims are infected with malware in the course of their normal Internet browsing and therefore have no idea where or how they were infected. Tracing the source is next to impossible, because the ad that delivered the malware has long since disappeared.



**SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT**



Really Bad Ads: Malvertising's Role in Ransomware

As reported in the *Cisco 2014 Annual Security Report*, malvertising played a key role in the distribution of the ransomware CryptoLocker. Ransomware is just as sinister as it sounds: It is a type of malware that encrypts files on victims' computers until they pay a ransom.²⁹

CryptoLocker was recently neutralized: The U.S. Department of Justice reported in June that it was working with law enforcement agencies in other countries and with technology companies to disrupt a massive two-year-old botnet known as "Gameover Zeus," a major distribution vehicle for CryptoLocker.³⁰ But it did not take long for a new brand of ransomware, "CryptoWall," to take its place.

During the first half of 2014, Cisco researchers dissected attack campaigns that use the web, specifically those that use malvertising to redirect users to websites that host exploit kits (rented or purchased by the adversary) that push a "dropper" onto users' systems and infect vulnerable systems. As part of that research, Cisco security experts observed high levels of traffic consistent with a new exploit kit known as "RIG," which was first observed in criminal forums in April 2014.³¹ RIG uses malvertising to perform a drive-by attack on visitors to high-profile, legitimate websites. The attack toolkit is being used by adversaries to distribute the CryptoWall ransomware.

As of early June, Cisco had blocked requests to many compromised WordPress sites that were redirected to by malvertising.

(See [WordPress Vulnerabilities: Who Is Minding the Store?](#), on page 37.)

The sites' landing pages host exploits for Java, Flash, and the multimedia protocol Microsoft Silverlight. According to Cisco researchers, use of the latter plug-in to help launch exploits appears to be gaining traction in the cybercrime community. Fiesta was the first known exploit kit to incorporate a Silverlight exploit in 2013. RIG and another exploit kit, Angler, soon followed suit in keeping with the highly competitive nature of the exploit kit marketplace. (See [Exploit Kits: The Field Opens Up to Competition](#), page 33.)



WordPress Vulnerabilities: Who Is Minding the Store?

Businesses of all sizes rely on WordPress, web software that is essentially a collection of scripts and add-ons that makes it easy for users to do whatever they want to do with their websites: blog, host forums, conduct e-commerce, and more.

WordPress was designed for functionality, not security.

Most WordPress users do not have the knowledge or skills to properly secure it. And quite often, users who set up a website with the WordPress content management system (CMS) and systems like it end up abandoning it in time.

There are countless sites like these across the web, and they are a significant weak link in the security chain. Attackers who breach these long-forgotten sites then have the ability to upload malicious binaries and use them as exploit delivery sites. Users encounter these sites by browsing other active and legitimate websites that also have been compromised; an iFrame pulls content from the abandoned site and serves it up to users on the legitimate site.

WordPress is not the only CMS with this problem, but it stands apart from others such as Joomla and e107 because of its popularity. Abandoned websites pose a high risk to the overall security of the Internet, and since no one is minding the store, getting these sites cleaned up or taken down is not easy. Even if site owners think to take action, most only patch the point of entry and do not check to see if they are already compromised. They do not find the backdoor and clean it off their site.

Many leading hosting providers are now offering low-cost, managed WordPress installation services for commercial websites as part of their hosting package. The providers make sure all patches are applied and the correct security settings are in place. Moving forward, as more people make use of this type of service, it will help to reduce the number of sites with WordPress vulnerabilities.





POS Attacks: Popular Threat Vector for Criminals Seeking Payment Card Data

Several intersecting trends have made POS systems an attractive venue for criminals looking to steal large amounts of credit card data and quickly monetize it. Recent high-profile security breaches at major retailers point to the fact that these types of attacks can be carried out successfully and swiftly. Examining detection capabilities before a payment card data attack makes good business sense, along with shortening remediation windows during and after an attack.

The attacks involve the theft of data that is held on the magnetic strips of payment cards. Once stolen, this data can be used to create fake credit cards that can be used for fraudulent in-store purchases. POS malware allows data to be pulled from memory, thus evading encrypted data on disks or the network. The trends that are making this exploit doable on a larger scale include:



POS Internet Connection

The increasing likelihood that POS systems are connected to the Internet, providing criminals with a point of entry to corporate networks



Lack of Understanding

Lack of understanding on the part of many organizations that payment card information should be considered critical data, which means it is less protected



Third-Party Vendors

Organizations' growing use of third-party vendors for all or part of their POS solutions, again, providing more access points for criminals

Payment card data is a hot commodity in the online criminal marketplace and offers a high return on investment. Criminals believe that stealing data from POS systems is more effective than stealing it directly from e-commerce merchants; banks have become more skilled at detecting and stopping this kind of theft.

In addition, because the United States is one of the few leading economies whose payment cards typically use magnetic strips, instead of the more secure "chip and PIN" system, data within the magnetic strip is easy to monetize. (However, without end-to-end encryption of card data, card numbers and expiration dates can still be stolen and used in online transactions, even with chip and PIN systems.)



More Critical Monitoring of Payment Card Data

Preventing theft of payment card data and other sensitive information at POS requires organizations to make greater investments in technological barriers to entry for criminals. They also need to recognize that payment card data deserves more attention from the security professionals they employ in their businesses.

Some organizations choose to add hardware encryption devices at the POS; this can help prevent payment card data from being intercepted as it travels across networks. If this is deemed too great an expense, then at the very least, organizations should mark this data “critical” and monitor it in order to detect unauthorized access and irregular movements through the data. There are too many ways to initially compromise the network, and organizations should generally assume that attackers can already get into a network.

The most logical IOCs that would shed light on a possible theft of payment card data are the importation of a tool set, a new process running on a POS terminal, and the exfiltration of compressed files with uniform size and frequency. Systems that can analyze these behaviors across the extended network should be considered.

It is also good practice to conduct application and process change detection on all payment card processing systems. Any change on an endpoint should be cause for immediate analysis. Also, although most protocols tend to use compression for efficiency and speed gains, compression tools themselves should be part of an organization’s “application whitelist.”

Finally, networks should be segmented so that enterprises do not make it easy for criminals to get access to treasure troves of data: POS systems should be on a separate network segment from the enterprise network to limit access and pivoting attacks on the POS systems.



With the explosion of mobile devices and their proliferation into the enterprise network, segmentation should include strong identity capabilities that can detect who the user is, the type of device the user is using to access the network, and the method in which the network is being accessed. For example, access via a corporate-owned laptop on the enterprise campus wireless LAN might be allowed, although access using a tablet via remote access VPN might be denied because of the POS data sensitivity.

Cisco expects that attackers seeking payment card data will continue to focus their efforts on POS systems. However, careful detection and alert systems, plus the implementation of hardware encryption, can help prevent such schemes from being carried out.



Social Engineering: Finding the Weak Links in Person

An enterprise can pay hundreds of thousands of dollars or more for the latest security software and imagine itself protected from targeted attacks that come in via the network. But if the threat is a real-live person who walks in the front door of an office or server farm, what good can the network edge software do?

Clever criminals are seeing bigger payoffs in showing up on-site to physically plug into a network rather than crafting phishing emails with links that lead to compromised websites. (Not to say that spam and other online social engineering campaigns have gone away; see [page 26](#) for more.) Simply being able to plug into an Ethernet

connection or unplug an IP phone and use that cable to access network information can have serious consequences. Social engineering is the act of hacking people. Therefore, people—your employees—become the weakest link in your digital and physical security posture.

Criminals use similar tactics for social engineering an in-person visit as they do with emails and compromised websites. The point is to build trust (albeit misplaced) with someone who can grant access to company premises.





By researching a targeted employee on LinkedIn—for instance, discovering everything from the tasks they perform on the job to where they went to college and which sports teams they like—the criminal can present himself or herself as someone the target might know or have reason to trust.

Thanks to the popularity of social networking, especially among professionals, there is a wealth of information and photos easily available to anyone who needs to get a literal foot in the door.

Armed with background gleaned from online searches, a criminal can pretend to be a journalist and request an interview or claim to be a potential partner or customer and ask for an in-person visit. The criminal might also wear a fake badge to provide the illusion of authority.

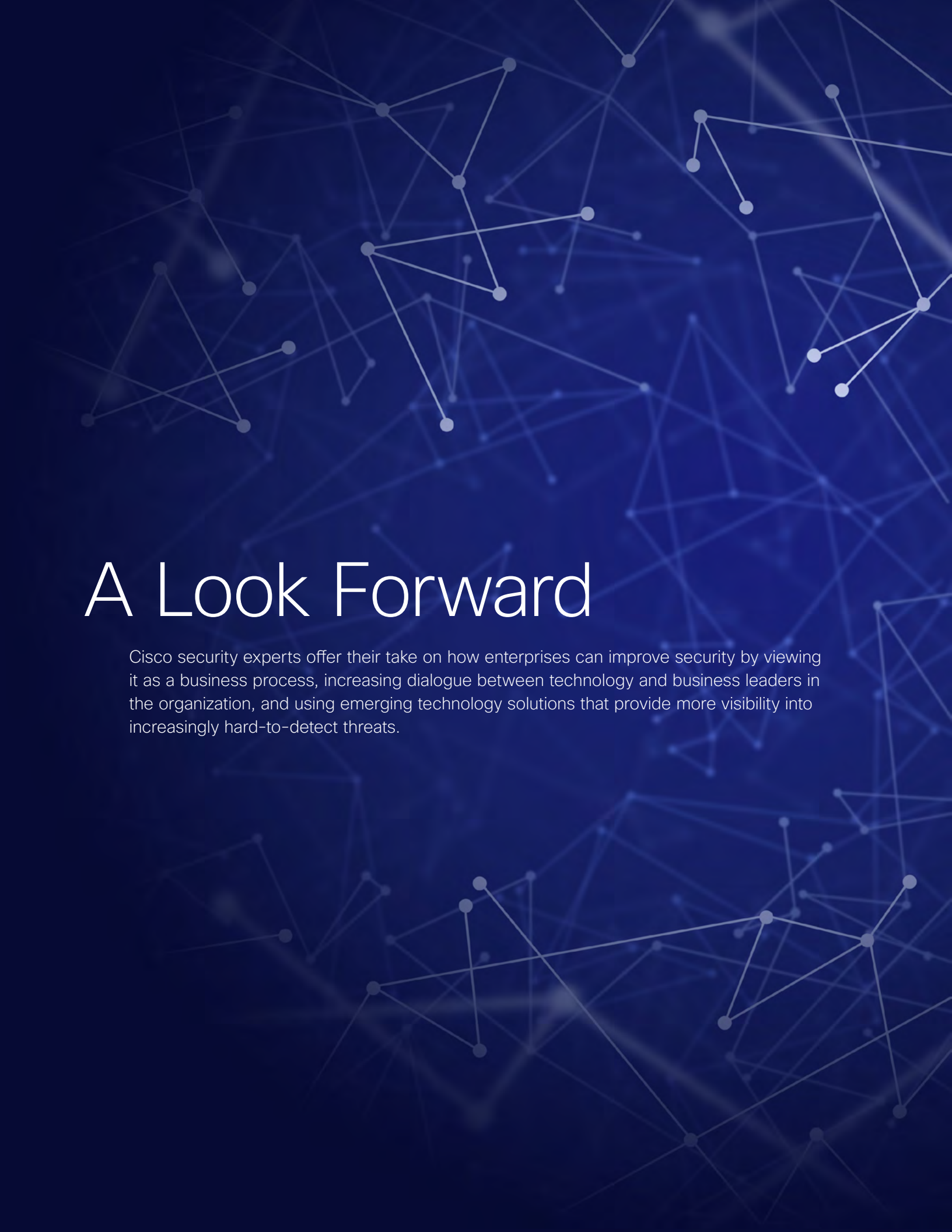
Criminals have also figured out that they do not need to launch such scams at the front door of the organization they are targeting. Instead, they will target a weaker link: that is, a less secure business partner or supplier that has access or connectivity to their real target, which is the network. This is an especially effective technique to use when the security of a target is high, but the security of a trusted business partner of your target is not. Hackers will always try to find the easiest route in.

A mitigation approach for social engineering-based security breaches that involve gaining physical network access is to make sure network access ports enforce authentication and authorization before granting network access. In addition, organizations can build “dynamic security domains” per user, per device, per user and device, or any other configuration needed. These dynamic security domains can use technology such as 802.1x, port access-control lists (ACLs), VPN, and host posture assessment.

Solution

No matter what access method an attacker uses (wired, wireless, or VPN), IT professionals can dynamically create a security domain or “bubble” made just for them. If a criminal connects a laptop into a port on-site, the network will stop the person, authenticate them, profile them, posture-assess them, watch their behavior, and then provide that user with very specific and dynamic authorization rights that restrict their network access based on a contextual policy.



The background of the slide is a dark blue gradient with a complex, abstract network diagram. It consists of numerous small, light blue circular nodes connected by thin, white lines, creating a web-like structure that spans the entire frame. The lines and nodes vary in opacity, giving a sense of depth and connectivity.

A Look Forward

Cisco security experts offer their take on how enterprises can improve security by viewing it as a business process, increasing dialogue between technology and business leaders in the organization, and using emerging technology solutions that provide more visibility into increasingly hard-to-detect threats.



Intelligent Cybersecurity for the Real World

Strengthening weak links across the security chain rests largely upon the ability of individual organizations and industry to create awareness about cyber risk at the board level and make cybersecurity an imperative for the business. Aligning business strategy, security operations, and the controls that enable cyber resilience is also critical, as is the aptitude to create greater network visibility across a “noisy” network by employing emerging, intelligent solutions such as predictive analytics.

To cover the entire attack continuum before, during, and after an attack, today’s organizations must address a broad range of attack vectors with security solutions that operate everywhere a threat can manifest itself. This includes the network, mobile devices, virtually, and in the cloud or data center.



Reducing security gaps—whether they are known and actively exploited vulnerabilities in Java, Flash, or Adobe PDF; abandoned WordPress-created websites; long-overlooked security flaws in OpenSSL software; unprotected physical access to networks; or vulnerable NTP servers—and the complexity caused by disparate products and disjointed solutions is the path to better security for all users. To make sure of network resiliency to support the business, evaluating the lifecycle status of discovered network devices, potential security vulnerabilities, and operating system version management is also critical.³²



Cisco's strategy to help organizations address these known and emerging security challenges is based on three strategic imperatives:



Visibility-driven

The more we can see, the more we can correlate information and apply intelligence to understand context, make better decisions, and take action—either manually or automatically.



Threat-focused

We must focus on detecting, understanding, and stopping threats through continuous analysis, and real-time security intelligence that is delivered from the cloud and shared across all security solutions to improve efficacy.



Platform-based

Security is now more than a network issue. It requires an integrated system of agile and open platforms that cover the network devices, and the cloud.

Intelligent cybersecurity for the real world is what will help to enable a secure Internet of Things, and form the foundation for an Internet of Everything world where security, just like computing, will be powerful and pervasive, and seamless to end users.



Operationalizing Security: Making Security a Business Process



Security assessments often reveal that the root cause of a security issue is an operational failure by the business and a technical failure. Lack of operational maturity or capabilities or both leads to weak or nonexistent security controls.

As cybersecurity becomes more of a strategic risk for today's businesses, there is growing focus on achieving "security operations maturity," where the organization has a holistic view of cybersecurity risks and is continually improving cybersecurity practices.

With help from service providers in this space, many organizations are working toward making security a highly standardized and measured business process, or set of processes, which is reviewed on a regular basis to make sure strategic objectives are being met. The decision to view security as a business process often stems out of broader business initiatives designed to improve governance, risk, and compliance (GRC) throughout the organization. Many businesses find, often too late, that when it comes to IT security, being compliant is not enough.

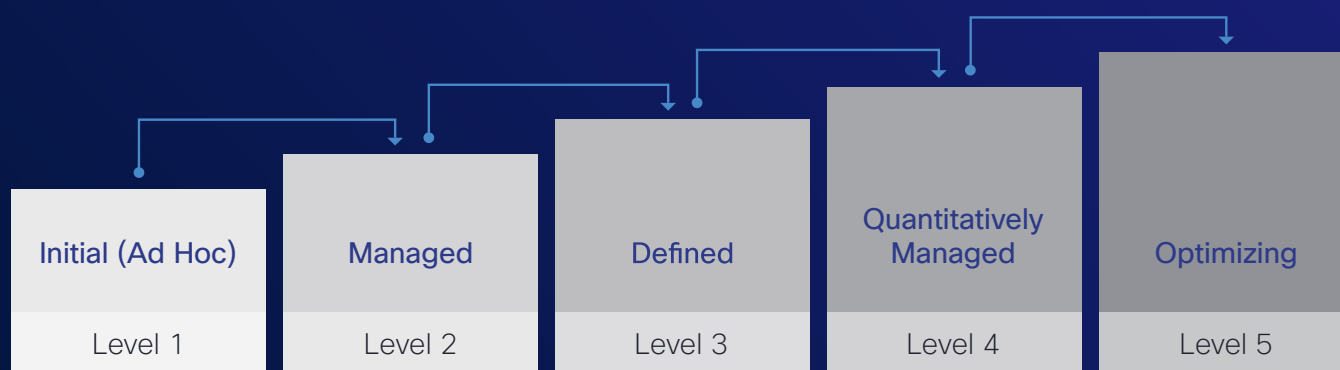


Organizations that operationalize security gain a better understanding of:

1. What they need to protect
2. How well their current security measures work
3. What they need to accomplish in terms of cybersecurity

FIGURE 17

CMMI Model



Operationalizing security leads to better visibility into what is happening with IT security throughout the organization: which employees are responsible for it; whether they are the right people to handle that responsibility; and, if so, whether they are doing their jobs well. Businesses that operationalize security also can determine whether IT resources are being deployed and used effectively.

A critical component of operationalizing security is a productive dialogue between security leaders, such as chief information officers (CIOs) and chief information security officers (CISOs), and business leaders. Making cybersecurity a formal business process necessitates that these two leadership groups work together more closely and frequently to define acceptable levels of risk and outline strategic goals around security for the organization. To help drive this dialogue, CISOs need to find ways to present cybersecurity information in terms that business leaders will clearly understand; metrics, for example, can help to translate the value of the business taking steps to avoid a particular cybersecurity risk.

Operationalizing security also involves following a “maturity model.” Carnegie Mellon’s Capability Maturity Model Integration (CMMI) is one example. This widely used model began as a project at the university’s Software Engineering Institute in the 1980s. As Figure 17 illustrates, the starting point of the maturity model is the “ad hoc” phase, which is essentially a “firefighting” mode. When an organization reaches the last phase, it is using standardized and repeatable processes that can be measured.



Understanding Cyber Risk in Business Terms

Many companies are staking the future of their business models on the pervasive connectedness that the Internet of Things world promises. But to prepare for and ultimately succeed in this rapidly emerging environment, executive leadership needs to understand, in business terms, the cyber risks associated with growing dependence on the network.

Not discussing cybersecurity issues in public has long been the status quo for many organizations, but things are changing. More business leaders are beginning to understand that cybersecurity risks are common challenges for all organizations, especially as enterprises become more digitized and information assets increasingly become strategic assets.

These executives are also starting to recognize that in an Internet of Things world, candid dialogue about threats and best practices for mitigating them needs to take place within the business, between businesses (including competitors), and between the public and private sectors. Increasing pressure from boards of directors, which seek to understand the potential business effects of cybersecurity risks, is helping to evolve this point of view at the C-level.

Recent actions by the U.S. Securities and Exchange Commission (SEC) have helped to make cybersecurity a top-of-mind topic for boards. The SEC issued cybersecurity reporting requirements for public companies in 2011,³³ requiring that these companies inform shareholders of “significant instances of cybertheft or attack, or even when they are at material risk of such an event.”³⁴ The SEC also held a cybersecurity roundtable earlier this year “to discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns.”³⁵

On the global stage, the World Economic Forum (WEF), an international institution committed to improving the state of the world through public-private cooperation, has introduced its concept of “cyber resilience” in 2011 as a way to help elevate cybersecurity and other Internet-related issues to the board level. WEF promotes cyber resilience as an interdependent ecosystem where every organization is only as strong as the weakest link in the security chain. This is outlined in one of the four guiding principles in WEF’s “Partnering for Cyber Resilience”³⁶ initiative:

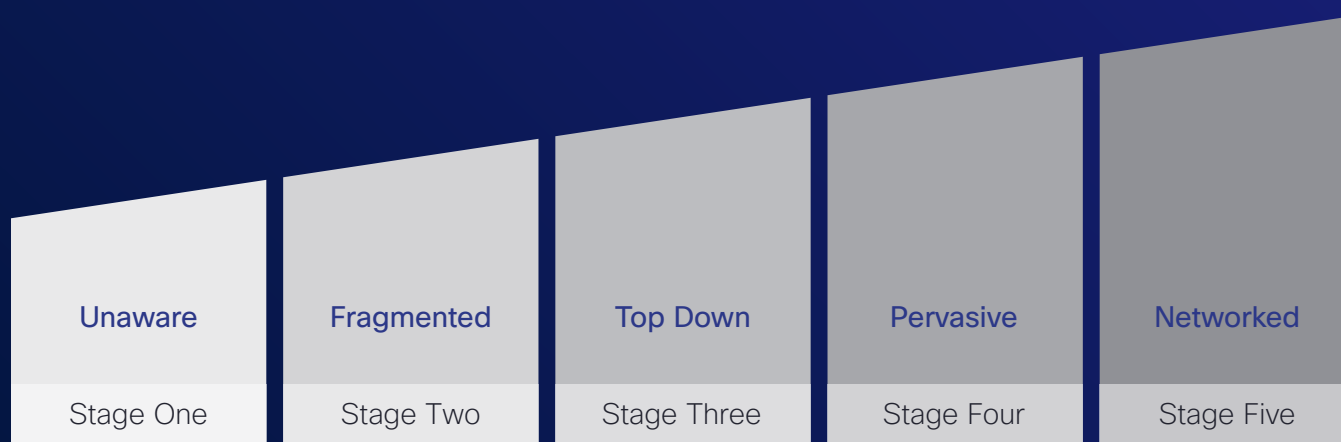
We are all only as strong as the weakest link in the chains upon which we all depend; we each contribute to the safety of our hyperconnected world. An open, secure, and resilient online space is a public good; all actors share responsibility for creating and supporting this resource.



WEF's cyber resilience initiative is designed to help chief executive officers and other C-level leaders, including CIOs and CISOs, drive the cybersecurity discussion in their organizations and speak in business terms about cyber risks and opportunities. For example: "What is the cost to the business if we decide not to invest in a value-producing technology because of concerns about cyber risk?"

FIGURE 18

Maturity Model for Organizational Cyber Resilience



Achieving cyber resilience requires that organizations take a risk-based approach to cybersecurity, according to WEF, which is a valid approach for any business that looks to improve cybersecurity. The institution offers this maturity model, which illustrates a path to cyber resilience.

Through its cyber resilience initiative, WEF emphasizes that cybersecurity is not something that can be accomplished by one department in an organization, namely, IT. This is because cyber capabilities are not only technical, but also institutional. Additionally, WEF underscores that promoting cybersecurity awareness in the organization is largely the responsibility of the chief executive, who is also ultimately accountable for helping the business to achieve cyber resilience.



SHARE THE CISCO 2014
MIDYEAR SECURITY REPORT

Predictive Analytics: A Detective That Enables Better Security

It is a vicious cycle: The security industry builds a threat-specific response to a cybersecurity threat, and the attackers find a new way to avoid detection. Adversaries are proactively working to understand what type of security solutions are being deployed and shifting to less visible, less content-detectable patterns of behavior so their threats are well concealed. Now, there is less “low-hanging fruit” for security solutions and professionals to detect; instead, there is more cipher traffic, more scrambling, and more randomization by malicious actors to make command-and-control behaviors indistinguishable from real traffic.



The lack of visibility organizations have into today’s “noisy” networks means pervasive threats have plenty of hiding places. Breaking through that noise and understanding whether something abnormal is happening on a network requires knowing what “normal” actually looks like. Predictive analytics is an emerging detection capability that provides that type of insight and helps organizations increase the resilience of their security solutions. It is a tool for spotting unusual behavior on a network—the symptoms of an infection—through behavioral analysis and anomaly detection.

Through the use of predictive analytics, organizations can assess the behavior of entities (host servers and users) in their network. A model, derived from many smaller models and a concise representation of past behavior, is created and used to predict how entities should behave in the future. Ideally, data is correlated in the cloud to enhance the speed, agility, and depth of threat detection. If there is a discrepancy in expected behavior that is significant or sustained, it is flagged for investigation.

Predictive analytics helps to make existing security techniques more accurate as well as more capable of detecting unknown or unusual behavior on the network. It involves advanced decision-making algorithms that analyze multiple parameters and take in live traffic data; machine learning capabilities allow the system to learn and adapt based on what it sees.

Machine learning systems are like detectives. They look for where dangers might be and for evidence of an incident that has taken place, is under way, or might be imminent. And although they do not necessarily handle security or policy enforcement, they empower other systems to find unexpected threats and perform enforcing actions. To provide value and help organizations elevate their security efficacy, predictive analytics needs to be deployed alongside content-based security solutions, perimeter management solutions, and policy management solutions.



About Cisco

Cisco delivers intelligent cybersecurity for the real world. This vision is based on a threat-centric approach to security that reduces complexity while providing superior visibility, continuous control, and advanced threat protection across the entire attack continuum. With this threat-centric security model, organizations can act quickly before, during, and after an attack.

Threat researchers in Cisco's Collective Security Intelligence ecosystem bring commanding knowledge and sophisticated big data systems to bear in discovering, analyzing, and protecting against both known and emerging threats. Cisco's renowned security experts are backed by sophisticated infrastructure and systems that provide unparalleled visibility from aggregation and analysis of Cisco's unrivaled telemetry of billions of web requests and emails, millions of malware samples, open-source data sets, and thousands of network intrusions.

The result is "big intelligence": intelligence that delivers superior security effectiveness that immediately and pervasively protects extended networks the world over.

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



Endnotes

- ¹ *Estimating the Cost of Cyber Crime and Cyber Espionage*, Center for Strategic and International Studies (CSIS), July 2013: <https://csis.org/event/estimating-cost-cyber-crime-and-cyber-espionage>.
- ² "Internet of Things," Cisco.com: <http://www.cisco.com/web/solutions/trends/iot/overview.html>.
- ³ "Internet of Things" infographic, Cisco Internet Business Solutions Group: <http://share.cisco.com/internet-of-things.html>.
- ⁴ "Hackers Reveal Nasty New Car Attacks—With Me Behind The Wheel," by Andy Greenberg, *Forbes*, August 12, 2013: <http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/>.
- ⁵ "Hackers Reportedly Targeted Three Large Medical Device Makers," iHealthBeat.com, February 11, 2014: www.ihealthbeat.org/articles/2014/2/11/hackers-reportedly-targeted-three-large-medical-device-makers.
- ⁶ "How secure is your baby monitor? What can happen when the 'Internet of Things' gets hacked," by Matt Hartley, *Financial Post*, May 3, 2014: http://business.financialpost.com/2014/05/03/how-secure-is-your-baby-monitor-what-can-happen-when-the-internet-of-things-gets-hacked/?_lsa=bc1b-f93e.
- ⁷ "The Internet of Everything, Including Malware," by Craig Williams, Cisco Security blog, December 4, 2014: <http://blogs.cisco.com/security/the-internet-of-everything-including-malware/>.
- ⁸ The focus of this report is to highlight the number of requests for potentially malicious FQDNs, domains, sites, and more that are emanating from the customer.
- ⁹ *Cisco 2014 Annual Security Report*: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
- ¹⁰ Customers interested in participating in direct intelligence sharing with the AEGIS program within the Vulnerability Research Team should email threatintel@cisco.com.
- ¹¹ Ibid.
- ¹² For more on Heartbleed, visit www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html.
- ¹³ "OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations," by Pano Kampanakis, Cisco Security blog, April 9, 2014: <http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations>.
- ¹⁴ For more information on OpenSSL Heartbleed vulnerability mitigation, see "Cisco Event Response: OpenSSL Heartbleed Vulnerability CVE-2014-0160," April 22, 2014, Cisco.com: www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html.
- ¹⁵ "New OpenSSL Defects – Another Heartbleed? Tor Stripped?" by James Lyne, *Forbes*, June 5, 2013: www.forbes.com/sites/jameslyne/2014/06/05/new-openssl-defects-another-heartbleed.
- ¹⁶ "Severe OpenSSL Security Bug Uncovered by Japanese Researcher Months After Heartbleed," by Luke Villapaz, *International Business Times*, June 5, 2014: www.ibtimes.com/severe-openssl-security-bug-uncovered-japanese-researcher-months-after-heartbleed-1594989.
- ¹⁷ *Cisco 2014 Annual Security Report*: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
- ¹⁸ Ibid.
- ¹⁹ "Spam Hits Three Year High-Water Mark," Cisco Security blog, May 2, 2014: <http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark>.
- ²⁰ "Major Apple security flaw: Patch issued, users open to MITM attacks," by Violet Blue, "Zero Day" blog, *ZDNet*, Feb. 22, 2014: <http://www.zdnet.com/major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/>.



- ²¹ "Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware and The Linux Foundation Form New Initiative to Support Critical Open Source Projects," media release, Linux Foundation, April 24, 2014. For more information on the Initiative, visit <http://www.linuxfoundation.org/news-media/announcements/2014/04/amazon-web-services-cisco-dell-facebook-fujitsu-google-ibm-intel>
- ²² *Cisco 2014 Annual Security Report*: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
- ²³ "When Network Clocks Attack," by Jaeson Schultz, Cisco Security blog, January 10, 2014: <http://blogs.cisco.com/security/when-network-clocks-attack/>.
- ²⁴ "Chronology of a DDoS: Spamhaus," by Seth Hanford, Cisco Security blog, March 28, 2013: <http://blogs.cisco.com/security/chronology-of-a-ddos-spamhaus/>.
- ²⁵ To find out if your NTP server is vulnerable, visit openntpproject.org. For more on DNS best practices, refer to "DNS Best Practices, Network Protections, and Attack Identification": <http://www.cisco.com/web/about/security/intelligence/>.
- ²⁶ Open Resolver project: www.openresolverproject.org.
- ²⁷ "Meet Paunch: The Accused Author of the Blackhole Exploit Kit," by Brian Krebs, KrebsOnSecurity blog, December 6, 2013: <http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/>.
- ²⁸ "Global Internet Ad Spend Sees Double-Digit Growth, Outpaces Other Media," *Nielsen*, July 10, 2012: [http://www.nielsen.com/us/en/newswire/2012/global-internet-ad-spend-sees-double-digit-growth-outpaces-other-media.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+NielsenWire+\(Nielsen+Wire\)](http://www.nielsen.com/us/en/newswire/2012/global-internet-ad-spend-sees-double-digit-growth-outpaces-other-media.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+NielsenWire+(Nielsen+Wire)).
- ²⁹ *Cisco 2014 Annual Security Report*: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
- ³⁰ "Malicious Advertisements on Major Websites Lead to Ransomware," by Jeremy Kirk, IDG News Service, June 6, 2014: <http://www.pcworld.com/article/2360820/malicious-advertisements-on-major-websites-lead-to-ransomware.html>.
- ³¹ "RIG Exploit Kit Strikes Oil," by Andrew Tsonchev, Cisco Security blog, June 5, 2014: <http://blogs.cisco.com/security/rig-exploit-kit-strikes-oil/>.
- ³² Network Barometer Report: A gauge of global networks' readiness to support business, *Dimension Data*, 2013: <http://www.dimensiondata.com/Global/Documents/Network%20Barometer%20Report%202013.pdf>.
- ³³ "CF Disclosure Guidance: Topic No. 2: Cybersecurity," Division of Corporation Finance, SEC, October 13, 2011: <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.
- ³⁴ "Cybersecurity: SEC outlines requirement that companies report data breaches," by Ellen Nakashima and David S. Hilzenrath, *The Washington Post*, October 14, 2011: http://www.washingtonpost.com/world/national-security/cybersecurity-sec-outlines-requirement-that-companies-report-data-breaches/2011/10/14/gIQAAGjskL_story.html.
- ³⁵ "Cybersecurity Roundtable," SEC: <http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml>.
- ³⁶ For more on WEF's Partnering for Cyber Resilience initiative, go to <http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience>.

