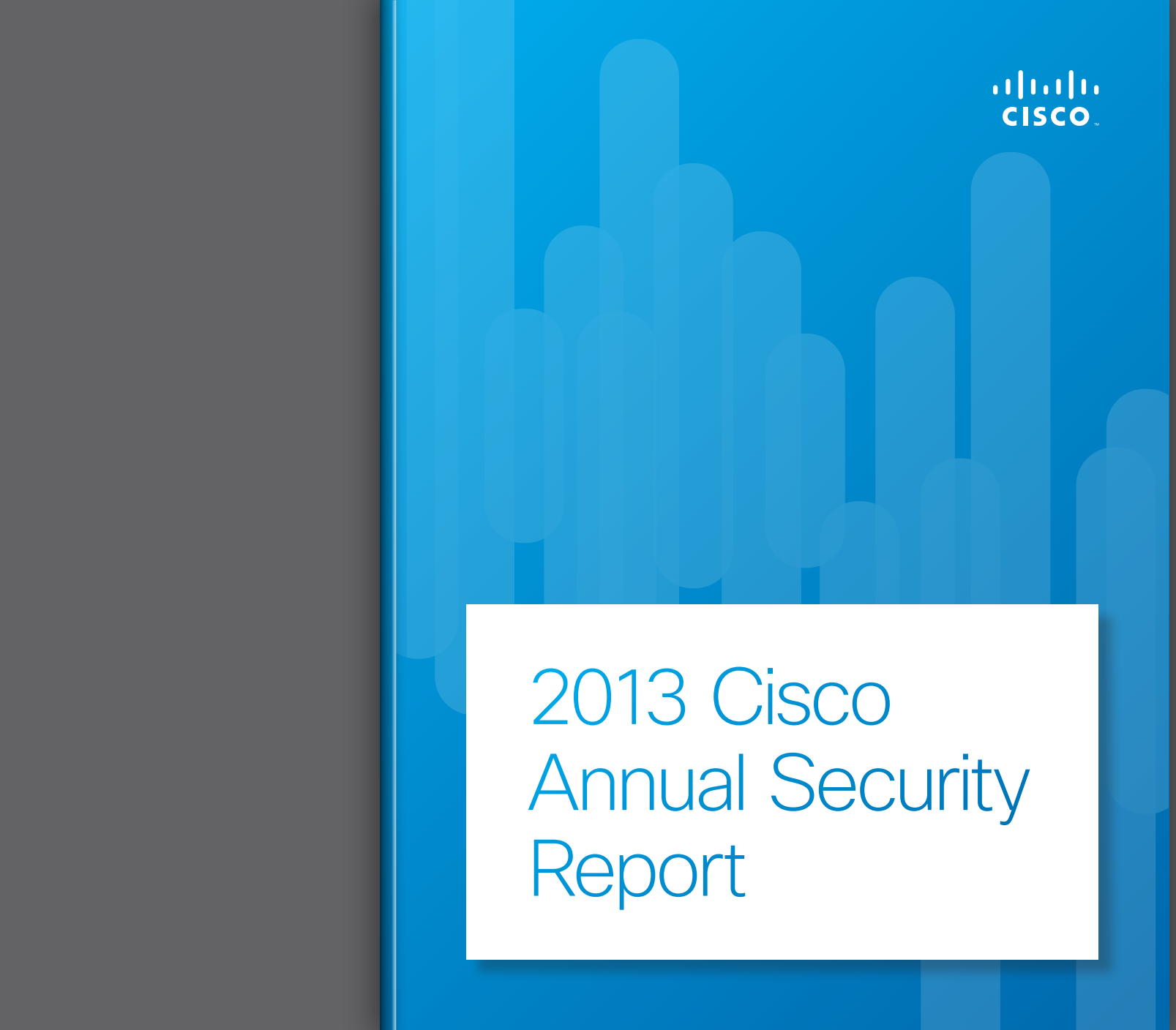

2013 Cisco
Annual Security
Report

Living in today's "Any-to-any" world.

Cybercriminals are taking advantage of the rapidly expanding attack surface found in today's "any-to-any" world, where individuals are using any device to access business applications in a network environment that utilizes decentralized cloud services. The *2013 Cisco® Annual Security Report* highlights global threat trends based on real-world data, and provides insight and analysis that helps businesses and governments improve their security posturing for the future. The report combines expert research with security intelligence that was aggregated from across Cisco, focusing on data collected during the 2012 calendar year.

Contents

The Nexus of Devices, Clouds, and Applications

The Any-to-Any World and the Internet of Everything is an evolution in connectivity and collaboration that is unfolding rapidly. It's the nexus of devices, clouds, and applications.

While this evolution is not unexpected, today's enterprises may be unprepared for the reality of navigating an "any-to-any" world—at least, from a security perspective.

"The crux of the any-to-any issue is this: We're quickly reaching the point where it is increasingly less likely that a user is going to access a business through an enterprise network," says Chris Young, Senior Vice President of the Security and Government Group at Cisco. "More and more, it's about any device in any location coming over any instantiation of the network. Internet-enabled devices—smartphones, tablets, and more—are trying to connect to applications that could be running anywhere, including in a public SaaS cloud, in a private cloud, or in a hybrid cloud."

At the same time, another evolution is underway—a steady movement toward the formation of the "Internet of Everything." This is the intelligent connection of:

- **People:** Social networks, population centers, digital entities
- **Processes:** Systems, business processes
- **Data:** World Wide Web, information
- **Things:** Physical world, devices and objects

"More and more, it's about any device in any location coming over any instantiation of the network. Internet-enabled devices—smartphones, tablets, and more—are trying to connect to applications that could be running anywhere."

"The growth and convergence of people, processes, data, and things on the Internet will make networked connections more relevant and valuable than ever before."

Nancy Cam-Winget, Distinguished Engineer, Cisco.

The Internet of Everything builds on an "Internet of Things"[1] foundation by adding network intelligence that allows convergence, orchestration, and visibility across previously disparate systems. Connections in the Internet of Everything aren't just about mobile devices or laptops and desktops, but also the rapidly growing number of machine-to-machine (M2M) connections coming online each day. These "things" are often objects we take for granted or rely on each day, and don't traditionally think of as being connected—such as a home heating system, a wind turbine, or a car.

The Internet of Everything is a future state, to be sure, but is not so distant when the any-to-any issue is considered. And while it, too, will create security challenges for enterprises, it will bring new opportunities as well. "Amazing things will happen and be created as the Internet of Everything grows," says Nancy Cam-Winget, a distinguished engineer, Cisco. "The growth and convergence of people, processes, data, and things on the Internet will make networked connections more relevant and valuable than ever before. Ultimately, the Internet of Everything will create new capabilities, richer experiences, and unprecedented economic opportunities for countries, businesses, and individuals."

How the Cloud Complicates Security

The challenge of securing a wide range of applications, devices, and users—whether in an "any-to-any" or Internet of Everything context—is made tougher by the popularity of the cloud as a means of managing enterprise systems. According to data compiled by Cisco, global data center traffic is expected to quadruple over the next five years, and the fastest-growing component is cloud data. By 2016, global cloud traffic will make up nearly two-thirds of total data center traffic.

Global data center traffic is expected to quadruple over the next five years, and the fastest-growing component is cloud data. By 2016, global cloud traffic will make up nearly two-thirds of total data center traffic.

Piecemeal security solutions, such as applying firewalls to a changeable network edge, don't secure data that is now constantly in motion among devices, networks, and clouds. Even among data centers—which now house organizations' "crown jewels" (big data)—virtualization is becoming more the rule than the exception. Addressing security challenges presented by virtualization and the cloud requires rethinking security postures to reflect this new paradigm—perimeter-based controls and old models of access and containment need to be changed to secure the new business model.

Connected Workers and Data Privacy

Another complicating factor in the any-to-any equation is young, mobile workers. This group believes they should be able to do business wherever they happen to be and on whatever devices they have at hand. Featured in this year's *2013 Cisco Annual Security Report* are findings from the *2012 Cisco Connected World Technology Report* which build on research conducted in 2011 about the changing attitudes that college students and young professionals around the globe have toward work, technology, and security.

Another complicating factor in the any-to-any equation is young, mobile workers. This group believes they should be able to do business wherever they happen to be and on whatever devices they have at hand.

The latest study shines even more light on these workers' attitudes toward security, with a special focus on privacy and how much or how often a company can intrude on an employee's desire to freely roam the Internet while at work. The *2012 Cisco Connected World Technology Report* study also examines whether online privacy is still something that all users actively worry about.

Data Analysis and Global Security Trends

The *2013 Cisco Annual Security Report* includes in-depth analysis of web malware and spam trends, based on research conducted by Cisco. While many who operate in the

"We are seeing some disturbing changes in the threat environment facing governments, companies, and societies."

John N. Stewart, Senior Vice President and Chief Security Officer at Cisco.

"shadow economy" have centered their efforts in recent years on developing increasingly sophisticated techniques, Cisco's research makes clear that cybercriminals are often turning to well-known and basic methods to compromise users.

The rise in distributed denial of service (DDoS) attacks over the past year is just one example of the trend toward "what's old is new again" in cybercrime. For several years, DDoS attacks—which can paralyze Internet service providers (ISPs) and disrupt traffic to and from targeted websites—have been low on the list of IT security priorities for many enterprises. However, recent campaigns against a number of high-profile companies—including U.S. financial institutions[2]—serve as a reminder that any cybersecurity threat has the potential to create significant disruption, and even irreparable damage, if an organization is not prepared for it. Therefore, when creating their business continuity management plans, enterprises would be wise to consider how they would respond to and recover from a disruptive cyber event—whether that event takes the form of a DDoS attack directed at the company; a critical, Internet-enabled manufacturing facility suddenly going offline; an advanced multistage attack by the criminal underground; or something else never before seen.

"While the IT security discussion has suffered more than its fair share of alarmism over the years, we are seeing some disturbing changes in the threat environment facing governments, companies, and societies," says John N. Stewart, Senior Vice President and Chief Security Officer at Cisco. "Cybercrime is no longer an annoyance or another cost of doing business. We are approaching a tipping point where the economic losses generated by cybercrime are threatening to overwhelm the economic benefits created by information technology. Clearly, we need new thinking and approaches to reducing the damage that cybercrime inflicts on the well-being of the world."

Endpoint Proliferation

The "any-to-any" evolution already involves billions of Internet-connected devices; in 2012, the number of these devices globally grew to more than 9 billion.[3]

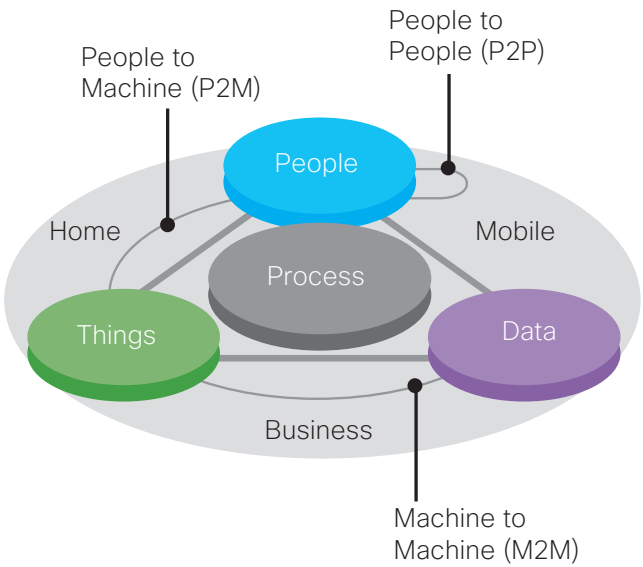
Considering that less than 1 percent of things in the physical world are connected today, there remains vast potential to "connect the unconnected."[4] It is projected that with an Internet that already has an estimated 50 billion "things" connected to it, the number of connections will increase to 13,311,666,640,184,600 by the year 2020. Adding just one more Internet-connected "thing" (50 billion + 1) will increase the number of connections by another 50 billion.[5]

As for the "things" that will eventually comprise the "everything," they will range from smartphones to home heating systems to wind turbines to cars. Dave Evans, Cisco's Chief Futurist with the Internet Business Solutions Group, explains the concept of endpoint proliferation like this: "When your car becomes connected to the Internet of Everything in the near future, it will simply increase the number of things on the Internet by one. Now, think about the numerous other elements to which your car could be connected—other cars, stoplights, your home, service personnel, weather reports, warning signs, and even the road itself."[6]

"When your car becomes connected to the Internet of Everything in the near future, it will simply increase the number of things on the Internet by one. Now, think about the numerous other elements to which your car could be connected—other cars, stoplights, your home, service personnel, weather reports, warning signs, and even the road itself."

David Evans, Chief Futurist, Cisco

Figure 1: The Internet of Everything
The Internet of Everything is the intelligent connection of people, processes, data, and things.



In the Internet of Everything, connections are what matter most. The types of connections, not the number, are what create value between people, processes, data, and things.

In the Internet of Everything, connections are what matter most. The types of connections, not the number, are what create value between people, processes, data, and things. And eventually, the number of connections will dwarf the number of things.[7] The explosion of new connections already becoming part of the Internet of Everything is driven primarily by the development of more and more IP-enabled device, but also by the increase in global broadband availability and the advent of IPv6. The security risks posed by the Internet of Everything are not just related to the any-to-any endpoint proliferation that is bringing us closer, day by day, to an even more highly connected world, but also the opportunity for malicious actors to utilize even more inroads to compromise users, networks, and data. The new connections themselves create risk because they will generate even more data in motion that needs to be protected in real time—including the ballooning volumes of big data that enterprises will continue to collect, store, and analyze.

"The Internet of Everything is quickly taking shape, so the security professional needs to think about how to shift their focus from simply securing endpoints and the network perimeter"

Chris Young

"The Internet of Everything is quickly taking shape, so the security professional needs to think about how to shift their focus from simply securing endpoints and the network perimeter," says Chris Young. "There will be too many devices, too many connections, and too many content types and applications—and the number will only keep growing. In this new landscape, the network itself becomes part of the security paradigm that allows enterprises to extend policy and control over different environments."

Cisco BYOD Update

Endpoint proliferation is a phenomenon Cisco knows well within its own organization of 70,000 employees worldwide. Since formalizing its BYOD practice two years ago, the company has witnessed a 79 percent growth rate in the number of mobile devices in use in the organization.

The *Cisco 2011 Annual Security Report*[8] first examined Cisco's unfolding BYOD journey, which is part of the organization's ongoing and broader transition toward becoming a "virtual enterprise." By the time Cisco reaches the last stage of its planned journey, which will take several years, the company will be increasingly location- and service-independent—and enterprise data still will be secure.[9]

In 2012, Cisco added about 11,000 smartphones and tablet computers companywide—or about 1,000 new Internet-enabled devices per month. "At the end of 2012, there were nearly 60,000 smartphones and tablets in use in the organization—including just under 14,000 iPads—and all of them were Bring Your Own (BYO)," says a Brett Belding, Senior Manager Overseeing Cisco IT Mobility Services. "Mobile at Cisco is now BYO, period."

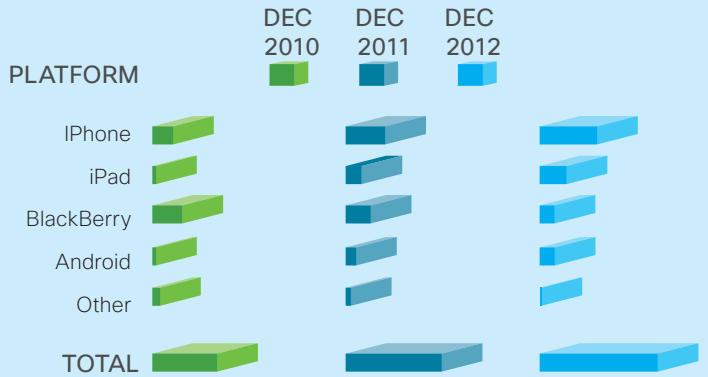
The device type that's seen the biggest increase in use at Cisco is the Apple iPad. "It's fascinating to think that three years ago, this product didn't even exist," says Belding. "Now, there are more than 14,000 iPads being used at Cisco every day by our employees for a variety of activities—both personal- and work-related. And employees are using iPads in addition to their smartphones."

As for smartphones, the number of Apple iPhones in use at Cisco has almost tripled in two years' time to nearly 28,600. RIM BlackBerry, Google Android, and Microsoft Windows devices are also included in the BYOD program at Cisco. Employees make the choice to trade having access to corporate data on their personal device with agreement on security controls. For example, if you want to check your email and calendar on your device, you have to take Cisco's security profile that enforces remote wipe, encryption, and passphrase.

"We have more devices supported than ever before and, at the same time, we've had the fewest number of support cases. Our goal is that someday an employee can simply bring in any device and self-provision using the Cisco Identity Services Engine (ISE) and set up our core WebEx collaboration tools, including Meeting Center, Jabber, and WebEx Social."

Brett Belding, Senior Manager Overseeing Cisco IT Mobility Services

Figure 2



"I understand you need to keep the enterprise secure, but don't interfere with my user experience."

Brett Belding, Senior Manager Overseeing Cisco IT Mobility Services

Social support has been a key component of the BYOD program at Cisco from the start. "We rely heavily on [the enterprise collaboration platform] WebEx Social as our BYOD support platform, and it's paid huge dividends," says Belding. "We have more devices supported than ever before and, at the same time, we've had the fewest number of support cases. Our goal is that someday an employee can simply bring in any device and self-provision using the Cisco Identity Services Engine (ISE) and set up our core WebEx collaboration tools, including Meeting Center, Jabber, and WebEx Social."

The next step for BYOD at Cisco, according to Belding, is to further improve security by increasing visibility and control over all user activity and devices, on both the physical network and virtual infrastructure, while improving the user experience. "Caring about the user experience is a core consumerization of IT trend," says Belding. "We're trying to apply this concept to our organization. We have to. I think what we're seeing now is an 'IT-ization' of users. We're beyond the point of them asking, 'Can I use this device at work?' Now they're saying, 'I understand you need to keep the enterprise secure, but don't interfere with my user experience.'"

Services Reside in Many Clouds

Global data center traffic is on the rise. According to the Cisco Global Cloud Index, global data center traffic is expected to quadruple over the next five years and will grow at a compound annual growth rate (CAGR) of 31 percent between 2011 and 2016.[10]

Of this tremendous growth, the fastest-growing component is cloud data. Global cloud traffic will increase six-fold over the next five years, growing at a rate of 44 percent from 2011 to 2016. In fact, global cloud traffic will make up nearly two-thirds of total data center traffic by 2016.[11]

This explosion in cloud traffic raises questions about the ability of enterprises to manage this information. In the cloud, the lines of control are blurred: Can an organization place safety nets around its cloud data when they don't own and operate the data center? How can even basic security tools such as firewalls and antivirus software be applied when the network edge cannot be defined?

No matter how many security questions are raised, it's clear more and more enterprises are embracing the benefits of clouds—and those

Global cloud traffic will increase six-fold over the next five years, growing at a rate of 44 percent from 2011 to 2016.

that have are not likely to return to a the private data center model. While the opportunities of the cloud for organizations are many—including cost savings, greater workforce collaboration, productivity, and a reduced carbon footprint—the possible security risks that enterprises face as a result of moving business data and processes to the cloud.

Hypervisors

If compromised, this software that creates and runs virtual machines could lead to mass hacking or data compromise against multiple servers—applying the same ease of management and access that virtualization provides to a successful hack. A rogue hypervisor (taken control of by "hyperjacking") can take complete control of a server.[12]

A rogue hypervisor (taken control of by "hyperjacking") can take complete control of a server.

Lowered cost of entry

Virtualization has lowered the cost of entry to provide services like a virtual private server (VPS). Compared to older hardware-based data center models, we are seeing a growth in quick, cheap, and easily available infrastructure for criminal activities. For instance, there are many VPS services available for instant sale (with the ability to purchase using Bitcoin or other hard-to-trace payment types) that are targeted to the criminal underground. Virtualization has made infrastructure much cheaper and easier to provide—with little to no policing of activities.

"Decoupling" of virtualized applications

Because virtualized applications are decoupled from the physical resources they use, it becomes more difficult for enterprises to apply traditional security approaches. IT providers seek to minimize cost with a very elastic offering in which they can move resources as needed—contrasted with the security group seeking to collocate services of like security posture and keep them apart from others that may be less secure.

"Virtualization and cloud computing create problems just like those of BYOD, but turned on their head," says Joe Epstein, former Chief Executive Officer of Virtuata, a company acquired by Cisco in 2012 that provides innovative capabilities for securing virtual machine-level information in data centers and cloud environments. "High-value applications and high-value data are now moving around the data center. And the notion of virtual workloads makes enterprises uncomfortable. In the virtual environment, how do you know you can trust what you're running? The answer is that you haven't been able to so far—and that uncertainty has been a key barrier to cloud adoption."

But Epstein notes that it is becoming increasingly difficult for enterprises to ignore virtualization and the cloud. "The world is going to share everything," he says. "Everything will be virtualized; everything will be shared. It will not make sense to continue running only private data centers; hybrid clouds are where IT is heading."

"Virtualization and cloud computing create problems just like those of BYOD, but turned on their head... High-value applications and high-value data are now moving around the data center."

Joe Epstein, Former Chief Executive Officer of Virtuata

The answer to these growing cloud and virtualization challenges is adaptive and responsive security. In this case, security must be a programmable element seamlessly integrated into the underlying data center fabric, according to Epstein. In addition, security needs to be built in at the design phase, instead of being bolted on post-implementation.

Blending of Business and Personal Use

Millennials and the Workplace

Modern workers—particularly young "Millennials"—want the freedom to browse the web not only when and how they want to, but also with the devices they choose. However, they don't want these freedoms impinged upon by their employers, a situation that can spell tension for security professionals.

According to the *2012 Cisco Connected World Technology Report* study, two-thirds of respondents believe employers should not track employees' online activities on company-issued devices. In short, they do not think employers have any business monitoring such behavior. Only about one-third (34 percent) of workers surveyed say they don't mind if employers track their online behavior.

Only one in five respondents say their employers do track their online activities on company-owned devices, while 46 percent say their employers do not track activity. Findings for the latest *Connected World* study also show that Millennials have strong feelings about employers' tracking the online activity of workers—even those who report they work at organizations where such tracking does not occur.

Only one in five respondents say their employers do track their online activities on company-owned devices, while 46 percent say their employers do not track activity.

Compounding the challenges for security professionals, there appears to be a disconnect between what employees think they can do with their company-issued devices and what policies IT actually dictates about personal usage. Four out of 10 respondents say they are supposed to use company-issued devices for work activity only, while a quarter say they are allowed to use company devices for non work activity. However, 90 percent of IT professionals surveyed say they do indeed have policies that prohibit company-issued devices being used for personal online activity—although 38 percent acknowledge that employees break policy and use devices for personal activities in addition to doing work. You can find information about Cisco's approach to these BYOD challenges on page 16.

There appears to be a disconnect between what employees think they can do with their company-issued devices and what policies IT actually dictates about personal usage.

Privacy and Millennials

According to the *2012 Cisco Connected World Technology Report*, Millennials have accepted the fact that, thanks to the Internet, personal privacy may be a thing of the past. 91 percent of young consumers surveyed say that the age of privacy is over and believe they can't control the privacy of their information, with one third of respondents reporting they are not worried about the data that is stored and captured about them.

In general, Millennials also believe their online identity is different from their offline identity. 45 percent say these identities are often different depending on the activity in question, while 36 percent believe these identities are completely different.
Only 8 percent believe these identities are the same.

Young consumers also have high expectations that websites will keep their information private, often feeling more comfortable sharing data with large social media or community sites given the cloak of anonymity the crowd provides. Forty-six percent say they expect certain websites to keep their information secure, while 17 percent say they trust most websites to keep their information private. However, 29 percent say that not only do they not trust websites to keep their information private; they are very concerned about security and identity theft. Compare this to the idea of sharing data with an employer who has the context about who they are and what they do.

"Millennials are now entering the workplace and bringing with them new working practices and attitudes to information and the associated security thereof. They believe in the demise of privacy—that it's simply defunct in practice, and it's in this paradigm that organizations must operate—a concept that will be alarming to the older generation in the workplace," says Adam Philpott, Director, EMEAR Security Sales, Cisco. "Organizations can, however, look to provide information security education to their employees to alert them to the risks and provide guidance on how best to share information and leverage online tools within the realms of data security."

"Millennials are now entering the workplace and bringing with them new working practices and attitudes to information and the associated security thereof. They believe in the demise of privacy—that it's simply defunct in practice, and it's in this paradigm that organizations must operate—a concept that will be alarming to the older generation in the workplace."

Adam Philpott, Director, EMEAR Security Sales, Cisco

Why Enterprises Need to Raise Awareness of Social Media Disinformation

by Jean Gordon Kocienda
Global Threat Analyst, Cisco

Social media has been a boon for many enterprises; the ability to connect directly with customers and other audiences via Twitter and Facebook has helped many organizations build brand awareness via online social interaction.

The flip side of this lightning-fast direct communication is that social media can allow inaccurate or misleading information to spread like wildfire. It isn't hard to imagine a scenario in which a terrorist coordinates on-the-ground attacks by using misleading tweets with the intent to clog roads or phone line, or to send people into the path of danger. One example: India's government blocked hundreds of websites and curbed texts(footnote:13) this summer in an attempt to restore calm in north-eastern part of the country after photographs and text messages were posted. The rumors prompted thousands of panicked migrant workers to flood train and bus stations.

Similar social media disinformation campaigns have affected market prices as well. A hijacked Reuters' Twitter feed reported that the Free Syrian Army had collapsed in Aleppo. A few days later, a Twitter feed was compromised, and a purported top Russian diplomat tweeted that Syrian President Bashar Al-Assad was dead. Before these accounts could be discredited, oil prices on international markets spiked.[14]

Security professionals need to be alert to such fast-moving and potentially damaging social media posts, especially if they are directed at the enterprise itself—and quick action is needed to defend networks from malware, alert employees to a bogus phishing attempt, re-route a shipment, or advise employees regarding safety. The last thing security executives want to do is alert managers to a breaking story that turns out to be a hoax.

The first safeguard against falling for fabricated stories is to confirm the story across multiple sources. At one time, journalists did this job for us, so that by the time we read or heard the news, it was vetted. These days, many journalists are getting their stories from the same Twitter feeds that we are, and if several of us fall for the same story, we can easily mistake re-tweets for story confirmation.

For fast-breaking news requiring quick action, your best bet may be to use the old-fashioned "sniff test." If the story seems far-fetched, think twice before repeating or citing it.[15]

For fast-breaking news requiring quick action, your best bet may be to use the old-fashioned "sniff test." If the story seems far-fetched, think twice before repeating or citing it.

Big Data

A Big Deal for Today's Enterprises

The business world is abuzz about "big data"—and the potential for analytics "gold" that can be mined from the vast volumes of information that enterprises generate, collect, and store.

The *2012 Cisco Connected World Technology Report* examined the impact of the big-data trend on enterprises—and more specifically, their IT teams. According to the study's findings, about three-quarters (74 percent) of organizations globally are already collecting and storing data, and management is using analysis of big data to make business decisions. Additionally, seven in 10 IT respondents reported that big data will be a strategic priority for their company and IT team in the year ahead.

As mobility, cloud, virtualization, endpoint proliferation, and other networking trends evolve or emerge, they will pave the way for even more big data and analytics opportunities for businesses. But there are security concerns about big data. The 2012 *Connected World* study's findings show that a third of respondents (32 percent) believe big data complicates security requirements and protection of data and networks because there is so much data and too many ways of accessing it. In short, big data increases the vectors and angles that enterprise security teams—and security solutions—must cover.

About 74 percent of organizations globally are already collecting and storing data, and management is using analysis of big data to make business decisions.

Korea, Germany, the United States, and Mexico had the highest percentages of IT respondents who believe big data complicates security.

Korea (45 percent), Germany (42 percent), the United States (40 percent), and Mexico (40 percent) had the highest percentages of IT respondents who believe big data complicates security. To help ensure security, the majority of IT respondents—more than two-thirds (68 percent)—believe the entire IT team should participate in strategizing and leading big data efforts within their companies. Gavin Reid, Director of Threat Research for Cisco Security Intelligence Operations, says "Big data doesn't complicate security—it makes it possible. At Cisco we collect and store 2.6 trillion records every day—that forms the platform from which we can start incident detection and control."

As for solutions designed to help enterprises both better manage and unlock the value of their big data, there are barriers to adoption. Respondents pointed to lack of budget, lack of time to study big data, lack of appropriate solutions, lack of IT staff, and lack of IT expertise. The fact that almost one in four respondents globally (23 percent) said lack of expertise and personnel was an inhibitor to their enterprise's ability to use big data effectively indicates a need for more professionals entering the job market to be trained in this area.

The cloud is a factor in big data success, as well, according to 50 percent of IT respondents to the 2012 *Connected World* study. They believe their organizations need to work through cloud plans and deployments to make big data a worthwhile venture. This sentiment was prominent in China (78 percent) and India (76 percent), where more than three out of four respondents believed there was a dependency on cloud before big data could truly take off. As a result, in some cases, the study indicates cloud adoption will impact the rate of adoption—and benefits—of big-data efforts.

As for solutions that are designed to help enterprises both better manage and unlock the value of their big data, there are barriers to adoption. Respondents pointed to lack of budget, lack of time to study big data, lack of appropriate solutions, lack of IT staff, and lack of IT expertise.

More than half of overall IT respondents also confirmed that big-data discussions within their companies are not fruitful yet. That is not surprising considering the market is just now trying to understand how to harness their big data, analyze it, and use it strategically. In some countries, however, big-data discussions are resulting in meaningful decisions on strategy, direction, and solutions. China (82 percent), Mexico (67 percent), India (63 percent), and Argentina (57 percent) lead in this regard, with well over half of the respondents from these countries claiming that big-data discussions in their organizations are well underway—and leading to solid actions and results.

Three out of five IT respondents to the *2012 Connected World Report* believe big data can help countries and their economies become more competitive in the global marketplace.

There are some countries where big-data discussions are resulting in meaningful decisions on strategy, direction, and solutions. China, Mexico, India, and Argentina lead in this regard, with well over half of the respondents from these countries claiming that big-data discussions in their organizations are well underway—and leading to solid actions and results.

State of the Exploit

Danger Lurks in Surprising Places

Many security professionals—and certainly a large community of online users—hold preconceived ideas about where people are most likely to stumble across dangerous web malware.

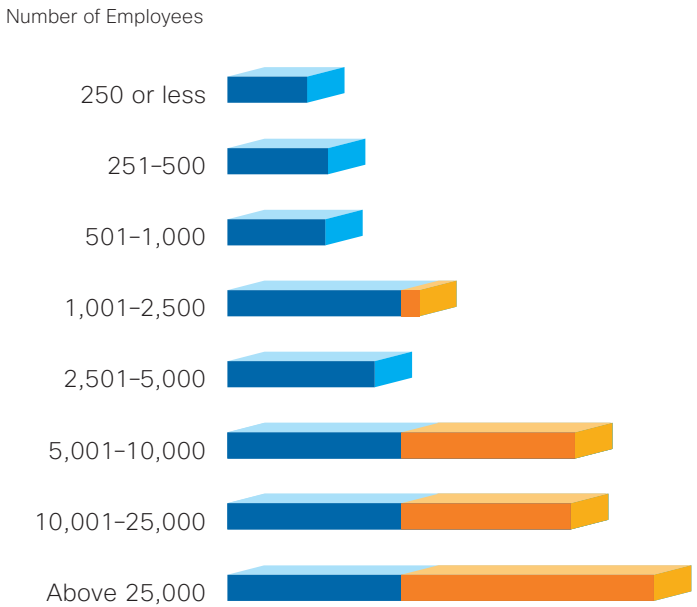
The general belief is that sites that promote criminal activity—such as sites selling illegal pharmaceuticals or counterfeit luxury goods—are most likely to host malware. Our data reveals the truth of this outdated notion, as Web malware encounters are typically not the by-product of "bad" sites in today's threat landscape.

"Web malware encounters occur everywhere people visit on the Internet—including the most legitimate of websites that they visit frequently, even for business purposes,"says Mary Landesman, Senior Security Researcher with Cisco. "Indeed, business and industry sites are one of the top three categories visited when a malware encounter occurred. Of course, this isn't the result of business sites that are designed to be malicious." The dangers, however, are often hidden in plain sight through exploit-laden online ads that are distributed to legitimate websites, or hackers targeting the user community on the common sites they use most.

In addition, malware-infected websites are prevalent across many countries and regions—not just in one or two countries, dispelling the notion that some countries' websites are more likely to host malicious content than others. "The web is the most formidable malware delivery mechanism we've seen to date, outpacing even the most prolific

Dangers are often hidden in plain sight through exploit-laden online ads.

Figure 3: Risk by Company Size
Up to 2.5 times more risk of encountering web malware for large organizations.



All companies—regardless of size—face significant risk of web malware encounters. Every organization should focus on the fundamentals of securing its network and intellectual property.

worm or virus in its ability to reach—and infect—a mass audience silently and effectively," says Landesman. "Enterprises need protection, even if they block common 'bad' sites, with additional granularity in inspection and analysis."

Malware Encounters by Company Size

The largest enterprises (25,000+ employees) have more than 2.5 times the risk of encountering web malware than smaller companies. This increased risk may be a reflection that larger companies possess more high-value intellectual property and thus are more frequently targeted.

While smaller companies have fewer web malware encounters per user, it's important to note that all companies—regardless of size—face significant risk of web malware encounters. Every organization should focus on the fundamentals of securing it's network and intellectual property.

Malware Encounters by Country

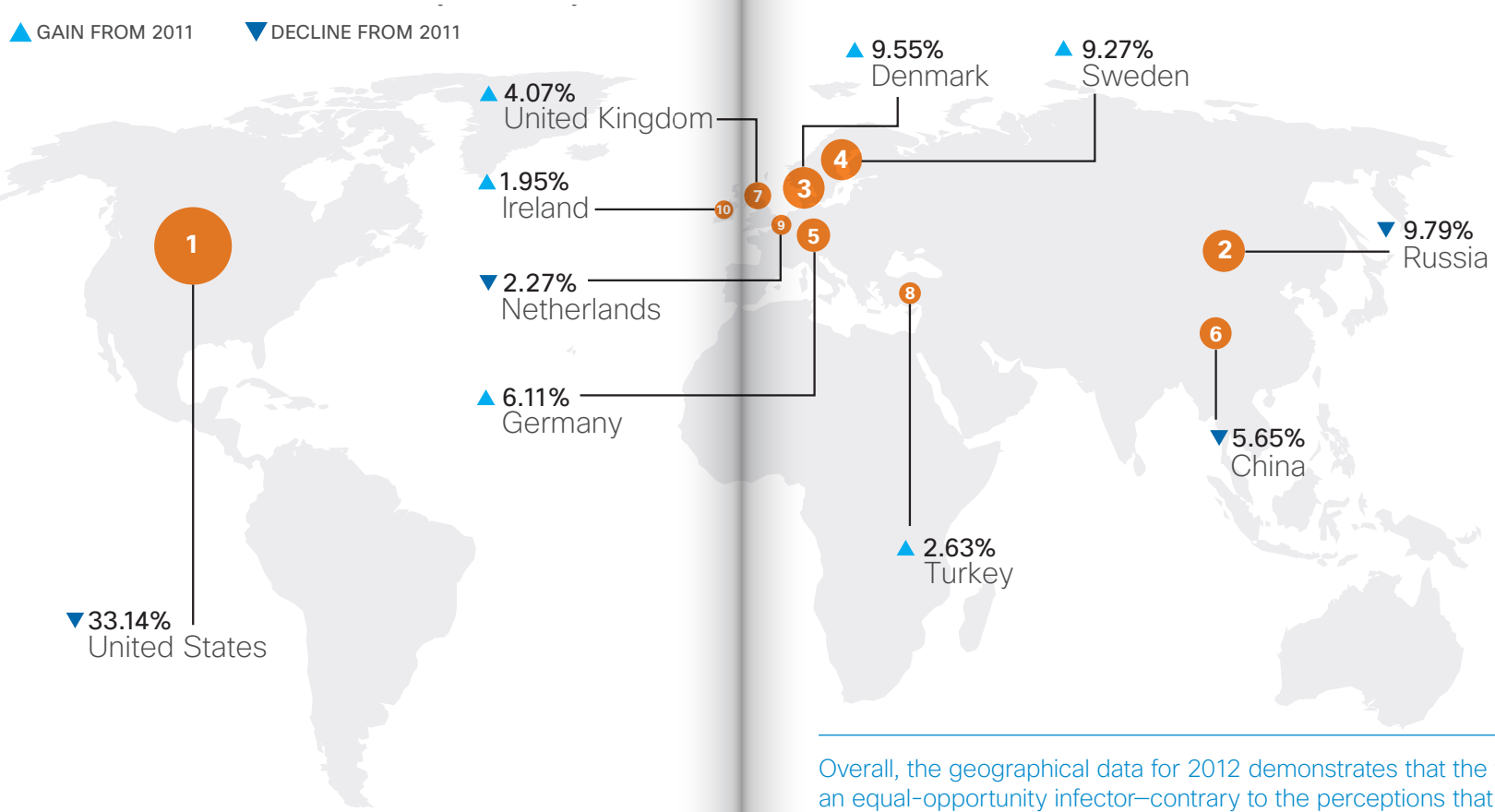
Cisco's research shows significant change in the global landscape for web malware encounters by country in 2012. China, which was second on the list in 2011 for web malware encounters, fell dramatically to sixth position in 2012. Denmark and Sweden now hold the third and fourth spots, respectively. The United States retains the top ranking in 2012, as it did in 2011, with 33 percent of all web malware encounters occurring via websites hosted in the United States.

Changes in geographical location between 2011 and 2012 likely reflect both changes in detection and user habits. For example, "malvertising," or malware delivered via online ads, played a more significant role in web malware encounters in 2012 than in 2011. It is worth repeating that web malware encounters most frequently occur via normal browsing of legitimate websites that may have been compromised or are unwittingly serving malicious advertising. Malicious advertising can impact any website, regardless of the site's origin.

Overall, the geographical data for 2012 demonstrates that the web is an equal-opportunity infector—contrary to the perceptions that only one or two countries are responsible for hosting web malware or that any one country is safer than another. Just as the dynamic content delivery of Web 2.0 enables the monetization of websites across the globe, it can also facilitate the global delivery of Web malware.

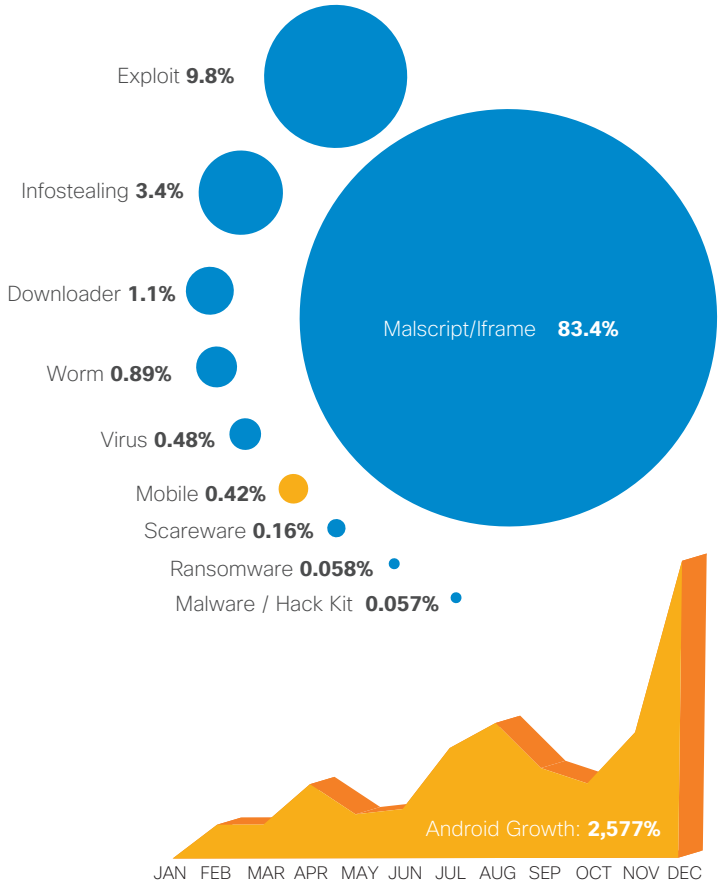
Figure 4: Web Malware Encounters by Country

One-third of all web malware encounters resulted from domains hosted in the United States.



Overall, the geographical data for 2012 demonstrates that the web is an equal-opportunity infector—contrary to the perceptions that only one or two countries are responsible for hosting web malware or that any one country is safer than another.

Figure 5: Top Web Malware Types
Android malware encounters grew 2,577 percent over 2012, though mobile malware only makes up a small percentage of total web malware encounters.



Of course, there is a distinct difference between where a Web malware encounter occurs and where the malware is actually hosted. In malvertising, for example, the encounter typically occurs when visiting a reputable, legitimate website that happens to carry third-party advertising. However, the actual malware intended for delivery is hosted on a completely different domain. Since our data is based on where the encounter occurred, it has no bearing on actual malware origin. For instance, increased popularity of social media and entertainment sites in Denmark and Sweden, coupled with malvertising risks, is largely responsible for increased encounters from sites hosted in those regions but is not indicative of actual malware origin.

Top Web Malware Types in 2012

Android malware grew substantially faster than any other form of web-delivered malware, an important trend given that Android is reported to hold the majority of mobile device market share worldwide. It is important to note that mobile malware encounters comprised only 0.5 percent of all web malware encounters in 2012, with Android taking over 95% of all these web malware encounters. In addition, 2012 saw the emergence of the first documented Android botnet in the wild, indicating that mobile malware developments in 2013 bear watching.

While some experts are claiming Android is the "biggest threat" or should be a primary focus for enterprise security teams in 2013—the actual data shows otherwise. As noted above, mobile web malware in general makes up less than 1 percent of total encounters—far from the "doomsday" scenario many are detailing. The impact of BYOD and the proliferation of devices cannot be overstated, but organizations should be more concerned with threats such as accidental data loss, ensuring employees do not "root" or "jailbreak" their devices, and only install applications from official and trusted distribution channels. If users choose to go outside official mobile app stores, they should ensure, before downloading an app, that they know and trust the app's author and can validate that the code has not been tampered with.

Looking at the wider landscape for web malware, it is not surprising that malicious scripts and iFrames comprised 83 percent of encounters in 2012. While this is relatively consistent with previous years,

it's a finding worthy of reflection. These types of attacks often represent malicious code on "trusted" webpages that users may visit every day—meaning an attacker is able to compromise users without even raising their suspicion.

Exploits take the second spot, with 10 percent of the total number of web malware encounters last year. However, these figures are largely a result of where the block occurred versus actual concentration of exploits on the web. For example, the 83 percent of malicious scripts and hidden iFrames are blocks that occur at an earlier stage, prior to any exploit rendering; hence, they may artificially decrease the number of exploits observed.

Exploits remain a significant cause of infection via the web, and their continued presence underscores the need for vendors to adopt security best practices in their product lifecycles. Organizations should focus on security as part of the product design and development process, with timely vulnerability disclosures, and prompt/regular patch cycles. Organizations and users also need to be made aware of the security risks associated with using products that are no longer supported by vendors.

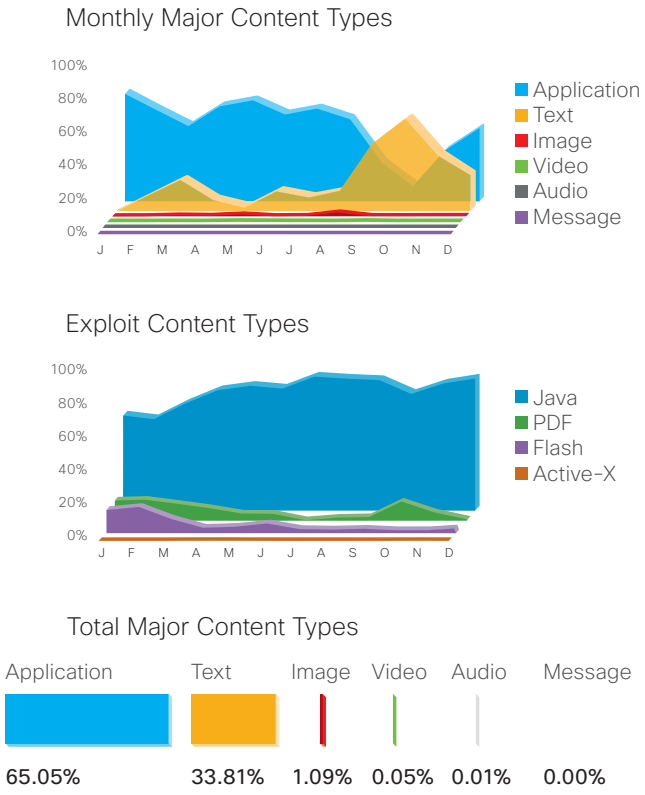
It is also critical for organizations to maintain a core vulnerability management process and for users keep to their hardware and software up to date.

Rounding out the top five are infostealers, with 3.5 percent of the total web malware encounters in 2012, downloaders (1.1 percent), and worms (0.8 percent). Once again, these numbers are a reflection of where the block occurs, generally at the point in which the malicious script or iFrame is first encountered. As a result, these numbers are not reflective of the actual number of infostealers, downloaders, or worms being distributed via the web.

Top Malware Content Types

Malware creators constantly seek to maximize their return on investment (ROI) by finding ways to reach the largest population of potential victims with the least effort, and they often take advantage of cross-platform technologies when possible. Toward these ends, exploit toolkits generally deliver exploits in a specific order; once a successful exploit has been delivered, no further exploits are attempted. The high concentration of Java exploits—87 percent of total web exploits—shows that these

Figure 6: Top Malware Content Types for 2012
Java exploits comprised 87 percent of total web exploits.

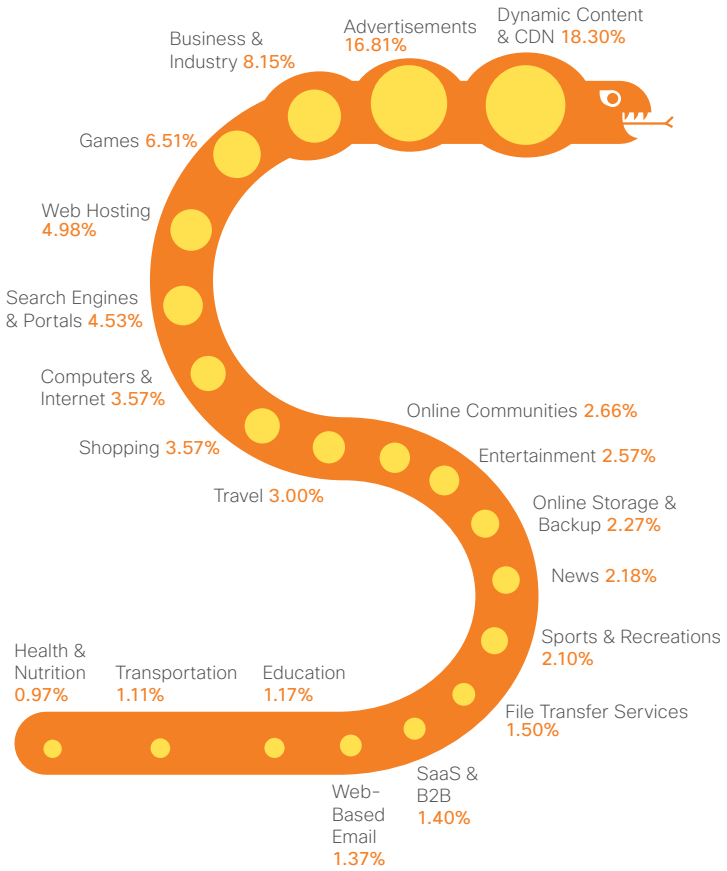


The high concentration of Java exploits shows that these vulnerabilities are attempted prior to other types of exploits and also demonstrates that attackers are finding success with Java exploits.

Figure 7: Top Site Category

Online shopping sites are 21 times more likely to deliver malicious content than counterfeit software sites.

Note: The "Dynamic Content" category is at the top of Cisco's list of top locations for the likelihood of malware infections. This category includes content-delivery systems such as web statistics, site analytics, and other non-advertising-related third-party content.



vulnerabilities are attempted prior to other types of exploits and also demonstrates that attackers are finding success with Java exploits. Additionally, with over 3 billion devices running Java,[16] the technology represents a clear way for hackers to scale their attacks across multiple platforms.

Two other cross-platform technologies—PDF and Flash—took the second and third spots in Cisco's analysis of the top content types for malware distribution. Though Active X is still being exploited, Cisco researchers have seen a consistently low use of the technology as a vehicle for malware. However, as noted earlier regarding Java, lower numbers of certain types of exploits are largely a reflection of the order in which exploits are attempted.

In examining media content, Cisco data reveals almost twice as much image-based malware than non-Flash video. However, this is due, in part, to the way browsers handle declared content types, and attackers' efforts to manipulate these controls by declaring erroneous content types. In addition, malware command-and-control systems often distribute server information via comments hidden in ordinary image files.

Top Site Category

As Cisco data shows, the notion that malware infections most commonly result from "risky" sites such as counterfeit software is a misconception. Cisco's analysis indicates that the vast majority of web malware encounters actually occur via legitimate browsing of mainstream websites. In other words, the majority of encounters happen in the places that online users visit the most—and think are safe.

Holding the second spot on the list are online advertisements, comprising 16 percent of total web malware encounters. Syndicated advertising is a common means of monetizing websites, so a single malicious ad distributed in this manner can have a dramatic, adverse impact.

The vast majority of web malware encounters actually occur via legitimate browsing of mainstream websites. In other words, the majority of encounters happen in the places that online users visit the most—and think are safe.

Cybercriminals have paid close attention to modern browsing habits to expose the latest possible deliver population to malware.

Looking further down the list of site categories through which malware encounters occurred, business and industry sites—which include everything from corporate sites to human resources to freight services—are in third place. Online gaming is in fourth place, followed by web hosting sites and search engines in fifth and sixth places, respectively. The top 20 website categories are absent of sites typically thought of as malicious. There is a healthy mix of popular and legitimate site types such as online shopping (#8), news (#13), and SaaS/business-to-business applications (#16).

Cybercriminals have paid close attention to modern browsing habits to expose the latest possible deliver population to malware. Where the online users are, malware creators will follow, taking advantage of trusted websites through direct compromise or third-party distribution networks.

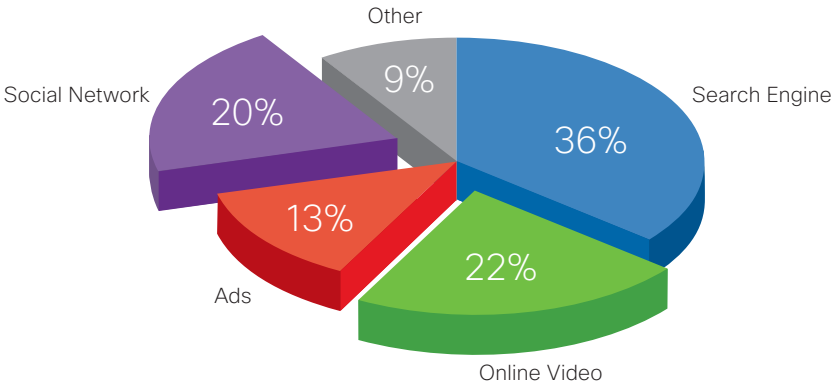
Popular Applications by Hits

Changes in how people spend their time online are expanding the surface for cybercriminals to launch exploits. Organizations of all sizes are embracing social media and online video; most major brands have a presence on Facebook and Twitter, and many are integrating social media into their actual products. As these web destinations draw massive audiences and are accepted into enterprise settings, more opportunities to deliver malware are also created.

According to data from Cisco Application Visibility and Control (AVC), the vast majority (91 percent) of web requests were split among search engines (36 percent); online video sites (22 percent); advertising networks (13 percent); and social networks (20 percent).

Organizations of all sizes are embracing social media and online video; most major brands have a presence on Facebook and Twitter, and many are integrating social media into their actual products.

Figure 8: Popular Applications by Hits
Social media and online video change how employees spend their time at work—and expose new vulnerabilities.



If the data on the top websites visited across the Internet is correlated with the most dangerous category of website, the very same places online users have the most exposure to malware, such as search engines, are among the top areas that drive web malware encounters.

If the data on the top websites visited across the Internet is correlated with the most dangerous category of website, the very same places online users have the most exposure to malware, such as search engines, are among the top areas that drive web malware encounters. This correlation shows once again that malware creators are focused on maximizing their ROI—and therefore, they will center their efforts on the places where the number of users and ease of exposure are greatest.

When Gothic Horror Gives Birth to Malware

by Kevin W. Hamlen
Associate Professor, Computer Science Department, The University of Texas at Dallas

Malware camouflage is an emerging threat that security professionals may increasingly face. While most malware already uses simple mutation or obfuscation to diversify and make itself harder to reverse-engineer, self-camouflaging malware is even stealthier, blending in with the specific software already present on each system it infects. This can elude defenses that look for software anomalies like runtime unpacking or encrypted code, which often expose more conventional malware.

The latest self-camouflaging malware technology—appropriately dubbed Frankenstein[17]—is a product of our research this year in the Cyber Security Research and Education Center at The University of Texas at Dallas. Like the fictional mad scientist in Mary Shelley's 1818 horror novel, "Frankenstein malware" creates mutants by stealing body parts (i.e., code) from other software it encounters and stitches the code together to create unique variants of itself. Each Frankenstein mutant is therefore composed entirely of non-anomalous, benign-looking software; performs no suspicious runtime unpacking or encryption; and has access to an ever-expanding pool of code transformations learned from the many programs it encounters.

Under the hood, Frankenstein brings its creations to life using an array of techniques drawn from compiler theory and program analysis. Victim binaries are first scanned for short byte sequences that decode to potentially useful instruction sequences, called *gadgets*. A small abstract interpreter next infers the possible semantic effects of each gadget discovered. Backtracking search is then applied to discover gadget sequences that, when executed in order, have the effect of implementing the malware payload's malicious behavior.

Like the fictional mad scientist in Mary Shelley's 1818 horror novel, "Frankenstein malware" creates mutants by stealing body parts (i.e., code) from other software it encounters and stitches the code together to create unique variants of itself.

In general, our research suggests that next-generation malware may increasingly eschew simple mutations based on encryption and packing in favor of advanced metamorphic binary obfuscations like those used by Frankenstein.

Each such discovered sequence is finally assembled to form a fresh mutant. In practice, Frankenstein discovers over 2,000 gadgets per second, accumulating over 100,000 from just two or three victim binaries in under five seconds. With such a large gadget pool at their disposal, the resulting mutants rarely share any common instruction sequences; each therefore looks unique.

In general, our research suggests that next-generation malware may increasingly eschew simple mutations based on encryption and packing in favor of advanced *metamorphic* binary obfuscations like those used by Frankenstein. Such obfuscations are feasible to implement, support rapid propagation, and are effective for concealing malware from the static analysis phases of most malware detection engines. To counter this trend, defenders will need to deploy some of the same technologies used to develop Frankenstein, including static analyses based on semantic, rather than syntactic, feature extraction, and semantic signatures derived from machine learning[18] rather than purely manual analysis.

This article reports research supported in part by National Science Foundation (NSF) award #1054629 and U.S. Air Force Office of Scientific Research (AFOSR) award FA9550-10-1-0088. Any opinions, findings, conclusions, or recommendations expressed are those of the author and do not necessarily reflect those of the NSF or AFOSR.

[17] Vishwath Mohan and Kevin W. Hamlen. "Frankenstein: Stitching Malware from Benign Binaries." In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, pp. 77-84, August 2012.

[18] Mohammad M. Masud, Tahseen M. Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han, and Bhavani Thuraisingham. "Cloud-based" Malware Detection for Evolving Data Streams. *ACM Transactions* on Management Information Systems (TMIS), *2*(3), October 2011.

2012 Vulnerability and Threat Analysis

The Vulnerability and Threat Categories chart shows a significant increase in threat totals—in 2012, threats increased 19.8 percent over 2011. This sharp increase in threats is placing a serious strain on the ability of organizations to keep vulnerability management systems updated and patched—especially given the shift to virtual environments.

Organizations are also attempting to address the increasing use of third-party and open-source software included in their products and in their environments. "Just one vulnerability in third-party or open-source solutions can impact a broad range of systems across the environment, which makes it very difficult to identify and patch or update all those systems," says Jeff Shipley, Manager of Cisco Security Research and Operations.

As for the types of threats, the largest group is resource management threats; this generally includes denial of service vulnerabilities, input validation threats such as SQL injection and cross-site scripting errors, and buffer overflows that result in denial of service. The preponderance of similar threats from previous years, combined with the sharp increase in threats, indicates that the security industry needs to become better equipped at detecting and handling these vulnerabilities.

The Cisco IntelliShield Alert Urgency Ratings reflect the level of threat activity related to specific vulnerabilities. The substantial increase in Level 3 urgency ratings indicates that more vulnerabilities are actually being exploited. This is likely due to the increase in publicly released exploits either by researchers or test tools, and the incorporation of those exploits into attack toolkits. These two factors are allowing more exploits to be available and used across the board by hackers and criminal groups.

The Cisco IntelliShield Alert Severity Ratings reflect the impact level of successful vulnerability exploits. The severity ratings also show a noticeable increase in Level 3 threats—for the same reasons indicated above relating to the ready availability of exploit tools.

Figure 9: Urgency and Severity Ratings

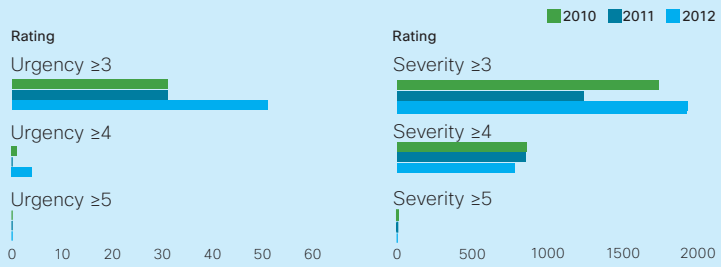
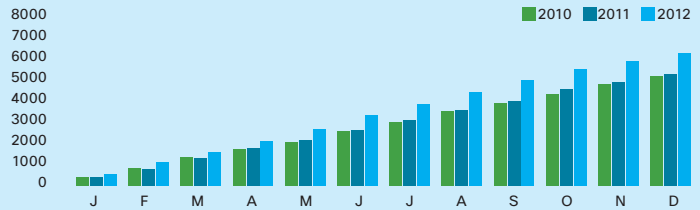


Figure 10: Vulnerability and Threat Categories

	2010 Monthly Alert Numbers				2011 Monthly Alert Numbers				2012 Monthly Alert Numbers			
	Total	Reamp	New		Total	Reamp	New		Total	Reamp	New	
January	417	259	158	417	403	237	166	403	552	344	208	552
February	430	253	177	847	400	176	224	803	551	317	234	1103
March	518	324	194	1364	501	276	225	1304	487	238	249	1590
April	375	167	208	1740	475	229	246	1779	524	306	218	2114
May	322	174	148	2062	404	185	219	2183	586	343	243	2700
June	534	294	240	2596	472	221	251	2655	647	389	258	3347
July	422	210	212	3018	453	213	240	3108	514	277	237	3861
August	541	286	255	3559	474	226	248	3582	591	306	285	4452
September	357	167	190	3916	441	234	207	4023	572	330	242	5024
October	418	191	227	4334	558	314	244	4581	517	280	237	5541
November	476	252	224	4810	357	195	162	4938	375	175	200	5916
December	400	203	197	5210	363	178	185	5301	376	183	193	6292
	5210	2780	2430		5301	2684	2617		6292	3488	2804	



"Just one vulnerability in third-party or open-source solutions can impact a broad range of systems across the environment, which makes it very difficult to identify and patch or update all those systems."

Jeff Shipley, Manager Cisco Security Research and Operations

Evolutionary Threats

New Methods, Same Exploits

Anything goes when it comes to cyber exploits today—as long as the method selected will get the job done.

This is not to say that actors in the shadow economy do not remain committed to creating ever-more sophisticated tools and techniques to compromise users, infect networks, and steal sensitive data, among many other goals. In 2012, however, there was a trend toward reaching back to "oldies but goodies" to find new ways to create disruption or evade enterprise security protections.

DDoS attacks are a primary example—several major U.S. financial institutions were the high-profile targets of two major and related campaigns launched by foreign hacktivist groups in the last six months of 2012 (for detailed analysis, see the 2012 Distributed Denial of Service Trends section. Some security experts warn that these events are just the beginning and that "hacktivists, organized crime rings, and even nation states will be the perpetrators"[19] of these attacks in the future, working both collaboratively and independently.

"We are seeing a trend in DDoS, with attackers adding additional context about their target site to make the outage more significant," says Gavin Reid. "Instead of doing a SYN flood, the DDoS now attempts to manipulate a specific application in the organization—potentially causing a cascading set of damage if it fails."

In 2012, however, there was a trend toward reaching back to "oldies but goodies" to find new ways to create disruption or evade enterprise security protections.

"Even against a sophisticated–but average–adversary, the current 'state of the art' in network security is often significantly outmatched."

Gregory Neal Akers, Senior Vice President for the Advanced Security Initiatives Group at Cisco

While enterprises may believe they are adequately protected against the DDoS threat, more than likely their network could not defend against the type of high-volume and relentless DDoS attacks witnessed in 2012. "Even against a sophisticated–but average–adversary, the current 'state of the art' in network security is often significantly outmatched," says Gregory Neal Akers, Senior Vice President for the Advanced Security Initiatives Group at Cisco.

Another trend in the cybercrime community revolves around the "democratization" of threats. We are increasingly seeing that the tools and techniques–and intelligence about how to exploit vulnerabilities–are being "broadly shared" in the shadow economy today. "Tradecraft capabilities have evolved a great deal," Akers says. "We're now seeing more specialization and more collaboration among malicious actors. It's a threat assembly line: Someone develops a bug, someone else writes the malware, another person designs the social engineering component, and so on."

Creating potent threats that will help them gain access to the large volumes of high-value assets coming across the network is one reason that cybercriminals are combining their expertise more often. But like any real-world organization that outsources tasks, efficiency and cost savings are among the primary drivers for the "build-a-threat" approach in the cybercrime community. The "freelance talent" hired for these tasks typically advertise their skills and pay rates to the broader cybercrime community via secret online marketplaces.

Amplification and Reflection Attacks

DNS amplification and reflection attacks[21] utilize domain name system (DNS) open recursive resolvers or DNS authoritative servers to increase the volume of attack traffic sent to a victim. By spoofing[22] DNS request messages, these attacks conceal the true source of the attack and send DNS queries that return DNS response messages 1,000 to 10,000 percent larger than the DNS request message. These types of attack profiles are commonly observed during DDoS[23] attacks.

Organizations are inadvertently participating in these attacks by leaving open recursive resolvers out on the Internet. They can detect the attacks using various tools[24] and flow telemetry[25] technologies and can help prevent them by securing[26] their DNS server or rate-limiting[27] DNS response messages.

2012 Distributed Denial of Service Trends

The following analysis is derived from the Arbor Networks ATLAS repository, which consists of global data gathered from a number of sources, including more than 240 IPSs, monitoring peak traffic of 37.8 Tbps.[28]

Attack Sizes Continue to Trend Upward

Overall, there has been an increase in the average size of attacks over the past year. There was a 27 percent increase in throughput of attacks (1.23 Gbps in 2011 to 1.57 Gbps in 2012) and a 15 percent increase in the packets per second used in attacks (1.33 Mpps in 2011 to 1.54 Mpps in 2012).

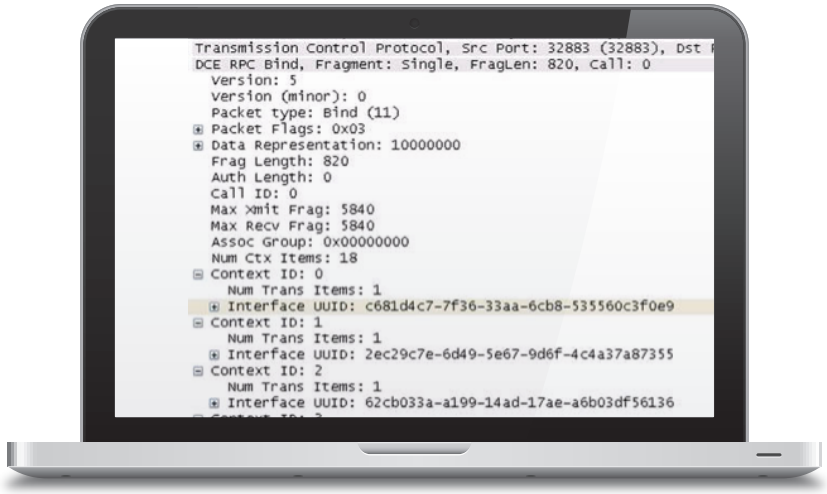
Attack Demographics

The top three monitored attack sources, after removing 41 percent of sources for which there is no attribution due to data anonymization, are China (17.8 percent), South Korea (12.7 percent), and the United States (8.0 percent).

Largest Attacks

The largest monitored attack was measured at 100.84 Gbps and lasted approximately 20 minutes (source of attack is unknown due to data anonymization). The corresponding largest monitored attack in (pps) was measured at 82.36 Mpps and lasted approximately 24 minutes (source of attack is unknown due to data anonymization).

Figure 11: Live Intrusion Prevention System (IPS) Evasions



Cisco Security Research and Operations runs several malware labs to observe malicious traffic in the wild. Malware is intentionally released in the lab to ensure security devices are effective; computers are also left intentionally vulnerable and exposed to the Internet.

Weaponization of Modern Evasion Techniques

Cybercriminals are constantly evolving new techniques to bypass security devices. Cisco researchers watch vigilantly for new techniques and the "weaponization" of well-known techniques.

Cisco Security Research and Operations runs several malware labs to observe malicious traffic in the wild. Malware is intentionally released in the lab to ensure security devices are effective; computers are also left intentionally vulnerable and exposed to the Internet.

During one such test, Cisco Intrusion Prevention System (IPS) technology detected a well-known Microsoft Remote Procedure Call (MSRPC) attack. Careful analysis determined that the attack was utilizing a previously unseen malware evasion tactic in an attempt to bypass security devices.[20] The evasion sent several bind context IDs inside the initial bind request. This type of attack can evade protections unless the IPS monitors and determines which of the IDs were successful.

Cybercriminals are constantly evolving new techniques to bypass security devices. Cisco researchers watch vigilantly for new techniques and the "weaponization" of well-known techniques.

CASE STUDY

Operation Ababil

During September and October 2012, Cisco and Arbor Networks monitored a targeted and very serious DDos attack campaign known as “Operation Ababil,” which was aimed at U.S.-based financial institutions, known as “Operation Ababil.” The DDoS attacks were premeditated, focused, advertised before the fact, and executed to the letter. Attackers were able to render several major financial sites unavailable to legitimate customers for a period of minutes—and in the most severe instances, hours. Over the course of the events, several groups claimed responsibility for the attacks; at least one group purported to be protesting copyright and intellectual property legislation in the United States. Others broadcast their involvement as a response to a YouTube video offensive to some Muslims.

From a cybersecurity standpoint, Operation Ababil is notable because it took advantage of common web applications and hosting servers that are as popular as they are vulnerable. The other obvious and uncommon factor used in this series of attacks was that simultaneous attacks, at high bandwidth, were launched against multiple companies in the same industry (financial).

As is often seen in the security industry, what’s old is new again.

On September 18, 2012, “Cyber Fighters of Izz ad-Din al-Qassam” posted on Pastebin[29] beseeching Muslims to target major financial institutions and commodities trading platforms. The threats and specific targets were put up for the world to see and continued for four consecutive weeks. Each week, new threats with new targets were followed up by actions at the appointed times and dates. By the fifth week, the group stopped naming targets but made it clear that campaigns would continue. As promised, the campaigns renewed in earnest in December 2012, once again targeting multiple large U.S. financial organizations.

Phase 2 of Operation Ababil was also announced on on Pastebin.[30] Instead of infected machines, a variety of PHP web applications, including the Joomla Content Management System, served as the primary bots in the campaign. Additionally, many WordPress sites, often using the out-of-date TimThumb plug-in, were being compromised around the same time. The attackers often went after unmaintained servers hosting these applications and uploaded PHP webshells to deploy further attack tools. The concept of “command and control” did not apply in the usual manner, however; the attackers connected to the tools directly or through intermediate servers, scripts, and proxies. During the cyber events in September and October 2012, a wide array of files and PHP-based tools were used, not just the widely reported “tsoknoproblembro” (aka “Brobot”). The second round of activity also utilized updated attack tools such as Brobot v2.

Operation Ababil deployed a combination of tools with vectors crossing application-layer attacks on HTTP, HTTPS, and DNS with volumetric attack traffic on a variety of TCP, UDP, ICMP, and other IP protocols. Cisco’s analysis showed that the majority of packets were sent to TCP/UDP port 53 (DNS) or 80 (HTTP). While traffic on UDP port 53 and TCP port 53 and 80 represent normally valid traffic, packets destined for UDP port 80 represent an anomaly not commonly used by applications.

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.[31]

Lessons Learned

While they are a critical part of any network security portfolio, IPS and firewall devices rely on stateful traffic inspection. Application-layer techniques used in the Operation Ababil campaign easily overwhelmed those state tables and, in several cases, caused them to fail. Intelligent DDoS mitigation technology was the only effective countermeasure.

Managed security services and ISPs have their limits. In a typical DDoS attack, the prevailing wisdom says to deal with volumetric attacks in the network. For application-layer campaigns that are deployed closer to the victim, these should be addressed at the data center or on the “customer edge.” Because multiple organizations were targeted concurrently, network scrubbing centers were strained.

It is critical to keep hardware and software current on DDoS mitigation appliances. Older deployments are not always able to deal with newer threats. It is also important to have the right capacity in the right locations. Being able to mitigate a large attack is useless if traffic cannot be channeled to the location where the technology has been deployed.

While cloud or network DDoS mitigation typically has much higher bandwidth capacity, on-premise solutions provide better reaction time against, control of, and visibility into the attacks. Combining the two makes for a more complete solution.

In conjunction with cloud and network DDoS technologies, and as part of the collateral produced for the Operation Ababil events, Cisco has outlined detection and mitigation techniques in the Identifying and Mitigating the Distributed Denial of Service Attacks Targeting Financial Institutions Applied Mitigation Bulletin.[32] These techniques include the use of Transit Access Control List (tACL) filtering, NetFlow data analysis, and unicast Reverse Path Forwarding (uRPF). In addition, there are a number of best practices that should be regularly reviewed, tested, and implemented that will greatly help enterprises to prepare for and react to network events. A library of these best practices can be found by referencing the Cisco SIO Tactical Resources[33] and Service Provider Security Best Practices.[34]

Spam the Ever Present

Spam volumes are continuing to decline worldwide, according to Cisco's research, but spam remains a go-to tool for many cybercriminals, who view it as an efficient and expedient way to expose users to malware and facilitate a wide range of scams.

However, despite the perception that malware is typically deployed through spam email attachments, Cisco's research shows that very few spammers today rely on this method; instead, they turn to malicious links within the email as a far more efficient distribution mechanism.

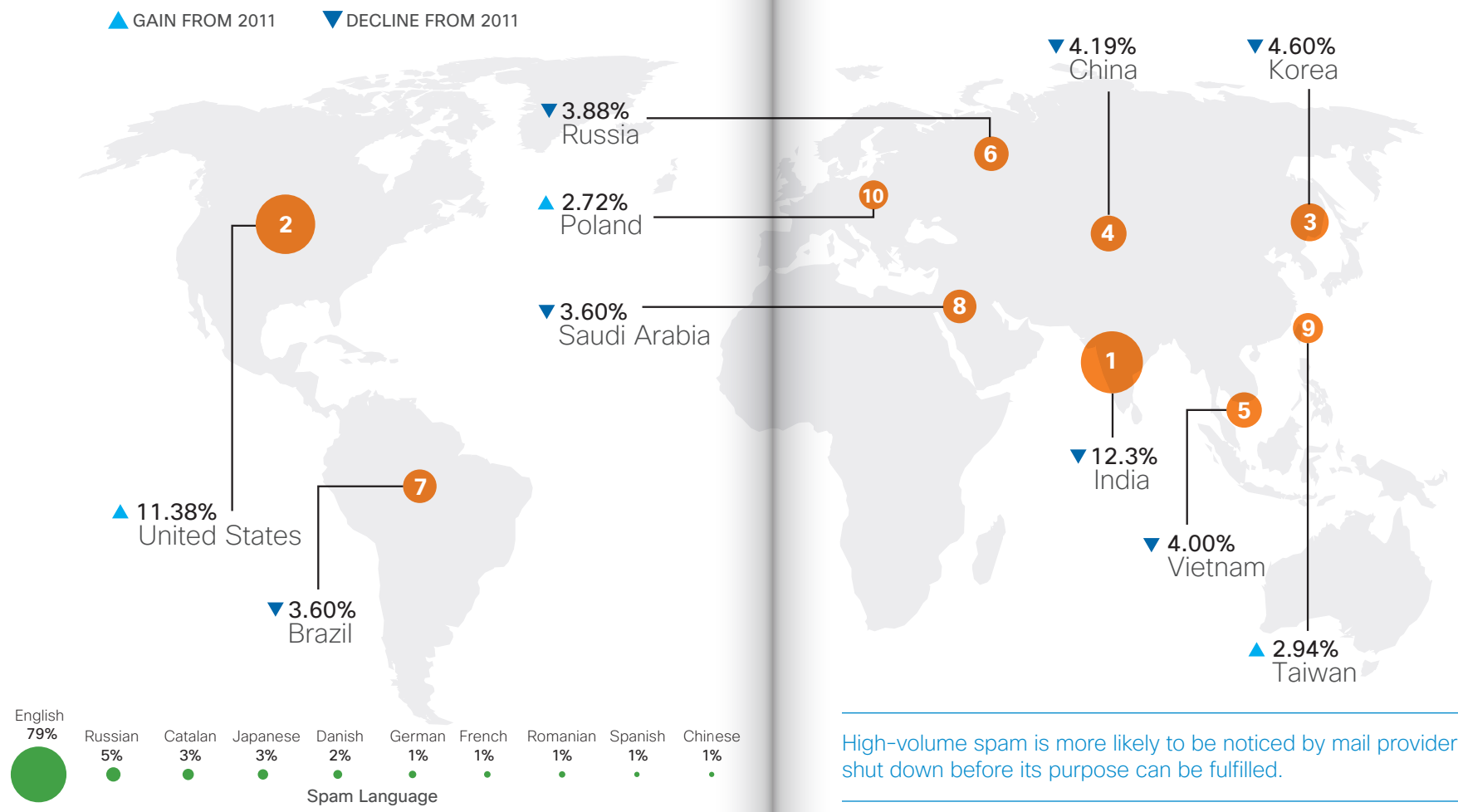
Spam is also less "scattershot" than in the past, with many spammers preferring to target specific groups of users with the hope of generating higher returns. Name-brand pharmaceuticals, luxury watch brands, and events such as tax season top the list of things that spammers promote most in their campaigns. Over time, spammers have learned that the quickest way to attract clicks and purchases—and to generate a profit—is to leverage spoofed brands and take advantage of current events that have the attention of large groups of users.

Global Spam Trends

Since the large-scale botnet takedowns of 2010, high-volume spam isn't as effective as it once was, and spammers have learned and changed their tactics. There is a clear evolution toward smaller, more targeted campaigns based on world events and particular subsets of users. High-volume spam is also more likely to be noticed by mail providers and shut down before its purpose can be fulfilled.

Figure 12: Global Spam Trends

Global spam volumes down 18 percent, with most spammers keeping bankers' hours on weekends.



High-volume spam is more likely to be noticed by mail providers and shut down before its purpose can be fulfilled.

In 2012, there were several examples of spammers using news about world events—and even human tragedy—to take advantage of users.

In 2011, overall global spam volumes were down 18 percent. This is far from the dramatic drop in volume seen in 2010 following the botnet takedowns, but the continued downward trend is a positive development nonetheless.

Spammers continue their focus on minimizing effort while maximizing impact. According to Cisco's research, spam volumes fall by 25 percent on weekends, when users are often away from their email. Spam volumes rise to the highest levels on Tuesday and Wednesday—an average of 10 percent higher than on other weekdays. This heightened activity in the middle of the week and lower volumes on the weekend allow spammers to live "normal lives."

It also gives them time to spend crafting tailored campaigns based on world events early in the week that will help them to generate a higher response rate to their campaigns.

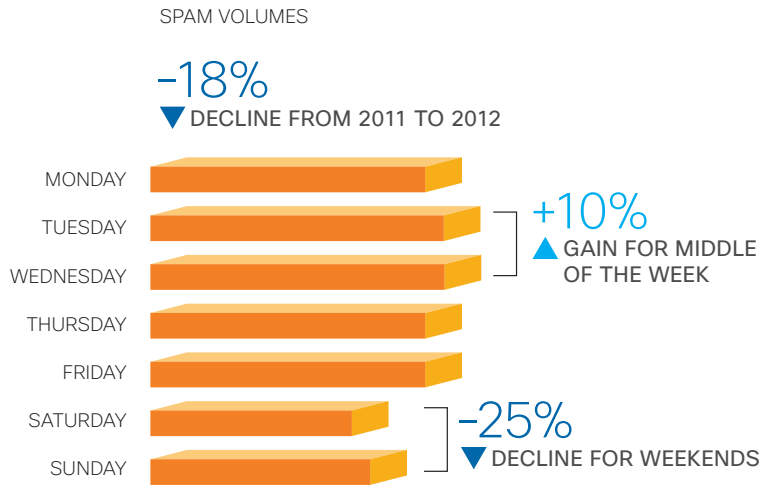
In 2012, there were several examples of spammers using news about world events—and even human tragedy—to take advantage of users. During Superstorm Sandy, for example, Cisco researchers identified a massive "pump and dump" stock scam based around a spam campaign. Using a pre-existing email message that urged people to invest in a penny stock focused on natural resource exploration, the spammers began attaching sensational headlines about Superstorm Sandy. An unusual aspect of this campaign is that the spammers utilized unique IP addresses to send a batch of spam—and have not activated those addresses since.

Spam Origination

In the world of spam, some countries remain the same while others dramatically change their rankings. In 2012, India retains the top spot as a source of spam worldwide, with the United States moving up from sixth in 2011 to second in 2012. Rounding out the top five spam-originating countries are Korea (third), China (fourth) and Vietnam (fifth).

Overall, the majority of spammers focus their efforts on creating spam messages that feature the languages

Figure 13: Spam Origination
India retains spam crown, and United States skyrockets into second position.



spoken by the largest audiences who use email on a regular basis. According to Cisco's research, the top language for spam messages in 2012 was English, followed by Russian, Catalan, Japanese, and Danish. Of note, there are gaps between where spam is being sent from and the languages that are being used in the spam message; for example, while India was the number one spam-originating country in 2012, local dialects did not break the top 10 in terms of languages used in spam sent from India. The same was true for Korea, Vietnam, and China.

Figure 14: Email Attachments
Only 3 percent of spam has an attachment versus 25 percent of valid email, but spam attachments are 18 percent larger.

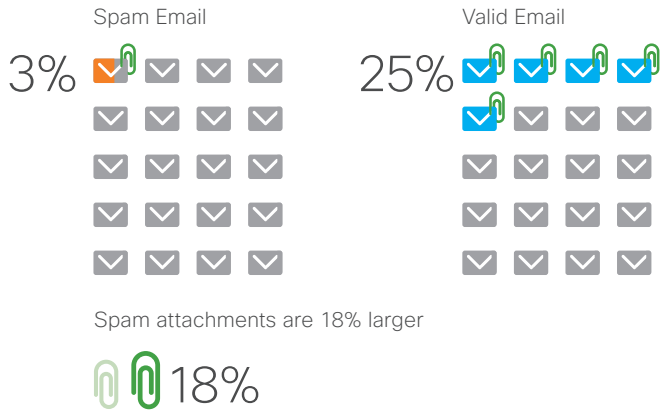
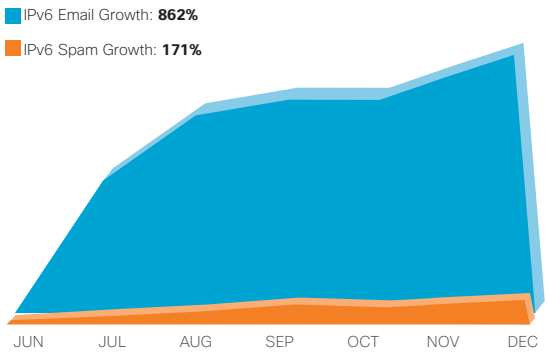


Figure 15: IPv6 Spam
While IPv6-based email remains a very small percentage of overall traffic, it is growing as more email users move to IPv6-enabled infrastructure.



Email Attachments

Spam has long been thought of as a delivery mechanism for malware, especially when an attachment is involved. But Cisco's recent research on the use of email attachments in spam campaigns shows that this perception may be a myth.

Only 3 percent of total spam has an attachment, versus 25 percent of valid email. And in the rare cases when a spam message does include an attachment, it is an average of 18 percent larger than a typical attachment that would be included in valid email. As a result, these attachments tend to stand out.

In modern email, links are king. Spammers design their campaigns to convince users to visit websites where they can purchase products or services (often dubious). Once there, users' personal information is collected, often without their knowledge, or they are compromised in some other way.

As the "Spoofed Brands" analysis that appears later in this section reveals, a majority of spam comes from groups who seek to sell a very specific group of name-brand goods—from luxury watches to pharmaceuticals—that are, in most cases, fake.

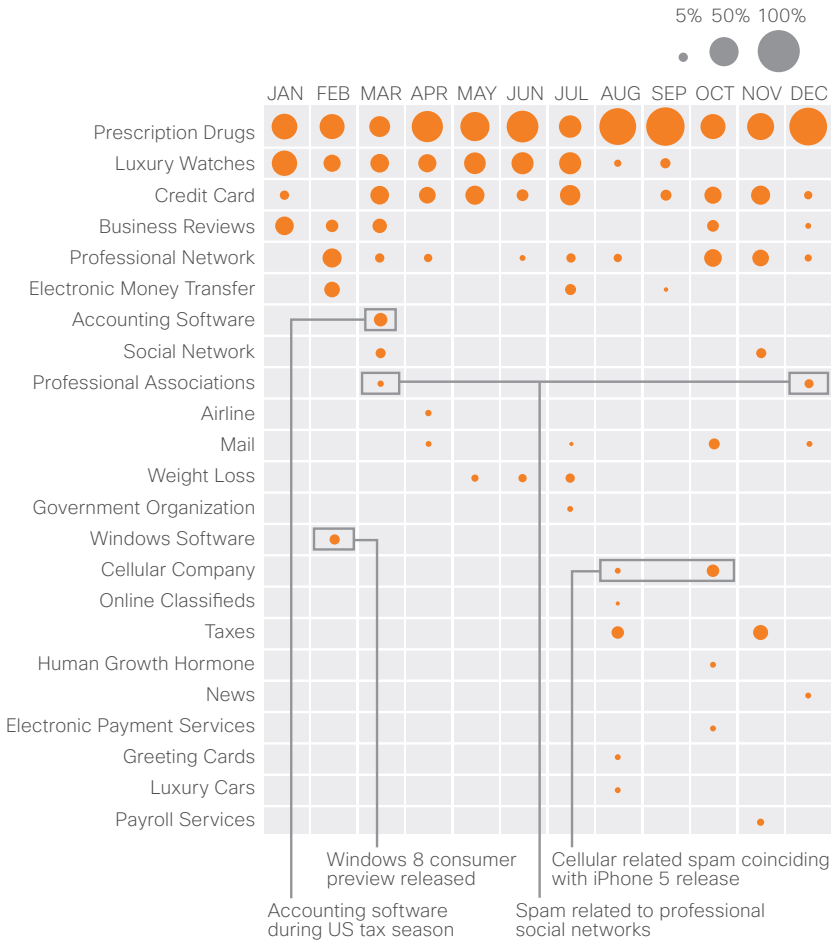
IPv6 Spam

While IPv6-based email remains a very small percentage of overall traffic, it is growing as more email users move to IPv6-enabled infrastructure.

However, while overall email volumes are growing at a rapid clip, this is not the case with IPv6 spam. This suggests that spammers are hedging against the time and expense to migrate to the new Internet standard. There is no driving need for spammers—and little to no material benefit—to cause such a shift at present. As IPv4 addresses are exhausted and mobile devices and M2M communication drive explosive growth in IPv6, expect spammers to upgrade their infrastructure and accelerate their efforts.

In modern email, links are king. Spammers design their campaigns to convince users to visit websites where they can purchase products or services. Once there, users' personal information is collected, often without their knowledge, or they are compromised in some other way.

Figure 16: Spoofed Brands
Spammers target pharmaceuticals, luxury watches, and tax season.



Spoofed Brands

With spoofed-brands spam email, spammers use organizations and products to send their messages in hopes that online users click on a link or make a purchase. The majority of spoofed brands are prescription drugs, such as anti-anxiety medication and painkillers. In addition, luxury watch brands form a constant layer of "noise" that retains consistency across the entire year.

Cisco's analysis shows that spammers are also skilled at tying their campaigns to news events. From January to March 2012, Cisco data shows a spike in spam relating to Windows software, which coincided with the release of the Windows 8 operating system. From February to April 2012, during the U.S. tax season, analysis shows a precipitous increase in tax software spam.

From January to March 2012, and then again from September to December 2012—the beginning and the end of the year—spam relating to professional networks made grand entrances, perhaps because spammers know that people often begin job searches during these times of the year.

The bottom line is spammers are in it for the money, and over the years, they have learned that the quickest way to attract clicks and purchases is by offering pharmaceuticals and luxury goods and by tailoring their attacks toward events to which much of the world is paying attention.

From September to November 2012, spammers ran a series of campaigns posing as cellular companies, coinciding with the release of the iPhone 5.

The bottom line: Spammers are in it for the money, and over the years, they have learned that the quickest way to attract clicks and purchases is by offering pharmaceuticals and luxury goods and by tailoring their attacks toward events to which much of the world is paying attention.

Vulnerability Management: A Vendor Has to Do More Than Enumerate Ambivalently[35]

How a vendor discloses its product security issues is the most visible aspect of their vulnerability management practices. At Cisco, Security Advisories[36] are researched and published by the Product Security Incident Response Team (PSIRT), a group of senior security experts who understand that protection of Cisco customers and of the corporation must go hand in hand.

"Security Advisories announce our most severe product security issues and are generally the first public evidence of a Cisco product vulnerability," says Russell Smoak, Senior Director of Cisco Security Research and Operations, "As such, it's critical that they be an effective communications vehicle that helps customers make informed decisions and manage their risk. Combined with the advanced mitigation techniques[37] we provide for our customers to leverage the capabilities in their existing Cisco gear, we are able to provide as many details as possible to respond quickly and confidently."

Vulnerability management, however, starts much earlier in the lifecycle of a vulnerability and can extend beyond initial disclosure. "Continuous improvement in vulnerability management practices is imperative to keeping pace with the changing security environment as a result of evolving threats as well as new products and technologies," says Smoak.

In other words, a vendor that fails to evolve with threat technologies—and that does not disclose threats—risks falling behind. For example, innovation of internal vulnerabilities management tools at Cisco has taken place in the area of bundled third-party software. Third-party software is any code included in a vendor's product that was not written by the vendor itself; this typically includes commercial third-party or open-source software.

Cisco takes advantage of custom-built tooling that uses vulnerability data from Cisco IntelliShield[38] to notify the product development teams when a security issue that originates in third-party software may impact a Cisco product. This tool, called the Cisco Internal Alert Manager, has greatly increased the ability to manage security issues that originate in non-Cisco code.

A vendor that fails to evolve with threat technologies—and that does not disclose threats—risks falling behind.

Improvement of security disclosure practices should be ongoing as well. In early 2013, Cisco will begin using a new document type—the Cisco Security Notices—to disclose low-to-medium-severity product security issues. Cisco Security Notice will improve the efficacy of communication around security issues not deemed severe enough to warrant a Cisco Security Advisory. These documents will be available publicly and indexed by a Common Vulnerability and Exposure (CVE) identifier to improve visibility.

To further enhance how to best digest the ongoing reporting of security issues, vendors (including Cisco) have begun to include the Common Vulnerability Reporting Framework (CVRF)[39] and Open Vulnerability Assessment Language (OVAL)[40] formats in their disclosures. These emerging standards help end users evaluate vulnerabilities across multiple platforms and technologies with confidence—and the standards are able to scale due to the benefits of machine-readable format. Smoak says, "Ensuring that our customers have the tools that they need to properly evaluate threats to their networks helps reduce risk and allows them to prioritize tasks required to secure their infrastructures."

In the year ahead, for additional updates and in-depth analysis on security trends, and for information about the latest enterprise security-related publications from Cisco, visit the Cisco Security Reports website.
http://www.cisco.com/go/securityreport

For ongoing insight from Cisco's experts on a wide range of security topics, visit the Cisco Security Blog.
blogs.cisco.com/security

Security Outlook 2013

The threat landscape of today is not a problem caused by uneducated users visiting malicious sites or is it solved by blocking known “bad” locations on the web.

This report has demonstrated how attackers have become increasingly more sophisticated, going after the sites, tools, and applications that are least likely to be suspected, and users visit most frequently. Modern threats are capable of infecting mass audiences silently and effectively, not discriminating by industry, business, size or country. Cybercriminals are taking advantage of the rapidly expanding attack surface found in today’s “any-to-any” world, where individuals are using any device to access their business network.

As critical national infrastructure, businesses, and global financial markets continue their move to cloud-based services and mobile connectivity, an integrated, layered approach to security is needed to protect the burgeoning Internet of Everything. “Hackers and cybercriminals take advantage of the fact that every private or public sector enterprise has its own IT security program,” says John Stewart. “Yes, we go to conferences and stay in touch with each other, but we really need to move from individualized IT security to one based on real-time intelligence sharing and collective response.”

Building a better security infrastructure doesn’t mean creating a more complex architecture—in fact, quite the opposite. It’s about making the infrastructure and the elements within

Modern threats are capable of infecting mass audiences silently and effectively, not discriminating by industry, business size, or country.

it work together, with more intelligence to detect and mitigate threats. With the rapid adoption of BYOD, the reality of multiple devices per user, and growth of cloud-based services, the era of managing security capabilities on each endpoint is over. “We must take a holistic approach to security that ensures we are monitoring threats across all vectors, from email to Web to users themselves,” says Michael Covington, Product Manager for Cisco SIO. “Threat intelligence needs to be elevated above individual platforms in order to gain a network perspective.”

As threats increasingly target users and organizations across multiple vectors, businesses need to collect, store, and process all security-relevant network activity to better understand the scope and extent of attacks. This level of analysis can then be augmented with the context of network activity to make accurate and timely security decisions. As attackers become more sophisticated, enterprises must design security capabilities into the network from the beginning, with solutions that bring together threat intelligence, security policy and enforceable controls across all touch points on the network.

As the attackers become more sophisticated so, too, must the tools used to thwart their efforts. With the network providing a common fabric for communication across platforms, it will also serve as a means to protect the devices, services, and users that routinely use it to exchange sensitive content. The network of tomorrow is an intelligent one that must provide better security through a collaborative framework than previously possible through the sum of its individual components.

The network of tomorrow is an intelligent one that must provide better security through a collaborative framework than previously possible through the sum of its individual components.

About Cisco Security Intelligence Operations

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

Online criminals continue 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 using real-time threat intelligence from Cisco Security Intelligence Operations (SIO). Cisco SIO is the world's largest cloud-based security ecosystem, in which more than 75 terabits of live data feeds from deployed Cisco email, web, firewall, and IPS solutions are analyzed each day.

Cisco SIO aggregates data from across threat vectors and analyzes it using both automated algorithms and manual processing in an effort to understand how the threats propagate. SIO then categorizes threats and creates rules using more than 200 parameters. Security researchers also analyze 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.

Cisco SIO is the world's largest cloud-based security ecosystem, in which more than 75 terabits of live data feeds from deployed Cisco email, web, firewall, and IPS solutions are analyzed each day.

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: **http://www.cisco.com/security**.

Methodology

The analysis presented in this report is based on data that was gathered from a variety of anonymized global sources, including Cisco email, web, firewall, and intrusion prevention system (IPS) security solutions; these platforms sit on the front lines protecting customer networks from malicious content and intruders. In addition to these on-premise customer protection mechanisms, Cisco also collects data from a worldwide deployment of sensors that perform functions such as trapping spam and crawling the web to actively seek out new instances of malware.

Using these tools and the data they collect, Cisco's massive network footprint gives SIO systems and researchers insight into a tremendous sampling of both legitimate and malicious activities on the Internet. No security vendor has total visibility into all malicious encounters. The data presented in this report is Cisco's perspective on the current state of the threat landscape and represents our best attempt to normalize data and reflect global trends and patterns based on the data available at the time.

Cisco collects data from a worldwide deployment of sensors that perform functions such as trapping spam and crawling the web to actively seek out new instances of malware.

Cisco Security IntelliShield Alert Manager Service

Cisco Security IntelliShield Alert Manager Service provides a comprehensive, cost-effective solution for delivering the vendor-neutral security intelligence organizations need to identify, prevent, and mitigate IT attacks. This customizable, web-based threat and vulnerability alert service allows security staff to access timely, accurate, and credible information about threats and vulnerabilities that may affect their environments. IntelliShield Alert Manager allows organizations to spend less effort researching threats and vulnerabilities, and focus more on a proactive approach to security.

Cisco offers a free 90-day trial of the Cisco Security IntelliShield Alert Manager Service. By registering for this trial, you will have full access to the service, including tools and threat and vulnerability alerts.

To learn more about Cisco Security IntelliShield Alert Manager Services, visit: https://intellishield.cisco.com/security/alertmanager/trialdo?dispatch=4.

For More Information

Cisco Security Intelligence Operations
www.cisco.com/security

Cisco Security Blog
blogs.cisco.com/security

Cisco Remote Management Services
www.cisco.com/en/US/products/ps6192/serv_category_home

Cisco Security Products
www.cisco.com/go/security

Cisco Corporate Security Programs Organization
www.cisco.com/go/cspo

[1] "The Internet of Things," by Michael Chui, Markus Löffler, and Roger Roberts, *McKinsey Quarterly*, March 2010: http://www.mckinseyquarterly.com/The_Internet_of_Things_2538.

[2] "Cisco Event Response: Distributed Denial of Service Attacks on Financial Institutions," October 1, 2012: http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[3] Ibid.

[4] "The World Market for Internet Connected Devices–2012 Edition," media release, IMS Research, October 4, 2012: http://imsresearch.com/press-release/Internet_Connected_Devices_Approaching_10_Billion_to_exceed_28_Billion_by_2020&cat_id=210&type=LatestResearch.

[5] Cisco Internet Business Solutions Group.

[6] Evans.

[7] Cisco Internet Business Solutions Group.

[8] http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

[9] "Remote Access and BYOD: Enterprises Working to Find Common Ground with Employees," *2011 Cisco Annual Security Report*, December 2011, p. 10: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

[10] "Cisco Global Cloud Index: Forecast and Methodology, 2011–2016": http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html.

[11] "Cisco Global Cloud Index: Forecast and Methodology, 2011–2016": http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html.

[12] "A Deep Dive Into Hyperjacking," by Dimitri McKay, SecurityWeek, February 3, 2011: http://www.securityweek.com/deep-dive-hyperjacking.

[13] India's government blocked hundreds of web sites and curbed texts: http://www.nytimes.com/2012/08/20/world/asia/india-asks-pakistan-to-help-investigate-root-of-panic.htmlIndia's government blocked hundreds of web sites and curbed texts: http://www.nytimes.com/2012/08/20/world/asia/india-asks-pakistan-to-help-investigate-root-of-panic.html.

[14] "Twitter Rumor Sparked Oil-Price Spike," by Nicole Friedman, WSJ.com, August 6, 2012: http://online.wsj.com/article/SB10000872396390444246904577573661207457898.html.

[15] This originally appeared on the Cisco Security blog: http://blogs.cisco.com/security/sniffing-out-social-media-disinformation/

[16] http://www.java.com/en/about/.

[17] Vishwath Mohan and Kevin W. Hamlen. *Frankenstein: Stitching Malware from Benign Binaries*. In Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), pp. 77-84, August 2012.

[18] Mohammad M. Masud, Tahseen M. Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han, and Bhavani Thuraisingham. Cloud-based Malware Detection for Evolving Data Streams. ACM Transactions on Management Information Systems (TMIS), 2(3), October 2011.

[19] "DDoS Attacks: 2013 Forecast, Experts Say Recent Hits Only the Beginning," by Tracy Kitten, BankInfoSecurity.com, December 30, 2012: http://ffiec.bankinfosecurity.com/ddos-attacks-2013-forecast-a-5396.

[20] IPS Testing, Cisco.com: http://www.cisco.com/web/about/security/intelligence/cwilliams-ips.html.

[21] "Maliciously Abusing Implementation Flaws in DNS," *DNS Best Practices, Network Protections, and Attack Identification*, Cisco.com: http://www.cisco.com/web/about/security/intelligence/dns-bcp.html#3.

[22] "IP Spoofing," by Farha Ali, Lander University, available at Cisco.com: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html.

[23] "Distributed Denial of Service Attacks," Cisco.com: http://www.nytimes.com/2012/08/20/world/asia/india-asks-pakistan-to-help-investigate-root-of-panic.html?_r=1&.

[24] "DNS Tools," The Measurement Factory: http://www.nytimes.com/2012/08/20/world/asia/india-asks-pakistan-to-help-investigate-root-of-panic.html?_r=1&.

[25] "Cisco IOS NetFlow," Cisco.com: http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html.

[26] "Secure BIND Template Version 7.3 07 Aug 2012," by TEAM CYMRU, cymru.com: http://www.cymru.com/Documents/secure-bind-template.html.

[27] "Response Rate Limiting in the Domain Name System (DNS RRL)," RedBarn.org: http://www.redbarn.org/dns/ratelimits.

[28] Arbor Networks' ATLAS data is derived from "honey pots" deployed within service provider networks around the world; ASERT malware research; and, an hourly feed of anonymized data based on NetFlow, BGP, and SNMP correlation. The anonymized data provided by Arbor Peakflow SP customers is collated and trended within ATLAS to provide a detailed view of the threats and traffic patterns on the Internet.

[29] "Bank of America and New York Stock Exchange Under attack unt [sic]," Pastebin.com, September 18, 2012: http://pastebin.com/mCHia4W5.

[30] "Phase 2 Operation Ababil," Pastebin.com, September 18, 2012: http://pastebin.com/E4f7fmB5.

[31] "Cisco Event Response: Distributed Denial of Service Attacks on Financial Institutions": http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[32] "Identifying and Mitigating the Distributed Denial of Service Attacks Targeting Financial Institutions Applied Mitigation Bulletin": http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=27115.

[33] "Security Intelligence Operations Tactical Resources," Cisco.com: http://tools.cisco.com/security/center/intelliPapers.x?i=55.

[34] "Service Provider Security Best Practices," Cisco.com: http://tools.cisco.com/security/center/serviceProviders.x?i=76.

[35] Anagram courtesy of anagramgenius.com.

[36] Cisco Security Advisories: http://cisco.com/go/psirt.

[37] Cisco Applied Mitigation Bullets, Cisco.com: http://tools.cisco.com/security/center/searchAIR.x.

[38] Cisco Intellishield Alert Manager Service: http://www.cisco.com/web/services/portfolio/product-technical-support/intellishield/index.html.

[39] CVRF, ICASI.com: http://www.icasi.org/cvrf.

[40] OVAL, Oval International: http://oval.mitre.org/.

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**.