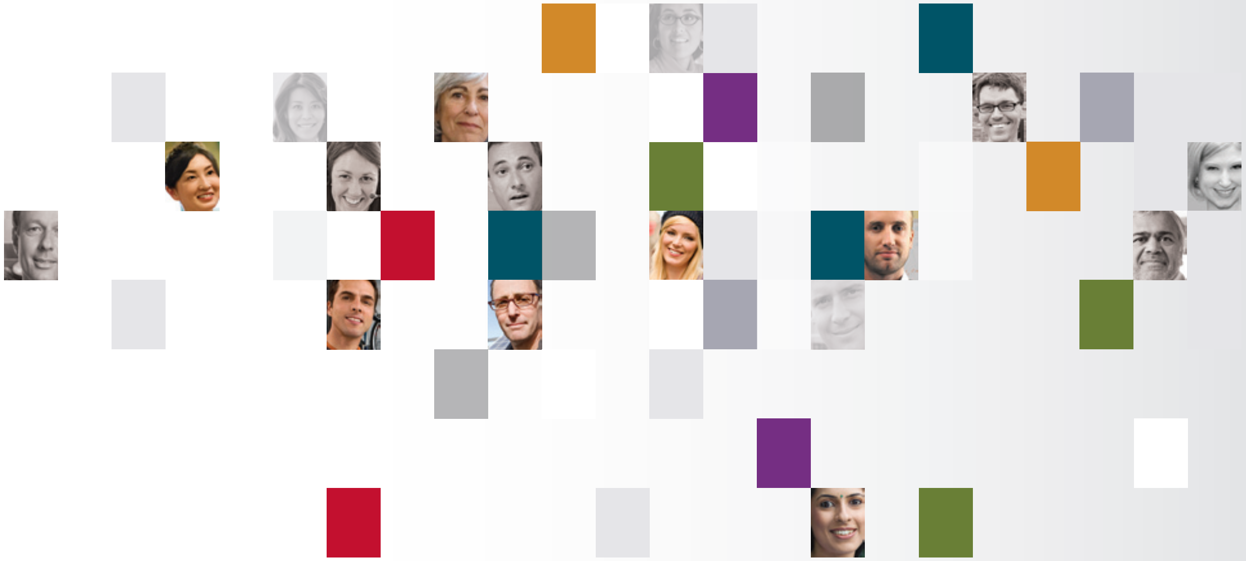
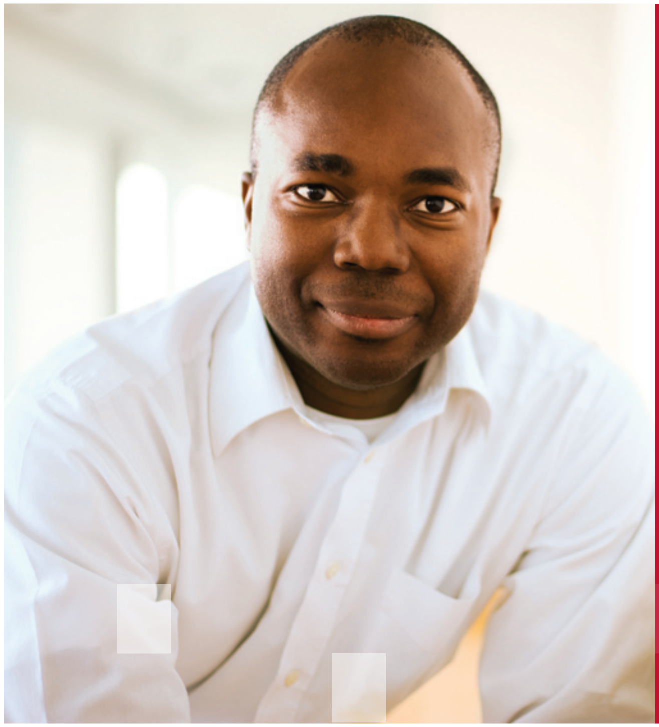
Cisco 2009 Annual Security Report

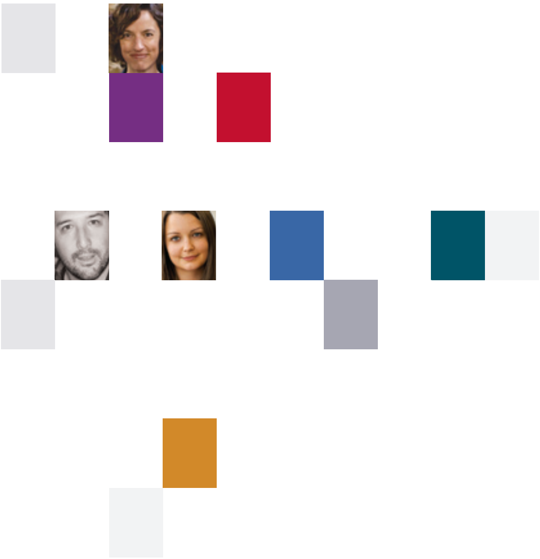
Highlighting global security threats and trends

Contents

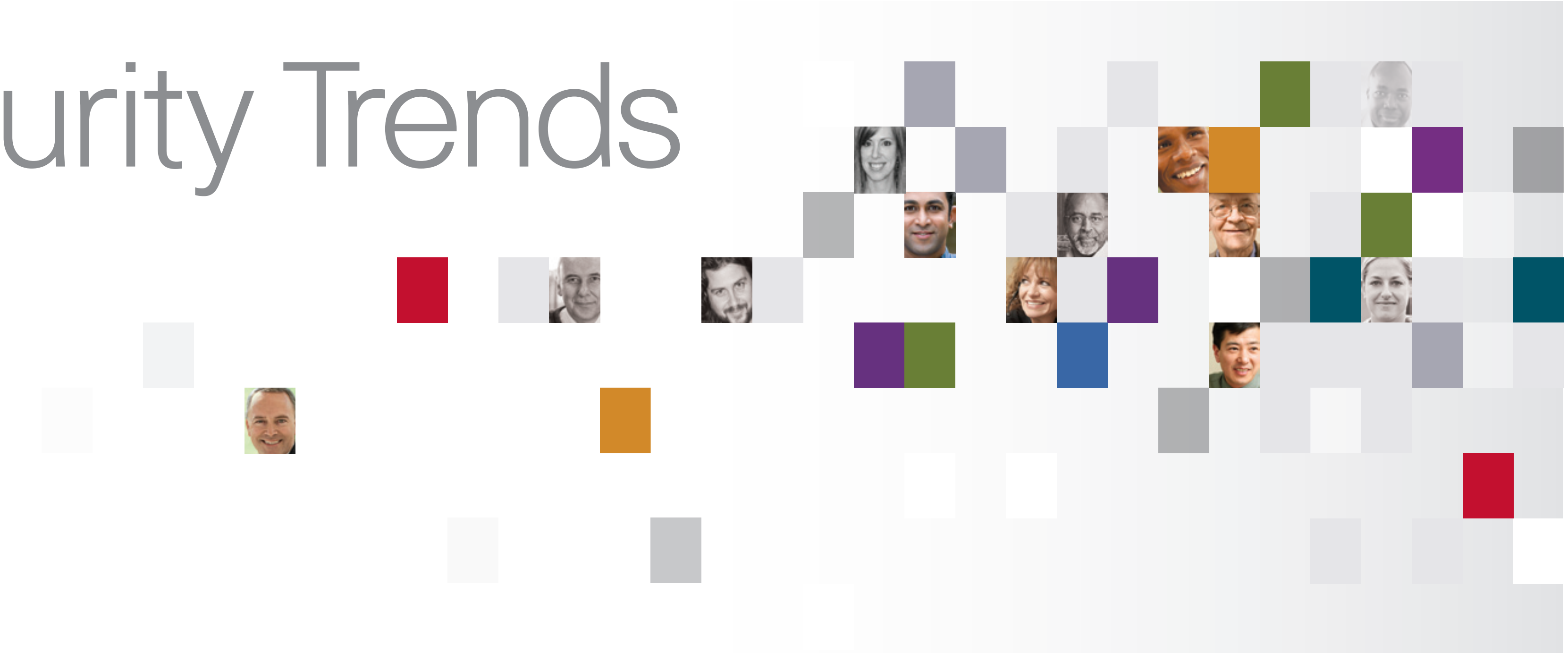




The Cisco® Annual Security Report provides an overview of the combined security intelligence of the entire Cisco organization. The report encompasses threat information and trends collected between January and December 2009. It also provides a snapshot of the state of security for that period, with special attention paid to key security trends expected for 2010.



Security Trends



Where does work happen? No longer does business take place solely behind network walls. The critical work of an organization is happening increasingly on social networks, on handheld devices, on Internet kiosks at airports, and at local cafes.

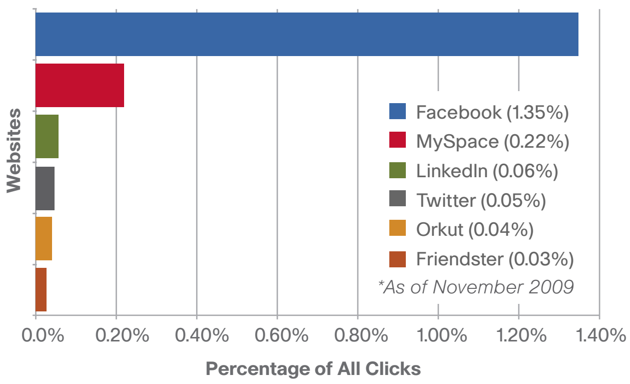
Where and how will work get done in 2010? On social networks, such as Facebook, Twitter, and LinkedIn; over handheld wireless devices like BlackBerries and iPhones; via webmail and instant messaging; and on airplanes, in cafes, and anywhere else there's an Internet connection.

And with each advance in technology that enhances connectivity and communication, the migration from the "traditional" office environment, where work happens behind fortified network walls, will intensify. The traditional corporate perimeter, with clearly identifiable boundaries, has diminished. In its place, a network with limitless potential is rising—one where companies, their customers, and their partners demand access to information whenever and wherever they need it.

These are exciting times, but the dramatic changes in how and where business is conducted demand a new way of thinking about how to secure an enterprise and what it cares most about—its people, operations, and assets. The mobility of information inside and outside of corporate networks, the emergence of personal devices and new applications being used on the corporate network, and the persistence and sophistication of the criminal community are transforming how the security industry approaches protecting businesses and averting threats.

It is information technology's role to ensure that the appropriate people, using the correct devices, are accessing the proper resources while having a highly secure yet positive user experience. Business operations, behaviors, and ideas are transcending the artificial boundary outside of the network perimeter—the firewall—and, in turn, are being shared in ways that current security models may not have considered.

Social Media Usage in the Enterprise*



*As of November 2009

In an examination of weblog data from more than 4000 Cisco web security customers, the impact of social media usage on the enterprise is clear. As much as 2 percent of all web traffic in these businesses comes from accessing social media sites, such as Facebook, MySpace, and LinkedIn. "While 2 percent may seem like a small number in terms of an employee's total daily web browsing, it indicates an increase in an organization's need to educate employees on potential losses which could occur via social media," said Christopher Burgess, a senior security advisor to the Chief Security Officer at Cisco.

Consider social media. Its impact on computer security cannot be overstated. It is now routine for workers of all generations to interact with colleagues, customers, or partners using social networks that, a few years ago, would have been populated mostly by computer users in their teens and twenties. In addition, it is common for workers to blend business and personal communications on these social networks, further blurring the network perimeter.

The high levels of trust that users place in social networks—that is, users' willingness to respond to information appearing within these networks—has provided ample opportunity for new and more effective scams. Instead of searching out vulnerabilities to exploit, criminals merely need a good lure to hook new victims. For example, an individual who is masquerading as a trusted social networking colleague could convince a user to visit a malware-laden website or pay for fake anti-virus software or spurious weight-loss remedies. Simply put, social media has been a tremendous benefit for the creators of online scams.

Vendors Increase Focus on Software Vulnerabilities

There is some positive news to report from 2009 that will likely carry into 2010: Software vendors appear to be working hard to patch vulnerabilities. In the months of September and October 2009 alone, Cisco, Microsoft, Oracle, and Adobe—whose products have been the targets of exploit attempts—released updates to patch more than 100 vulnerabilities in their respective software products. In addition, the vulnerability that allowed the Conficker botnet to gain strength was patched. And the newest releases of the Microsoft Internet Explorer and Mozilla Firefox web browsers offer significant security upgrades.

And the bad news? According to Cisco research, the number of vulnerabilities and threats remained relatively consistent in 2009 compared to previous years, but the exploit and attack threat levels increased by 57 percent. New attacks rely on social media users' willingness to respond to messages that supposedly originate from people they know and trust. It is easier—and often, more lucrative—to fool a social media user in order to launch an attack or exploit or steal personal information. (Learn more about specific vulnerabilities on pages 15 and 17.)

Although cybercriminals can profit from their exploits quickly and with little effort, money is not always the motive.

Political Attacks: Controlling the Conversation

Although cybercriminals can profit from their exploits quickly and with little effort, money is not always the motive. Some attackers are on a mission to cripple servers and other critical infrastructure to create communications nightmares and disrupt the operations of specific entities, such as governments, the offices of spiritual leaders, and media outlets. Others are interested simply in controlling the conversation on the Internet, especially when they disagree with what they read.

Since 2007, politically motivated online attacks—big and small—have increased worldwide, and they can be expected to increase. Distributed denial of service (DDoS) attacks appear to be the weapon of choice. The growing numbers of botnets, another big story from 2009, are partly to blame for this trend. So, too, are the increasingly abundant, cheap, and easy-to-use toolkits that hackers can purchase to control a botnet and launch an effective and well-coordinated Internet attack.

For example, in August 2009, hackers sent a clear message to blogger Georgy Jakhaia—known online as Cyxymu—that someone, somewhere, did not care for his open criticism of the Russian government. Jakhaia lives in the former Soviet republic of Georgia and has written about tensions between his country and Russia on sites such as Twitter, Facebook, YouTube, and the blogging site LiveJournal.

Hackers intent on silencing Jakhaia launched a DDoS attack that not only overwhelmed Twitter but also took it down for hours. It also affected Facebook, YouTube, and LiveJournal. The attackers called a botnet into action, and thousands of "zombie" computers deluged the web with spam, which included links to various webpages associated with the blogger. In an interview with *BusinessWeek*, security researcher and Cisco Fellow Patrick Peterson said the hackers essentially used "a hand grenade to silence a fly."[1]

Even so, mischief-makers clearly like to use this swift and high-impact method when they want to make a point. In September, a company managing online donations for United States (U.S.) Representative Joe Wilson of South Carolina—who made headlines earlier that month for shouting "You lie!" during President Obama's address to the U.S. Congress on the topic of healthcare reform—experienced a DDoS attack that knocked its servers offline for hours. At its peak, the DDoS flood generated about 1 gigabit of traffic per second, or nearly 1000 times the website's normal amount of traffic.

[1] "Computer Hacking Made Easy," by Joel Schectman, *BusinessWeek*. August 13, 2009.

Announcing the 2009 “Winners” of the Cisco Cybercrime Showcase

There are four “winners” named in the first-ever Cisco Cybercrime Showcase, but only two deserve applause. Two categories—Cybercrime Hero and Cybercrime Sign of Hope—shine a spotlight on individuals and entities who have made significant, positive contributions during the past year toward making the Internet a safer place for all users. Meanwhile, the other two categories, Most Audacious Criminal Operation and Most Notable Criminal Innovation, are reserved for the “worst of the worst” from 2009: cybercrime events that truly belong in a “Hall of Shame.”

Category: Cybercrime Hero

Winner: Brian Krebs, journalist, *The Washington Post*

Kudos to Brian Krebs, who reports on computer security issues in his *Security Fix* blog on the website of *The Washington Post*. Krebs has spent a significant amount of time researching and reporting on banking Trojans like Zeus and Clampi and exposing how they operate.

In the fall of 2009, Krebs published a series of articles about the online “bank jobs” conducted by the sophisticated malware that Zeus and Clampi distribute. Through his extensive research and reporting, Krebs managed to discover a great deal about these Trojans. The tactics and routines associated with the malware—and the significant number of businesses and individual users who have been affected by it—would likely impress even some of the most successful bank thieves in history.

Krebs has taken time not only to report on these dangerous threats, but also to provide readers with practical and easy-to-understand advice about how not to fall victim to such scams.

See “The Rise of the Banking Trojans,” page 11, to read about Zeus and Clampi.

Category: Most Audacious Criminal Operation

Winner: Zeus

Zeus is a Trojan that delivers malware to unsuspecting users via phishing emails and drive-by downloads. The malware can “listen” to computer activity and, through this intelligence gathering, can steal login names and passwords for banking and email accounts. It can even defeat hardware tokens and onetime passwords that people assume provide protection from this type of attack.

Cybercriminals can use a convenient and affordably priced toolkit to create new variants on the Zeus Trojan, making it undetectable to anti-virus programs. Enormous and powerful, the botnet created by the Zeus Trojan certainly lived up to its mythological name during 2009 by infecting nearly 4 million computers worldwide.

To read about Zeus, see “The Rise of the Banking Trojans” on page 11.

Category: Cybercrime Sign of Hope

Winner: The Conficker Working Group

Experts agree that the impact of network worm Conficker —which was expected to set some type of “evil plan” into motion on April 1, 2009—was significantly muted by the impressive fight-back effort of the security community and industry. Multiple entities strategically and proactively combined their knowledge, best practices, and technology to prevent the Conficker worm from spreading.

The collaboration and cooperation among these “forces for good” proved that swift and effective action against a major threat to Internet security is possible. An important lesson learned from this experience: Although not every infected computer in the world can be cleaned up, future infections can be prevented.

To learn more about the Conficker Working Group and the Conficker threat in 2009, download the *Cisco 2009 Midyear Security Report* at http://cisco.com/web/about security/intelligence/midyear_security_review09.pdf.

Category: Most Notable Criminal Innovation

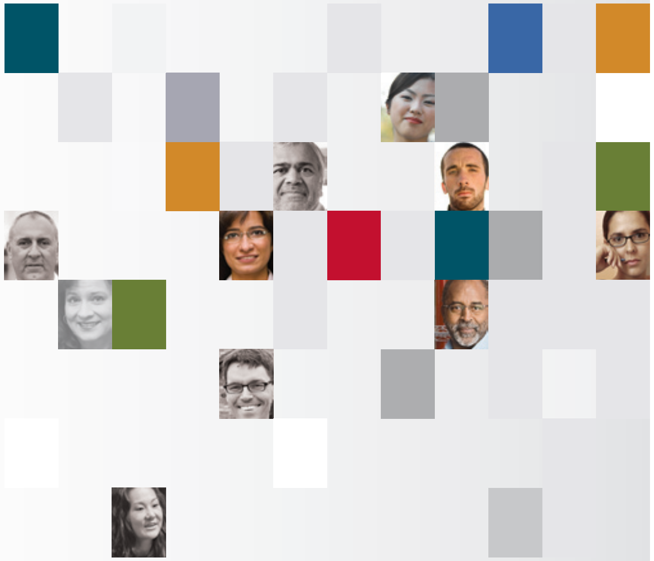
Winner: Koobface

Many worms have the power to regenerate—even in the cyber world—as the Koobface worm proved in 2009. It first appeared on social networking websites such as Facebook in 2008. Later, it was “reborn” on Twitter, the microblogging service that has become a social media sensation, attracting millions of followers worldwide.

Koobface sends “tweets” that lure Twitter users into clicking a link for a YouTube video that instructs them to update their Flash player. That’s when the “fun” begins: Users download a file and launch the worm, and Koobface is off to “wriggle” its way toward even more potential victims. Thanks to variants of this malicious software, it is estimated that nearly 3 million computers have been infected.

See “Social Media: We’re the Problem,” page 6.

Social Media: We're the Problem

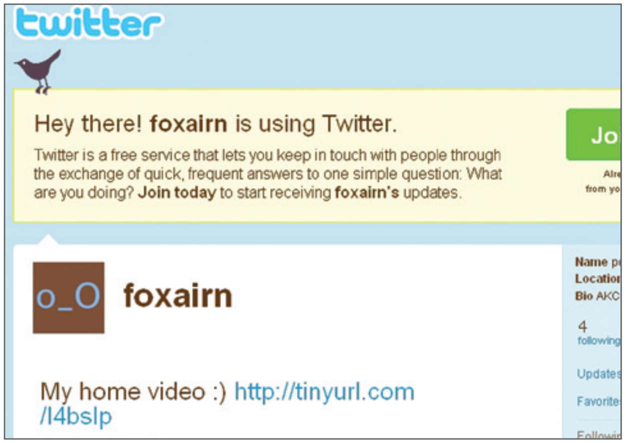


Social media users believe there is protection in being part of a community of people they know. Criminals are happy to prove this notion wrong.

The threats and security issues that come with social media aren't usually caused by vulnerabilities in software. More commonly, these threats originate from individuals who place an unwarranted amount of "transitive trust" in the safety of these communities. Users will trust something or someone because a user they know has also expressed trust in that person or subject.

Throughout 2009, the explosive growth of social media has been fueled by business' embrace of these tools—in other words, social networking's popularity has extended far beyond young people, who were the early adopters. This exponential growth is expected to continue into 2010, as more organizations realize that having a presence on social networks is a need-to-have, not a nice-to-have. A few years ago, businesses enthusiastically adopted Second Life and other virtual communities for social networking, but this trend fizzled out. The new generation of social media offerings promises much more staying power in the business community.

Social networking site Facebook reports that from August 2008 to December 2009, its active user base more than tripled, from 100 million to 350 million. As Cisco has continued to report, criminals migrate attacks to where their victims are. They have wasted no time targeting this huge audience, and they are creating more sophisticated ways to take advantage of the trust users place in social media. The Koobface worm, first detected on social networking websites such as Facebook in 2008, appeared again in 2009, when yet more variants of the malicious software popped up on Twitter, the microblogging service. Estimates indicate that almost 3 million computers have been infected with Koobface.



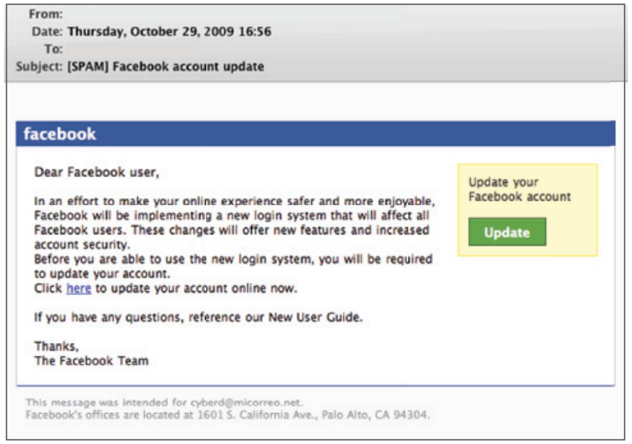
Hey there! **foxairn** is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? **Join today** to start receiving **foxairn's** updates.

o_O **foxairn**

My home video :) http://tinyurl.com/l4bslp

Twitter Spam
"Twitter spam" delivers tweets that suggest users click on a video link, which then downloads the Koobface worm onto their computers.



From:
Date: Thursday, October 29, 2009 16:56
To:
Subject: [SPAM] Facebook account update

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.
Before you are able to use the new login system, you will be required to update your account.
Click here to update your account online now.

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

Update your Facebook account

This message was intended for cyberd@micorreo.net.
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

Social Media Scams
"Facebook spam" lures recipients into submitting login information for the social networking site and then redirects victims to websites that sell products such as weight-loss remedies.

In the Twitter attack, Koobface hooks its victims by delivering tweets (likely from previously infected users) that instruct users to click on a link that appears to be a YouTube video. The user is then directed to download an update to their Flash player, but the downloaded file actually launches the worm. In an effort to snare more victims, the next time the user logs on to Twitter, the worm will add new tweets about the supposed video.

Facebook's massive worldwide audience has also spurred the use of Facebook as a hook for malicious messages, the vast majority of which originate outside of the social networking site. An increasingly common spam tactic involves sending emails, supposedly from a Facebook friend, suggesting the recipient click through to view the message on the Facebook site. The emails mimic real messages sent out by Facebook to alert users that one of their Facebook friends is interacting with them.

Although there are links to Facebook.com within the messages, the real calls to action are links to websites selling weight-loss remedies, among other items. One example in 2009 was the acai berry weight-loss remedy craze, which proved to be very popular with scammers. Through these scams, users are urged to buy overpriced products, or those that require a subscription that proves remarkably difficult to cancel. Victims discover too late that there is no "customer service department" to contact.

Facebook has also been used to launch "419" scams. The scam normally starts when a Facebook user is fooled into handing over Facebook login credentials, or has their login credentials stolen by keylogger malware on their machine. With these stolen credentials, the criminal logs in to the user's Facebook account and sends messages to the user's Facebook friends, asking them to wire money—supposedly because the user is stranded in a foreign country.

Skype, the Internet telephony and instant messaging service, is increasingly a target of online scammers, as is Twitter. In June 2009, the Twitter account of venture capitalist and avid Twitter user Guy Kawasaki was used to send his Twitter followers to a malware-infected

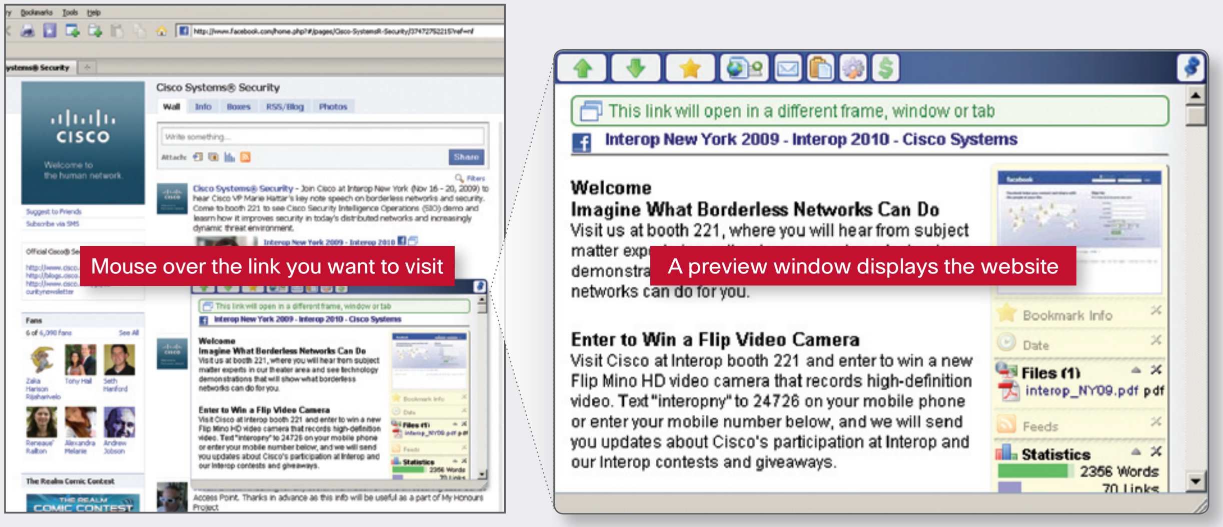
Tiny URLs Equal Big Security Threat

The telegraphic nature of communicating via social media—such as the 140-character limit of Twitter postings—has raised the profile of services that will shorten unwieldy webpage URLs. The free services, such as bit.ly and ow.ly, replace the long URL with a shorter unique address. Individuals who want to share webpages, such as news articles or blog posts, with friends or business colleagues prefer to post short URLs to keep their tweets or Facebook status updates concise.

The problem with short URLs is that they eliminate the user's ability to read the real web address and decide if a link is safe to follow. For instance, a colleague's tweet may indicate that a link leads to a *New York Times* article, but since the link isn't visible, there's no way of knowing where the link will take the user. Many recent Twitter spam attacks (see page 7) use shortened URLs that lead to malware-laden sites.

Unfortunately, as discussed on the previous page, many social media users place so much transitive trust in material posted by friends and colleagues that they do not stop to consider the dangers of following an unidentifiable link. And users who are savvy enough to understand the risks are hesitant to click through on any link they can't see.

Organizations that are raising their profile on social networks and want to encourage web users to follow shortened links are advised to generate their own short URLs and host them on their own domains. Computer users can also protect themselves against malicious links by installing widely available add-ons for their web browsers; these add-ons will display the full URL that is masked by the shortened URL. Such add-ons include Long URL Mobile Expander for Firefox, among many others. In addition, some services like TinyURL.com offer their own full URL preview features.


Mouse over the link you want to visit
A preview window displays the website
Bookmarks Tools Help
Cisco Systems® Security
Wall Info Boxes RSS/Blog Photos
Share
Bookmark Info
Date
Files (1)
Feeds
Statistics

http://www.facebook.com/home.php?#/pages/Cisco-SystemsR-Security/37472752215?ref=nf

Cisco Systems® Security - Join Cisco at Interop New York (Nov 16 - 20, 2009) to hear Cisco VP Marie Hattar's key note speech on borderless networks and security. Come to booth 221 to see Cisco Security Intelligence Operations (SIO) demo and learn how it improves security in today's distributed networks and increasingly dynamic threat environment.

This link will open in a different frame, window or tab

Interop New York 2009 - Interop 2010 - Cisco Systems

Welcome

Imagine What Borderless Networks Can Do

Visit us at booth 221, where you will hear from subject matter expe... demonstra... networks can do for you.

Enter to Win a Flip Video Camera

Visit Cisco at Interop booth 221 and enter to win a new Flip Mino HD video camera that records high-definition video. Text "interopny" to 24726 on your mobile phone or enter your mobile number below, and we will send you updates about Cisco's participation at Interop and our Interop contests and giveaways.

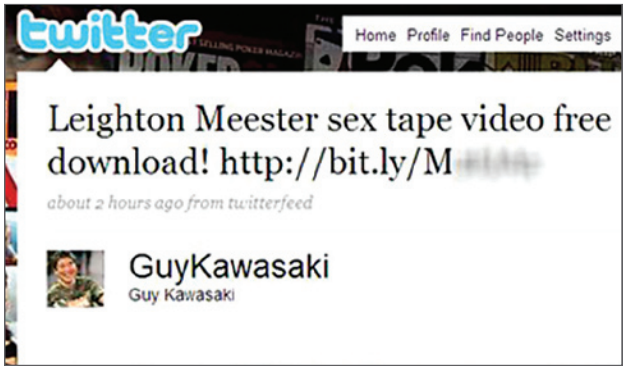
interop_NY09.pdf pdf

2356 Words

70 Links

How to Read Shortened URLs

Web browser add-ons such as Interclue for Firefox expand shortened URLs, helping viewers understand exactly which websites they are visiting.



Leighton Meester sex tape video free download! http://bit.ly/M[redacted]

about 2 hours ago from twitterfeed

GuyKawasaki
Guy Kawasaki

Guy Kawasaki's Twitter account was used to direct visitors to a malware link.

website. The tweet—which came from a news website that Kawasaki added to his Twitter feed—offered a link to an adult video that supposedly featured a star of the U.S. television show *Gossip Girl*. Followers of Kawasaki's Twitter feed who clicked on the link were asked to download a supposed ActiveX update that was, in fact, malware.

The spam, scams, and malware that tie in with social media have one lure in common: They prey on users' comfort level with people they "know" within their social networks. Social networkers assume that since Guy Kawasaki wouldn't throw a malware-infected site in their path, he can be "trusted." However, as Cisco security blogger and researcher Henry Stern recently noted, trust in one's friend network is only as strong as their password security and ability to keep keylogging malware off their machine. This trust makes it easy for users to be misled.

The problem is compounded by the large audiences for social media. People with significant Twitter audiences who mistakenly publish a link to malware will cause far more problems than someone who only tweets to a few friends. The addition of third-party content, such as the newsfeed used by Kawasaki, removes even further control from the account holder in terms of vetting potentially dangerous links. (Read about the problems associated with decentralized content on page 15.)

Criminal Classics: No Shortage of Spam

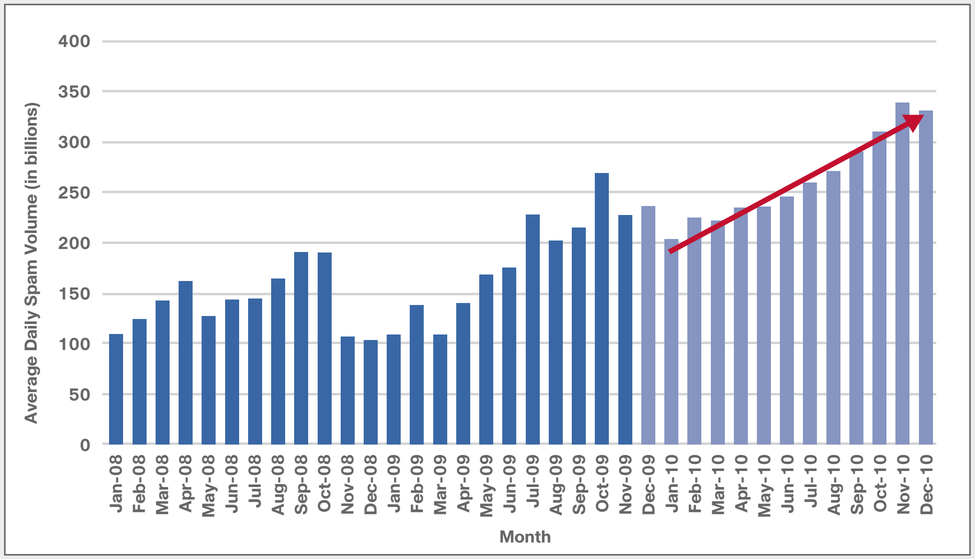
Although criminals continue to use social media to hook new victims, they've by no means abandoned spam, that tried-and-true method for convincing individuals to buy fake pharmaceuticals or download malware. In 2010, spam volume is expected to rise 30 to 40 percent worldwide over 2009 levels, so it's clear that spam is still a threat to business security and productivity.

About 90 percent of the spam delivered by botnets is what the anti-spam industry calls "easy spam." This is the untargeted spam that floods inboxes with messages that appear to originate from various banks, pharmacies, educational institutions, and service providers. Scammers hope to convince the unwary to click through to a malware-laden site or a scam site for pharmaceuticals. Easy spam is trivial to stop for sophisticated anti-spam providers.

"Hard spam," the other 10 percent of spam messages, consumes 90 percent of anti-spam vendors' resources. It is not only much harder to block, but also more dangerous and sophisticated—and it's on the rise. For instance, so-called targeted attacks involve sending a few spam messages to a specific corporate domain, in hopes the messages evade spam-detection systems.

Spear-phishing and "whaling" attacks also fall into this category. These attacks are aimed at just a few high-level individuals in an organization. Since these email messages are usually personalized toward the recipient, they are difficult to block with traditional spam-filtering technology.

Rising Spam Volume in 2010



In 2010, spam volume is expected to rise 30 to 40 percent worldwide over 2009 levels.

Shining a Light on the "Dark Web"

Thanks in part to the popularity of social media, the "Dark Web" is challenging organizations' ability to provide protection from malware and enforce acceptable use policies. The term is applied to the dynamic and transient section of the web that contains billions of webpages, often served up by blogs and social networking sites, that are not categorized by traditional URL filtering databases. Cisco Security Intelligence Operations (SIO) estimates that more than 80 percent of the web can be classified as "dark." The majority of malware threats lurk in the Dark Web, and users who access inappropriate sites hidden in the Dark Web (either intentionally or unintentionally) can raise compliance issues, create legal liabilities, and cause productivity loss.

As the web grows in size, so does the Dark Web. Some 32 million new domains are added every year, and the pace will increase when internationalized domain names (using letters from local languages, such as Arabic and Chinese) are introduced in mid-2010. "New technologies for identifying threats and objectionable content in the Dark Web are helping businesses block websites that previously were nearly impossible to identify," said Ambika Gadre, director of security marketing for Cisco. "Proactive and heuristic techniques that accurately predict the risk of any web server hosting malware, combined with anti-virus and anti-malware scanning, can provide an effective protection against malware. In addition, augmenting URL databases with real-time content analysis to categorize unknown sites on the fly can improve the effectiveness of acceptable use policies in light of the Dark Web."

Online Risks

Online criminals find growing opportunity in accessing and stealing financial account information, as well as tricking computer users into buying “rogue” anti-virus software.

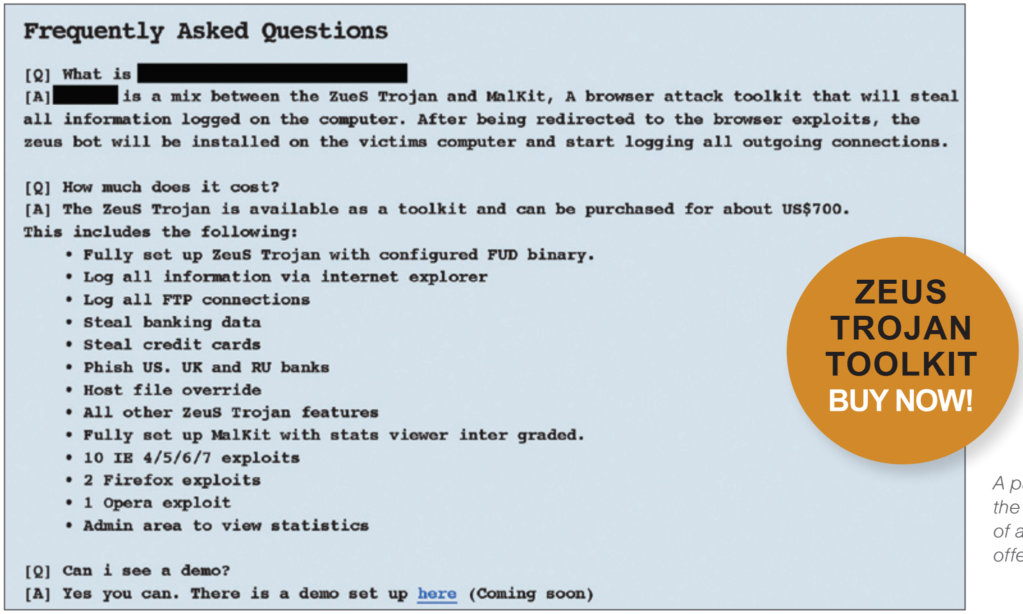
The Rise of the Banking Trojans

Online criminals show every sign of continuing their campaign to steal lucrative financial login information—and they're growing ever smarter and more sophisticated with their tactics. The Zeus and Clampi botnets, which steal online account credentials with a focus on bank accounts, have gained in size and strength in recent months, and no doubt will continue to do so throughout 2010. The Zeus Trojan is estimated to have infected 3.6 million computers as of October 2009; the newer Clampi Trojan is estimated to have infected hundreds of thousands of computers.

The Zeus Trojan is actually available as a toolkit that can be purchased for approximately US$700 (read more about the Zeus package on page 23). Included is a kit that creates new variants of the Trojan, providing each new version with a unique signature that enables it to evade detection by anti-virus programs. The Zeus Trojan commonly infects computers via email phishing attacks or by "drive-by downloads," in which malware infects a user's computer without their knowledge when they visit a webpage. The Zeus malware "listens" in the background for signs that a user is logging in to an account (such as banking or webmail) and then collects those authentication credentials and passes them to the botmaster.

In a particularly innovative twist, when the malware is operational on secure sites that require onetime passwords for logins, the Trojan will ask the user to generate several of these passwords (usually from a hardware token). The malware will then deliver these legitimate passwords to the botmaster, instead of the banking website. The malware can also generate requests for other credentials, such as ATM passwords and "secret questions."

The Clampi Trojan was first spotted in 2007 but is showing high levels of activity as of late 2009. This is sobering since the Trojan, which infects computers using Flash and Active X, is gathering sensitive banking and financial information, just as Zeus does. While Clampi does not include a kit that allows users to create unique variants, it is modular in design, which means criminals can easily modify the malware.



Frequently Asked Questions

[Q] What is [redacted]
[A] [redacted] is a mix between the ZueS Trojan and MalKit, A browser attack toolkit that will steal all information logged on the computer. After being redirected to the browser exploits, the zeus bot will be installed on the victims computer and start logging all outgoing connections.

[Q] How much does it cost?
[A] The ZeuS Trojan is available as a toolkit and can be purchased for about US$700.
This includes the following:

- Fully set up ZeuS Trojan with configured FUD binary.
- Log all information via internet explorer
- Log all FTP connections
- Steal banking data
- Steal credit cards
- Phish US. UK and RU banks
- Host file override
- All other ZeuS Trojan features
- Fully set up MalKit with stats viewer inter graded.
- 10 IE 4/5/6/7 exploits
- 2 Firefox exploits
- 1 Opera exploit
- Admin area to view statistics

[Q] Can i see a demo?
[A] Yes you can. There is a demo set up here (Coming soon)

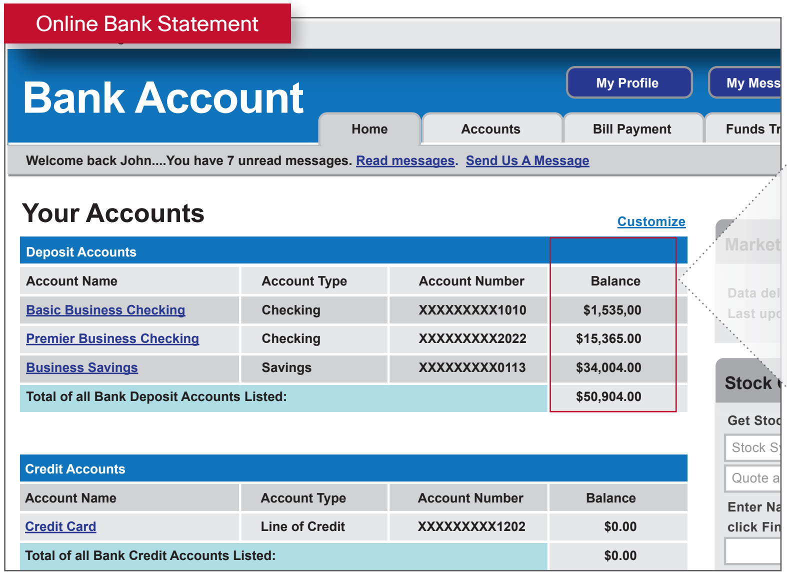
A page on a website selling the Zeus Trojan toolkit as part of a "crimeware-as-a-service" offering.

Once Clampi is installed on an infected system, it sits in the background and monitors user activity for any sign of logins. Because the Trojan searches for signs that a computer user has administrative privileges, Clampi appears to have the potential to spread even faster than Zeus. If this is the case, and an administrator logs in to an infected computer, Clampi could spread throughout an entire network.

Making Clampi even more dangerous is the fact that it obfuscates its code to make anti-virus detection and protection difficult. In one notable attack in September 2009, the Clampi Trojan infected a computer at a Pennsylvania bank, and the criminals who launched the malware were able to steal US$479,000 from the account of the Cumberland County Redevelopment Authority.

A newer entry on the banking Trojan scene is URLZone, which exhibits new methods to shield itself from detection by computer users: When the criminal using the Trojan makes a transfer from a victim's bank account, the Trojan can alter the online bank statement to disguise the fact that an illegal transfer has occurred. Victims who check their bank accounts online only, instead of reading paper statements, would not realize their money had been stolen.

"The sophistication built into Trojans like URLZone and Clampi points to an escalation in the race between user security technologies and attacker capabilities," said Scott Olechowski, Cisco threat research manager. "Online criminals will continue to seek out low-cost efforts to bypass user protections, maximizing their profit and the number of victims. If these sophisticated attacks continue to be adopted by malware creators, the security and financial industries must fight back with solutions that make such attacks cost-ineffective for the attackers."



Online Bank Statement

Bank Account

Welcome back John....You have 7 unread messages. Read messages. Send Us A Message

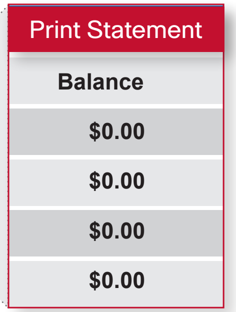
Your Accounts

Deposit Accounts

Account Name	Account Type	Account Number	Balance
Basic Business Checking	Checking	XXXXXXXXX1010	$1,535,00
Premier Business Checking	Checking	XXXXXXXXX2022	$15,365.00
Business Savings	Savings	XXXXXXXXX0113	$34,004.00
Total of all Bank Deposit Accounts Listed:			$50,904.00

Credit Accounts

Account Name	Account Type	Account Number	Balance
Credit Card	Line of Credit	XXXXXXXXX1202	$0.00
Total of all Bank Credit Accounts Listed:			$0.00



Print Statement

Balance
$0.00
$0.00
$0.00
$0.00

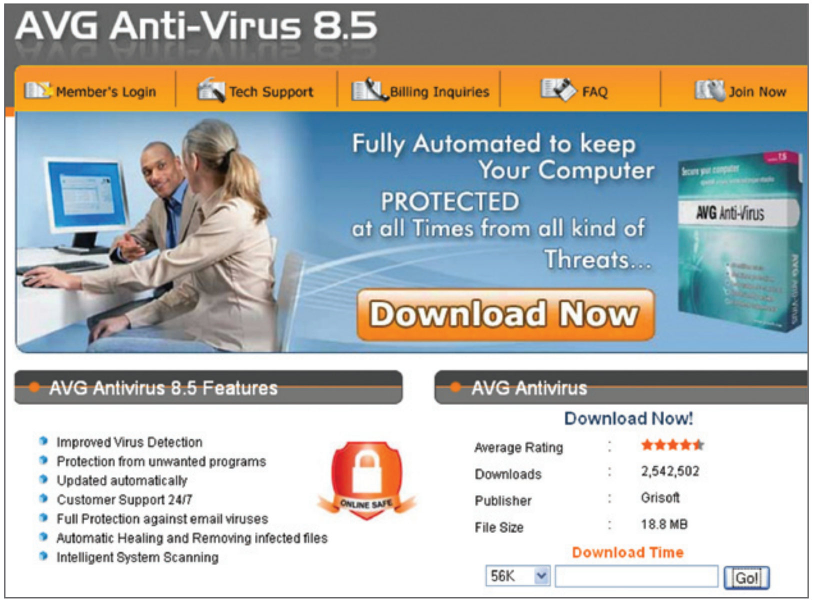
URLZone Offers New Twist on Banking Scams
When a criminal using the URLZone Trojan makes a transfer from a victim's bank account, the Trojan can alter the online bank statement to disguise the fact that an illegal transfer has been made.

Anti-Virus Software Scams

Instead of pretending that their malware is actually legitimate anti-virus software and risking that users will conduct an online search and identify the scam, some criminals are now selling the real thing—sort of. Fake or "rogue" anti-virus software has become a popular and successful social engineering scheme over the past year. In fact, according to the Anti-Phishing Working Group, there has been a five-fold increase in the number of fake anti-virus detections since 2008. Some scams have brought in as much as US$10,000 per day, as well as an abundant supply of victims' credit card numbers.

Users are redirected from *legitimate* websites to sites that attempt to install rogue anti-virus software or dupe users into purchasing free or trial versions of real software from legitimate companies. A pop-up window may appear on the user's screen and display a warning like, "Your computer is infected with a virus! Click here to fix the problem." The solution offered, of course, is a download of the fake anti-virus program. In many cases, users find they are in a "closed loop" situation—unable to click "X" or "Cancel" to close the pop-up and return to their surfing. Out of frustration, many end up just clicking "OK." (Note: If users find themselves in such a loop, simply launch the "Task Manager" application and terminate the browser.)

In the example on this page of a fake anti-virus social engineering scheme, criminals are using an "imposter" version of AVG's website. Through this site, customers are lured into paying for a link to download the *free* version of the real AVG Anti-Virus 8.5 software. Many leading commercial anti-virus companies, like AVG, offer both free and for-fee versions of their anti-virus software.



AVG Anti-Virus 8.5

AVG Antivirus 8.5 Features

- Improved Virus Detection
- Protection from unwanted programs
- Updated automatically
- Customer Support 24/7
- Full Protection against email viruses
- Automatic Healing and Removing infected files
- Intelligent System Scanning

AVG Antivirus

Download Now!

Average Rating	:	★★★★★
Downloads	:	2,542,502
Publisher	:	Grisoft
File Size	:	18.8 MB

Download Time

56K ▾ Go!

Scammers Trick Users with Imposter Websites
Fake or "rogue" anti-virus software has become a popular and successful social engineering scheme over the past year, with criminals using fraudulent websites to dupe users into paying for links to free versions of anti-virus software from legitimate companies.

On the homepage, users are provided with many opportunities to "Download Now!" Even savvy users who take time to investigate whether AVG is a legitimate company are easily duped by the imposter AVG site, which seems real because it is well designed and professional looking. With false confidence, users click the "Download" button.

A login screen is displayed and users are taken through what appears to be a legitimate enrollment process. Victims are asked to choose between a one-year or three-year membership option (US$35 for the latter). But again, they are only paying for a link to download the *free* version of AVG's anti-virus software. Many scammers don't even bother to provide users with something to download; they just take their credit card numbers and disappear. And if you become a victim of this scam, don't bother trying to call the "customer service" number provided—even if a phone rings, no one will answer.

The U.S. Federal Trade Commission (FTC) has been very active in educating consumers about phony security alerts and anti-virus software scams. The agency, through the use of traditional legal channels, has also been successful in undermining the activities of rogue security software distributors.

Cloud Computing and Hosted Services

Ten years ago, when companies guarded information within closed networks, the idea of handing over a sizable chunk of competitive data to a place called the "cloud" didn't have much appeal. Why take the chance of placing sensitive corporate information at so much risk when you could safely monitor it behind your own firewalls?

Today, these solutions are pursued because they are seen as cost-effective, and because they can help create mobile and agile businesses for workers who move far beyond the confines of the home office. However, not only have enterprises become less concerned about the risk inherent in the cloud, but they've swung in the opposite direction from their 1990s colleagues: Many are so trusting of cloud computing that they conduct minimal due diligence when selecting hosting providers and evaluating data security.

The high levels of trust in the cloud computing concept echo the acceptance of social networking—in both professional and personal life—and the willingness of computer users to transmit sensitive information in ways that would have been unthinkable a decade ago. Online users routinely share everything from birth dates to family vacation photos over social networks.

In the workplace, these same users see little threat in exchanging business information over cloud computing applications, instant messaging systems, and other networks that break through the traditional network perimeter. So, how can organizations embrace the benefits that cloud computing brings while not putting valuable business information at risk? They should consider adopting the healthy dose of skepticism traditionally employed 10 years ago, sprinkled with a high level of consciousness to broaden awareness and educate users.

Seeing More Clearly Into the Cloud

Cloud computing increases workforce accessibility to critical business applications, data, and services, while providing a new platform that can help ignite or accelerate new business models. However, many organizations are steadfastly resistant to cloud computing, uncomfortable with relinquishing control of processes and data. Meanwhile, others are perhaps too quick to embrace the cloud—blindly putting faith in their chosen service provider's ability to secure their data and prevent any regulatory headaches.

Without a doubt, cloud computing carries with it the challenge of protecting cloud-enabled business operations, especially in service-provider-managed, hybrid, and public cloud infrastructures. With externalized services, some basic business concerns emerge:

- Where are our information assets going?
- How are they being protected?
- Who will have access to our information?
- How can we navigate policy shifts, regulatory compliance, or audits?

These are the types of questions that business decision-makers *should* be asking of their service providers. In fact, many are doing so more often now—and expecting good answers in return. This is why many leading providers of externalized services are taking steps to help demystify the cloud for their customers and clearly explain their approach to data security.

Many customers are also asking to maintain at least some control over their data once it is in the cloud, such as being able to self-administer controls to assure compliance. Expect to see more providers seriously exploring that option in the near future; it likely will be a business differentiator for many companies, as more businesses decide to embrace cloud computing and look specifically for a provider who can present that capability.

"Organizations also need to recognize that employees have become so used to accessing hosted solutions like web-based email and social networks at home, they naturally bring these solutions into the workplace," said Cisco Vice President and General Manager of Security Products, Tom Gillis. "Workers will use technologies like popular collaboration applications offered from free or affordable service providers without asking the IT department for permission. These applications are now ingrained in the way people share information and work together."

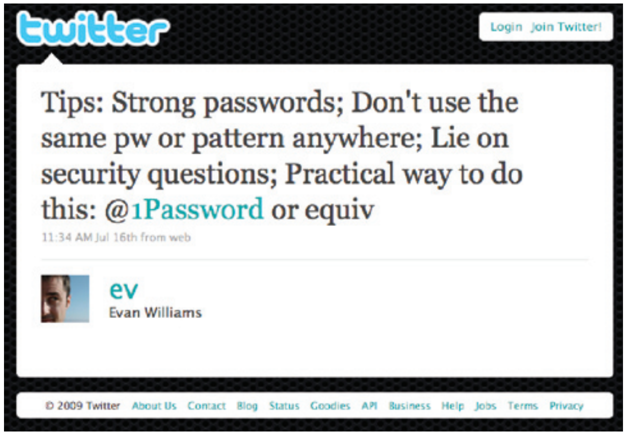
Emerging cloud operating models introduce new risks to an organization or amplify existing ones. A significant challenge with cloud adoption is in relation to its specific use in an enterprise. There are also risks that will extend from incubating technologies or the marriage of technologies that support cloud-based services. These range from new threats like "hyper-jacking" (attackers take control of the hypervisor, the software that serves as the virtualization manager) or "side-channel VM" attacks (attackers monitor CPU and memory cache utilization on a shared server to pinpoint periods of high activity on target servers and launch attacks) to simple access configuration errors and even inadvertent data exposure in multitenant storage models.

The Password Problem: Recycling Is Not a Good Idea

When hackers recently posted several thousand Hotmail, Gmail, and Yahoo! passwords and user IDs on a public website, security watchers scanned the list for the most common passwords. The number string "123456" was at the top of the list—an unsafe password that criminals can easily guess to compromise webmail accounts.

Most organizations try to avoid weak passwords by establishing rules about length and use of alphanumeric combinations, and requiring employees to change their passwords periodically. However, the rise of social media and cloud computing is exacerbating the password problem and making it easier to make predictable guesses about passwords.

In mid-2009, a hacker gained access to the Twitter account of Twitter CEO Evan Williams. The hacker initially used the password recovery tool to access accounts at the Gmail webmail service, and then used information gleaned from these accounts to access the accounts belonging to Williams and other Twitter employees.


twitter
Login Join Twitter!

Tips: Strong passwords; Don't use the same pw or pattern anywhere; Lie on security questions; Practical way to do this: @1Password or equiv

11:34 AM Jul 16th from web

ev
Evan Williams

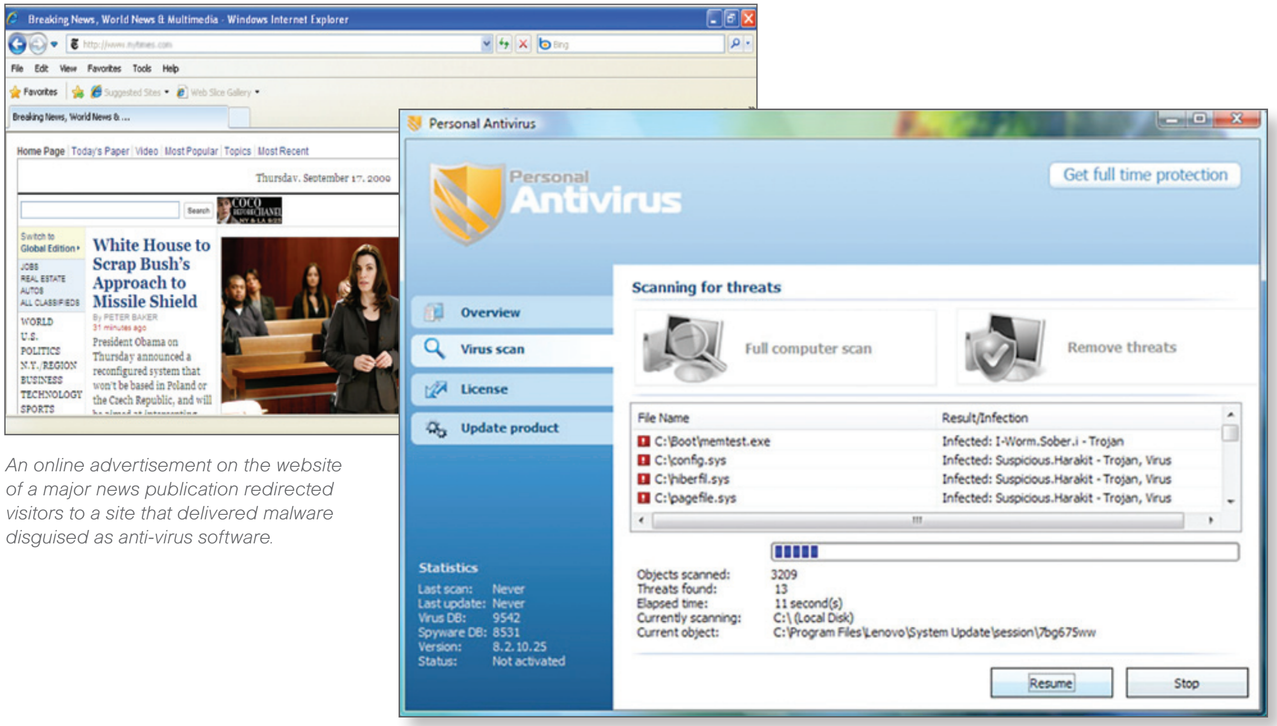
© 2009 Twitter About Us Contact Blog Status Goodies API Business Help Jobs Terms Privacy

Words of Advice from Twitter's Evan Williams
After his Twitter account was hacked, Twitter CEO Evan Williams offered some advice on password security.

The hacker was able to make educated password guesses using publicly available information about Williams and the other employees. Once the criminal took control of employee Twitter accounts, he was able to leverage that data to compromise related accounts and eventually access confidential business documents and employee records.

Although most individuals' personal details are not as well known as those of a high-profile business executive, it is certainly true that social media encourages sharing of data that is either tied to passwords, or to password recovery questions. For instance, if a hacker knows your cat's name is Fluffy, he also knows there's a good chance that one or more of your passwords has Fluffy's name embedded in it. With the rise of tools for password guessing, criminals can leverage botnets to try every variant of strings that contain "fluffy" until they hit the right password. More importantly, you may be using this information as an answer to password recovery questions for not just one, but multiple accounts.

The apparent ease of cracking weak passwords is exacerbated by the multiple-password problem. As organizations embrace externalized services such as cloud computing, they require workers to log in to outsourced applications with separate passwords. Fatigued employees, tired of coming up with a dozen or more unique passwords, may simply create passwords that are only slightly different from each other—perhaps by adding a number to the end of a name. Or, worse, they'll just use the same passwords over and over again.



Thursday, September 17, 2009

White House to Scrap Bush's Approach to Missile Shield

By PETER BAKER
31 minutes ago
President Obama on Thursday announced a reconfigured system that won't be based in Poland or the Czech Republic, and will

Scanning for threats

File Name	Result/Infection
C:\Boot\memtest.exe	Infected: I-Worm.Sober.i - Trojan
C:\config.sys	Infected: Suspicious.Harakit - Trojan, Virus
C:\hiberfil.sys	Infected: Suspicious.Harakit - Trojan, Virus
C:\pagefile.sys	Infected: Suspicious.Harakit - Trojan, Virus

```
Objects scanned:     3209
Threats found:       13
Elapsed time:        11 second(s)
Currently scanning:  C:\ (Local Disk)
Current object:      C:\Program Files\Lenovo\System Update\session\7bg675ww
```

Statistics

```
Last scan:    Never
Last update:  Never
Virus DB:     9542
Spyware DB:   8531
Version:      8.2.10.25
Status:       Not activated
```

An online advertisement on the website of a major news publication redirected visitors to a site that delivered malware disguised as anti-virus software.

To combat this problem, corporate IT departments can implement password manager solutions that collect all necessary passwords, encrypt them, and make it easy for users to access programs without having to remember passwords. This allows employees more freedom to create passwords that are complex and unique, which means they are more secure. Individual computer users can do the same, using password management solutions built into web browsers, such as Mozilla Firefox's master password feature and many others. However, when this measure is used on a laptop, users must retain physical control of the machine or risk handing a criminal easy access to all of their systems.

Web Threats and Other Vulnerabilities

Online criminals leave no stone unturned when seeking out new ways to exploit vulnerabilities or lure new victims into downloading malware—for instance, by creating malware using the Java programming language. Such Java-based malware can spread quickly because it will run regardless of the device or platform being used, and because it is difficult for anti-virus programs to detect Java code.

While the social media world is the venue seen by many cybercriminals as offering the best return on investment for illegal campaigns, other methods for launching scams or distributing malware have not been abandoned. The following threats are expected to cause concern in 2010.

Decentralized content: As websites increasingly pull content from a wide range of sources—as many as 150 sources for a typical webpage—computer users may fall victim to threats and scams even from legitimate online businesses.

In September 2009, a major news publication announced that a homepage online advertisement, served up by one of the newspaper's ad networks, was delivering malware to people who clicked on it. The advertiser initially claimed to represent Vonage, the telecommunications company; however, once posted, the ad was switched to a computer virus warning that offered "anti-virus" software. Unsuspecting users who installed the fake software appear to have also installed malware.

In its own coverage of the incident, the publication reported that other news websites have fallen victim to similar scam ads, owing to their reliance on ad networks. This incident, along with other notable examples, have made it clear that it is advisable for organizations to review ads carefully and ensure that they are working with legitimate third-party vendors. Of more concern are smaller websites, particularly blogs, whose owners don't have the manpower to inspect every ad they display.

According to Cisco Security Intelligence Operations, one in every 600 PDF files downloaded from the web contains malicious software.

In October 2009, two popular blogs, Gawker.com and Gizmodo.com, fell victim to fake ads for Suzuki vehicles. The ads served up malicious code to any site visitors who clicked on them. In this particular scam, the criminals gained the trust of the blogs' ad sales staff by exchanging several rounds of emails regarding ad placement and payment terms—using industry lingo that gave the targeted salespeople a comfort level that they were dealing with authentic vendors.

"For corporate users, the solution to the decentralized content problem lies in web reputation technology, which would block such an ad's malware download," said Cisco Fellow and security researcher, Patrick Peterson. "By analyzing URLs to assess their trustworthiness—for instance, how long the domain has been registered and the country in which it's registered—web reputation systems can instantly block a suspect URL from loading."

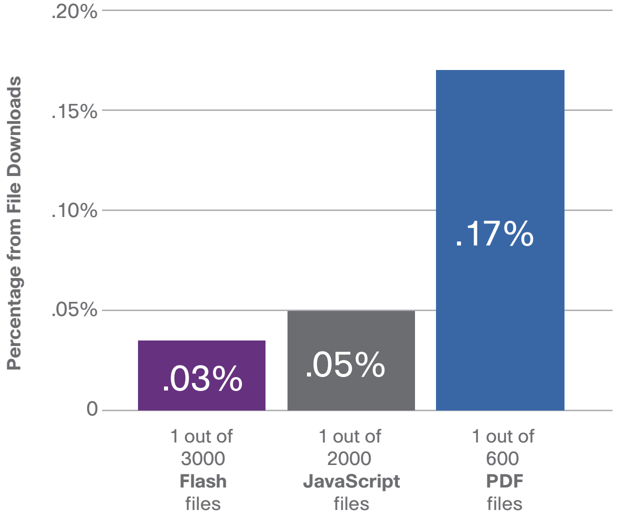
PDF/Flash/JavaScript exploits: On a given day, computer users run hundreds, if not thousands, of JavaScript and Flash objects while they browse the web. Business users also make heavy use of documents based on the Adobe PDF format.

According to information gathered by Cisco Security Intelligence Operations, these ubiquitous web file types are some of the most dangerous, with one in every 600 PDF files downloaded from the web containing malicious software. The data showed that one out of every 2000 JavaScript files, and one out of every 3000 Flash files, also contain malware.

Although these numbers may not seem significant, the heavy use of these applications on the web and the high profile of the software in the business world magnify the threat. According to Adobe's own statistics, its Flash Player is installed on 99 percent of all personal computers; Adobe also states that 500 million copies of its reader software have been distributed worldwide.

The answer to this threat is fairly straightforward: Users need to be vigilant about installing the latest versions of application software because new versions will contain the latest security patches. In addition, updated anti-virus and firewall programs will provide protection against malware that is associated with these applications.

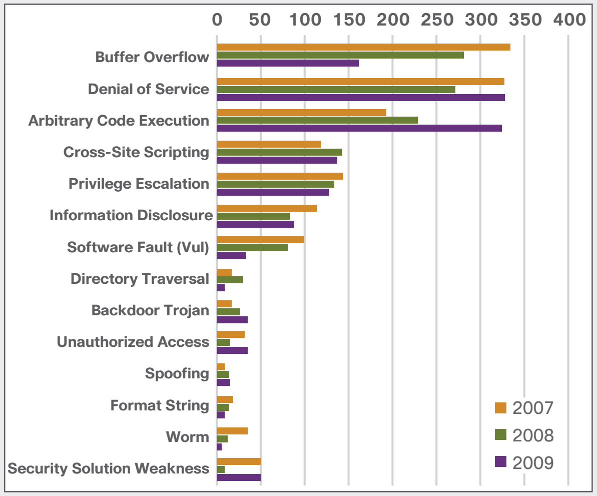
Malicious Software in Common Web Downloads



A growing number of PDF, Flash, and JavaScript files contain malicious software.

2009 Vulnerabilities and Threat Analysis

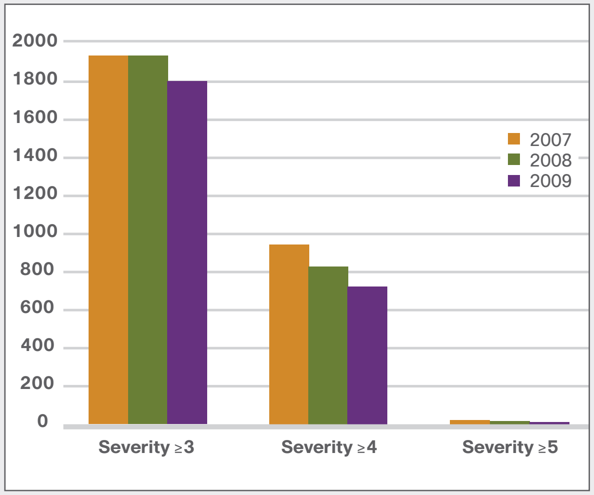
Vulnerabilities and Threat Categories



The "**Vulnerability and Threat Categories**" chart above depicts threat and vulnerability categories and shows a shift toward increased arbitrary code execution vulnerabilities and Trojans, as well as a substantial decrease in buffer overflow vulnerabilities, software faults, directory traversal attacks, and worms during 2009.

In addition, the metrics show continued high levels of denial of service, cross-site scripting, privilege escalations, unauthorized access, and spoofing vulnerabilities and threats. The increased number of Trojans, unauthorized access vulnerabilities, and spoofing vulnerabilities and threats are consistent with the shifts in criminal activity that seeks access to and control over a compromised system.

IntelliShield Alert Severity Ratings

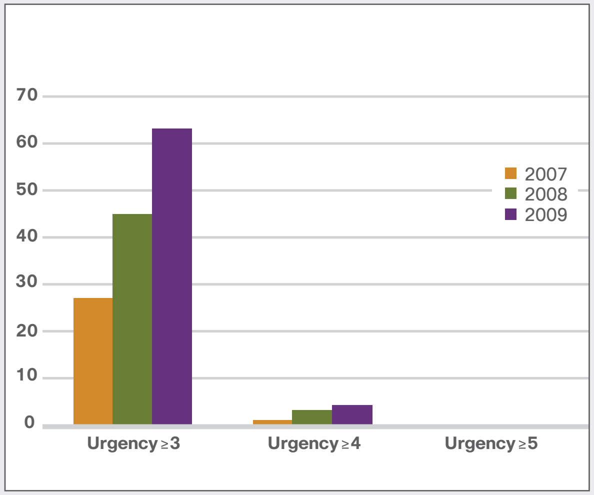


The "**Intellishield Alert Severity Ratings**" data indicates that severity vulnerability and threat metrics in 2009 remained consistent with previous years—and even decreased slightly.*

* The metrics in these charts are based on Cisco Security IntelliShield Alert Manager year-over-year alert production statistics and do not necessarily reflect or conflict with metrics of other sources that may show increased or decreased levels of vulnerability and threat activity. To reduce the noise levels for customers, IntelliShield provides a first level of threat filtering and does not alert customers to vulnerabilities and threats that are not likely to impact business and government environments.

Other similar vulnerability and reporting sources may have different reporting criteria and vary from these metrics. IntelliShield bases its reporting on individual vulnerabilities or threats. For example, the multiple variations of the Koobface worm are reported in a single alert and regarded as one threat. That single alert and threat is updated with the latest information and variants and republished, not reported or counted as a separate threat.

IntelliShield Alert Urgency Ratings



The urgency ratings depicted in the "**IntelliShield Alert Urgency Ratings**" chart reflect a significant increase in exploit and attack activity. An urgency rating of three or greater indicates vulnerability exploits and attacks have been identified and are actively occurring.

The significant increase in level-3 ratings also indicates that a greater—and broader—number of vulnerabilities and attacks are occurring. In previous years, exploits and attacks could often be credited to a smaller number of vulnerabilities that were being widely exploited, such as with worms or other malicious codes. However, the 2009 data shows a more extensive number of vulnerabilities that are being actively exploited, requiring a higher number of patches, mitigations, and broader monitoring activity.

The Cybercrime Monetization Primer

Scammers earn millions annually by stealing personal information from worldwide Internet users. Ever wonder how they reap rewards from their exploits? Read on.

Without question, cybercrime that is not financially motivated—including politically motivated DDoS and website defacement, state-sponsored attacks, and general vandalism—is, and will continue to be, a serious issue. However, the vast majority of attacks are designed to make money. Most incidents are not publicized unless a very large group of people are compromised at once. But they are happening right now, everywhere, to many people.

How do cybercriminals turn their exploits into cash? Even knowledgeable security professionals who understand these types of attacks may not understand the numerous schemes used to monetize them. The following primer, broken down into "moneymaker" categories (not ranked), is designed to provide an overview of popular techniques that can reap financial rewards—and unfortunately for victims, often with great success.

Moneymaker # 1: Financial Fraud

Unauthorized bank transactions or credit card charges

Top techniques include account and identity theft with credential phishing, keylogging malware, and data theft from merchants and processors being the largest source of credentials.

EXAMPLE: Zeus

Advanced fee fraud

Numerous schemes exist to trick a consumer into providing an advanced payment for future gain. Most notorious are the so-called "419" spammers who promise millions to naïve users who offer to help the deposed King of Nigeria transfer a fortune out of the country. Modern variants involve fraudulent posts on social networking sites or online marketplaces. Top techniques include spam and public forums, especially social networks.

EXAMPLE: Craigslist property scams

Moneymaker #2: Product Sales and Advertising

Product sales

A leading moneymaker for criminals continues to be the advertisement and sale of products. Top-producing examples include "spamvertized" sales of pharmaceutical products, spamvertized or "spamdexed" advertisements for pirated software, and scareware. 2009 saw massive profits generated by scareware spyware and weight-loss remedy scams. Spam, spamdexing, advertisements on social networks, and use of malware are common techniques.

EXAMPLE: Spam driving sales of acai berry weight-loss products

Advertising

Criminals aggressively pursue advertising revenue via a number of successful channels. In these cases, the criminal is not involved in the scam or product fulfillment but is compensated simply for traffic or subscriptions. Spam, spamdexing, click fraud, and impression fraud are all techniques. In many cases, the criminal profits by enrolling in a legitimate business's affiliate marketing program.

EXAMPLE: Name your favorite search engine

Moneymaker #3: Criminal Services

Criminals selling products and services to other criminals to enable cybercrime is big business. Top techniques include:

Selling malware and exploits

Examples in this category include the sale of zero-day exploits, malware packages such as Zeus, and exploit kits like Liberty and Fragus. There is even a business "opportunity" just to provide software that helps package exploits so they are not easily detectable by anti-virus scanners.

EXAMPLE: Fragus

Selling account information (usernames and credentials)

The rise of criminal specialization has resulted in an environment where those who steal credentials are often not the criminals who carry out the financial fraud. Numerous businesses exist for the sole purpose of stealing and selling credentials. Nonfinancial credentials, such as social networking and email credentials, have been a growing revenue source as well.

EXAMPLE: URLZone

Selling CAPTCHA breaking

Cybercriminals are generating revenue by selling specialized account creation and CAPTCHA-breaking services. Criminals who create millions of social networking and email accounts on free services must sometimes break CAPTCHAs to do so. They use these accounts to send spam or penetrate social networks for the purposes of stealing credentials, launching social engineering schemes by writing on people's online walls, and so on.

EXAMPLE: CAPTCHA King

Selling virus testing

The real purpose of this scheme is to determine whether popular virus packages will indentify binaries.

EXAMPLE: VirTest

Selling search redirecting

A user enters a search into Google but is redirected to a website paid for by a criminal or a criminal's victim.

EXAMPLE: Koobface (see page 7)

Which cybercrime techniques will likely be “winners” and “losers” in 2010? Cisco security experts have made some predictions.

The Cisco CROI Matrix

As noted in previous Cisco security reports, more cybercriminal operations are behaving like “legitimate” businesses. Therefore, using standard business assessment methods may be the best way to track the performance of underworld marketplaces.

Which cybercrime techniques appear to have the edge going into 2010? Cisco security experts have made some predictions on attack methods and scams that are likely to be the real “winners” and “losers” in the coming year.

The results of this analysis are depicted on page 21 in the Cisco Cybercrime Return on Investment (CROI) Matrix. The format for this illustration is inspired by the well-known “Growth-Share Matrix,” which was introduced by the Boston Consulting Group in the 1970s. The matrix is a tool for helping businesses determine which areas of their operations deserve more investment. The exploits appearing on the Cisco CROI matrix are explained in greater detail in this report, including in the “Cybercrime Monetization Primer” on page 18.

Rising Stars: Which methods of duping or stealing from unsuspecting users will be most popular next year? Organizations can bet that many savvy cybercriminals will focus their investment activities in 2010 on supporting the continued success of massive banking Trojan Zeus, as well as the entire field of lucrative and easy-to-deploy web exploits like those seen in 2009.

Cash Cows: Who can say no to easy money? Don’t expect tried-and-true methods such as scareware, spyware, click fraud, advanced fee fraud, and pharma spam to fade anytime soon.

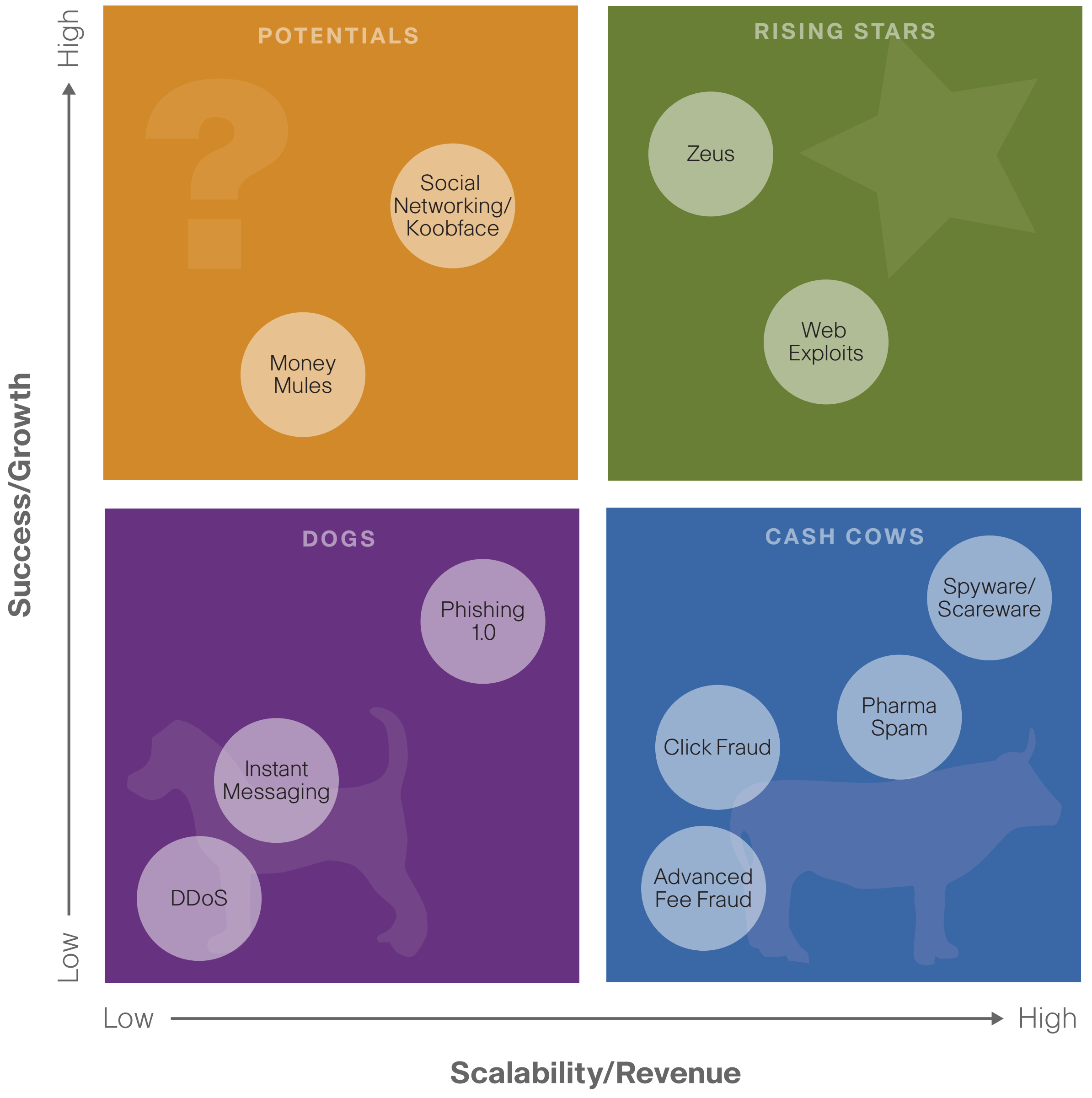
Dogs: Who are the tired old hounds in the pack? You can expect to see cybercriminals abandon well-worn and unsophisticated phishing and instant messaging scams.

In addition, there isn’t much growth or monetary success expected in the area of DDoS attacks—only because the motive behind these types of disruptive attacks is typically political. (See Political Attacks: Controlling the Conversation, page 4.)

Potentials: What tricks and techniques are the wait-and-see moneymakers for 2010? Social networking exploits, including the Koobface worm, have been successful but are really only starting to hit their stride when it comes to investment returns for cybercriminals. This is because social networking is still new territory for many users worldwide—but that’s changing fast.

Another unknown, “money mules,” represent an important link in the monetization food chain, but they keep getting caught. The bad economy has made it easy for cyber-criminals to recruit new participants, but as the global financial crisis eases, money mules could dwindle in numbers. (See sidebar, “Letting Money Mules Carry the Load,” page 22.)

The Cisco Cybercrime Return on Investment Matrix



The Cisco CROI Matrix predicts cybercrime techniques that will be "winners" and "losers" in 2010.

Who can say no to easy money? Don't expect "cash cows" like pharma spam to fade in popularity with cybercriminals anytime soon.

Letting Money Mules Carry the Load

One way that many cybercriminals cash in on their exploits is through the use of "money mules." Although sophisticated scammers may be able to gather enough information about victims to use their credit cards and access their online bank accounts, there are some significant hurdles in cashing out those accounts. First, international money transfers are usually met with great scrutiny. Second, such transfers often leave a money trail behind, which increases the chances of criminal prosecution. The solution: recruiting money mules to facilitate money laundering.

Money mules can be lower-level criminals willing to engage in a shady financial transaction to make some quick cash. But more often, they are people seeking legitimate employment who end up being tricked by criminals. Does this too-good-to-be-true offer sound familiar? "Work from Home—Make Thousands Every Month!" Although there are certainly legitimate businesses that advertise for help in this fashion, many "opportunities" are just schemes that criminals use to snare naïve or down-on-their-luck individuals who are then fooled into becoming unsuspecting money mules.

It is not unusual for criminals to recruit dozens of victims and collaborators to stage just one large operation. Here's how the fraud might occur: A criminal obtains access to a victim's bank account (through the Zeus Trojan, for example). A team is assembled. Money is transferred from the victim to the mules' bank accounts. The mules are told to withdraw the funds, transfer the majority of the money overseas, and keep a small percentage. They are instructed to wire the cash via Western Union or MoneyGram, typically to locations in Africa and Eastern Europe.

Not surprisingly, many money mules are caught quickly—and face heavy fines and jail time—so the criminals are constantly in need of replacements. But the real criminal remains safely overseas, unknown to law enforcement.

In addition to using spam to recruit money mules, some criminals actually troll popular employment sites looking for candidates. A "recruiter" contacts a job seeker, saying that he or she represents a generic but credible-sounding organization that is looking to hire "local agents" or "financial agents." Job seekers believe they are being contacted by a legitimate company because the individual on the phone references their resume and job search aspirations. This scam represents yet another good reason for users to be mindful about personal details they post online—and for businesses, such as employment sites, to make sure the information they host is more secure.

The use of money mules is not new. But in the historic economic conditions of 2009, cybercriminals had little difficulty assembling a bountiful amount of victims and cohorts. Consider two examples of crimes in the United States from the past year involving money mules. In mid-July, a demolition company in California lost nearly half a million dollars when cybercriminals initiated a large batch of transfers from the firm's online bank account to nearly 40 money mules. That same month, attackers sent false payroll deposits to more than two dozen money mules, stealing roughly US$400,000 from a county in Kentucky.

For additional insight into how money mules are recruited and how they operate, see *Washington Post* reporter Brian Krebs' *Security Fix* blog entry, "'Money Mule' Recruitment Network Exposed," http://voices.washingtonpost.com/securityfix/2009/09/money_mule_recruitment_101.html. (Note: Krebs was named the 2009 "Cybercrime Hero" in the Cisco Cybercrime Showcase, page 5.)

Do Online Criminals Read *BusinessWeek*?

A growing market for business services, strong competition, and a race for strategic acquisitions—these are the hallmarks of any emerging industry. Unfortunately, these are also the hallmarks of the online criminal world, which continues to borrow the best ideas from legitimate businesses.

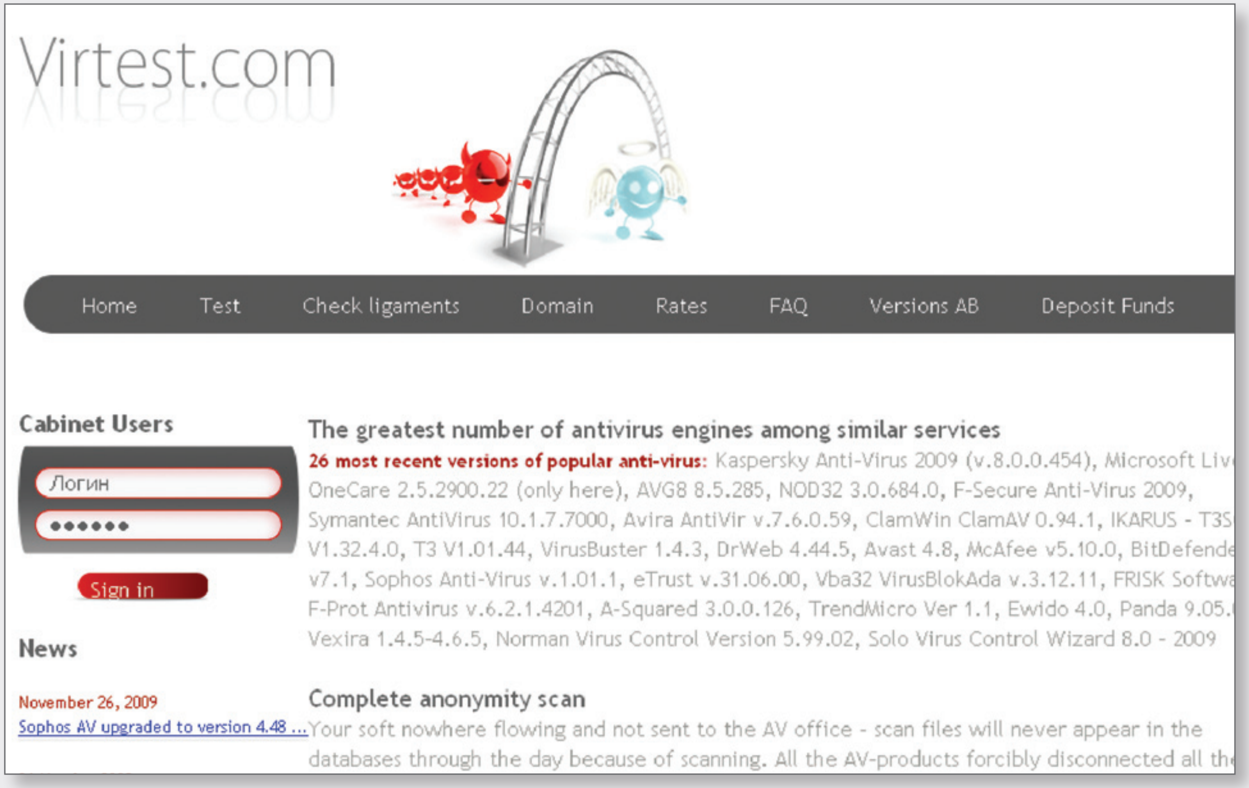
Online marketplaces: Criminals have created markets in which their colleagues can buy the goods they need to launch or manage their own illegal enterprises. Such marketplaces might offer anything from keylogging software to stolen credit card numbers and webmail passwords.

Software testing services: Criminals can now have their malware tested by a service to see if the malware can be detected by major anti-virus programs. If the malware sails through the test, its creator has some assurance that his or her product will sidestep such barriers.

Affordable and fast "customer" acquisition model: Large botnets, such as the one built from the Clampi banking Trojan, have perfected the art of automatically adding new "customers" (victims) by invisibly infecting unpatched computers and then spreading via networks.

Driving down costs via competition: Criminals have become so adept at stealing credit card numbers and other sensitive financial information that supply has outpaced demand, and the value per record has dropped dramatically. In mid-2009, Verizon Business reported that prices for stolen credit card data declined from between US$10 and US$16 per record in 2007 to less than 50 cents per record in 2009.

Developing "startup kits": The Zeus/Zbot kit offers online criminals everything they need to steal financial login data. The package, which can be purchased for about US$700, includes the Trojan that launches the attack, along with a kit to create new variants of the Trojan with unique signatures to avoid detection by anti-virus programs. (Read more about Zeus on page 11.)



The greatest number of antivirus engines among similar services

26 most recent versions of popular anti-virus: Kaspersky Anti-Virus 2009 (v.8.0.0.454), Microsoft Liv OneCare 2.5.2900.22 (only here), AVG8 8.5.285, NOD32 3.0.684.0, F-Secure Anti-Virus 2009, Symantec AntiVirus 10.1.7.7000, Avira AntiVir v.7.6.0.59, ClamWin ClamAV 0.94.1, IKARUS - T3S V1.32.4.0, T3 V1.01.44, VirusBuster 1.4.3, DrWeb 4.44.5, Avast 4.8, McAfee v5.10.0, BitDefende v7.1, Sophos Anti-Virus v.1.01.1, eTrust v.31.06.00, Vba32 VirusBlokAda v.3.12.11, FRISK Softwa F-Prot Antivirus v.6.2.1.4201, A-Squared 3.0.0.126, TrendMicro Ver 1.1, Ewido 4.0, Panda 9.05. Vexira 1.4.5-4.6.5, Norman Virus Control Version 5.99.02, Solo Virus Control Wizard 8.0 - 2009

November 26, 2009
Sophos AV upgraded to version 4.48 ...

Complete anonymity scan

Your soft nowhere flowing and not sent to the AV office - scan files will never appear in the databases through the day because of scanning. All the AV-products forcibly disconnected all th

Emulating Anti-Virus "Testing" Services
Criminals can now hire third-party vendors to test their malware and determine whether it can be detected by major anti-virus programs.

United States Government Update

The Obama administration has identified innovation as the key to making the Internet more secure for all users. It is also taking an interagency approach to improving national cybersecurity—with coordination and direction from the White House.

In May 2009, the Obama administration issued the *Cyberspace Policy Review* report[2], which includes key findings and recommendations from the "60-Day Review" of the United States (U.S.) cybersecurity infrastructure and from the *2008 Securing Cyberspace for the 44th Presidency* report developed by bipartisan, nonprofit organization, the Center for Strategic and International Studies (CSIS)[3]. It was obvious, based on President Barack Obama's public comments, that he had personally spent time on the report, underscoring his pledge to focus on improving the nation's cybersecurity and technology.

The *Cyberspace Policy Review* report examines some serious, substantive cybersecurity issues and is intended to be a firm starting point on the path toward increasing the security of government, critical infrastructure, and consumer systems, both domestically and globally. One issue the new administration grappled with early on was what the proper role of government should be—more specifically, how intrusive it should be in the economy, and with business in the private sector to improve national cybersecurity. So far, it appears the administration understands that security is a fast-changing discipline. It has identified innovation as the key to making the Internet more secure. Embracing innovation shows the president and his cybersecurity advisors understand that today's threats and vulnerabilities will not be those of tomorrow, and that having access to the best resources and knowledge available is essential.

The Obama administration has decided that an interagency approach to cybersecurity, with coordination and direction from the White House, is critical. National economic and security agencies included in the interdisciplinary team are the National Security Council, the National Economic Council, the Office of Science and Technology Policy, the Office of the United States Trade Representative, the Department of Justice, the Department of Defense, the Department of Commerce, the State Department, the Federal Trade Commission, the Federal Communications Commission, the Federal Bureau of Investigation, and the U.S. Secret Service. However, as of November 2009, President Obama had not yet named a cybersecurity coordinator.

Meanwhile, the U.S. government is working to increase staff at the Department of Homeland Security (DHS) in the name of cybersecurity. The DHS recently announced it intends to hire up to 1000 cyber experts over the next three years, including analysts, developers, and engineers who can detect, investigate, and deter cyber attacks. This was the first major personnel move related to the administration's cybersecurity mission, although the government does face the challenge of locating and then convincing these experts to give up jobs in education and private industry to work for the DHS.

In addition, in June 2009, Defense Secretary Robert Gates issued an order that established the U.S. CyberCommand—or "CYBERCOM." This subunit of U.S. Strategic Command is responsible for defending the U.S. military's cyberspace territory, including the .mil domain. The order "is recognition that cyberspace is a distinct military domain, along with land, sea, and air, and the Defense Department must be prepared to defend and conduct offensive operations in it."[4] CYBERCOM, headquartered with the National Security Agency (NSA) in Fort Meade, Maryland, is expected to reach full operating capacity in October 2010. The first CYBERCOM commander is expected to be the NSA's director, Army Lt. Gen. Keith Alexander.

In 2010, organizations should expect to see a continuing emphasis from the U.S. government on the improvement of best practices, guidelines, information-sharing, public-private partnerships in critical infrastructure, education, and R&D focused on breakthrough technologies. The Obama administration will also look for ways to simplify and accelerate the procurement and certification process, so that the U.S. government itself can have access to the latest innovations.

This year's U.S. *Cybersecurity Policy Review* report also acknowledged the interconnectedness of the Internet and the international community, as well as the need to create acceptable norms for all countries concerned about cybersecurity. It is clear President Obama's actions demonstrate that he would like the United States to be seen as taking leadership in the area of cybersecurity. It also appears that he hopes the international community will be inspired to collaborate with the United States on establishing norms—both in regard to development of cybersecurity best practices and law enforcement activities—that will lead to making the Internet a safer place for citizens worldwide.

So far, the international community has also recognized that cybersecurity is an important issue and has discussed it in various forums and venues worldwide. It is apparent from these discussions that countries have taken different approaches, particularly on the issue of the proper role of government intervention in security, the role of domestic and international technical standards, and the maturity of international law enforcement activities. The global community is still in the process of settling on the norms for these interactions. But the

[2] "Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure," May 2009, www.whitehouse.gov.

[3] "Securing Cyberspace for the 44th Presidency," CSIS, December 2008, http://csis.org/program/commission-cybersecurity-44th-presidency.

[4] "DOD Creates Cyber Command as U.S. Strategic Command Subunit," by William Jackson, *Federal Computer Week*, June 24, 2009.

Compliance Does Not Equal Security

In recent years, the federal government and several states, including Massachusetts and Nevada, have enacted legislation to protect sensitive data as well as consumers and their privacy. The Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Trade Commission's "Red Flags Rules" are only some of these measures. (For detail on these regulations, see the *Cisco 2009 Midyear Security Report*, http://cisco.com/web/about/security/intelligence/midyear_security_review09.pdf.)

Compliance regulations are necessary in a world where fraud—from mortgage scams to ponzi schemes—is rampant. However, these rules often lack flexibility and adaptability, which can make it challenging for companies to maintain compliance as technology used to create, exchange, and store data continues to evolve at a rapid pace. It is also becoming increasingly evident that these measures cannot be fully effective without adequate enforcement and clarity about penalties.

Many organizations only take a strong interest in compliance if they or a company they do business with suffers a security breach. In addition, the repercussions of noncompliance—such as fines—are often minimal, even nonexistent. Although there are some exceptions (such as PCI DSS 1.2), it's easy to see why compliance measures are often viewed by businesses as routine "check-box" activities for satisfying auditors, instead of best practices that organizations should embrace from the top down.

Even with the new U.S. administration, although there may be new regulations, such as expansion of HIPAA's security and privacy provisions, the enforcement component is still lacking. It remains unclear, for example, how it will be enforced and how audits to ensure compliance will be performed. However, for healthcare agencies to receive federal funding, they must be compliant with these regulations and meet deadlines, or they will lose that money. This will likely serve as a "carrot" to ensure compliance.

Carrots or not, no company should risk noncompliance with regulations. Organizations that must comply with one or more data security and consumer privacy regulations must understand that a security breach *could* happen at their organization at any time, and it could originate from outside or *inside* the company. As for risking noncompliance, organizations must consider how much risk they are willing to take, and how much a potential breach could cost.

Policies to ensure compliance remain a must-have for businesses, particularly for compliance audits. But maintaining policy has taken a backseat at many companies due to the financial crisis.

Advice for the year ahead: Revisit compliance policies now because the financial crisis has brought a great deal of change—not just globally, but likely within an organization. For example, has your company shut down offices? Hired or fired contractors? Started outsourcing? Moved critical data and key functions to the cloud? Although it's true that your organization may have been compliant before, it may not be now.

Compliance is becoming a top-of-mind issue for organizations outside of the United States as well, due partly to increased financial regulations, like the Sarbanes-Oxley Act, which prompted similar regulations internationally (such as Japan's J-SOX initiative). In 2009, there were several non-U.S. compliance violations reported in the news—particularly in Europe, where disclosure laws and data privacy laws are being formulated, and in Asia.

Obama administration's review of U.S. cyber policy and its innovation and public-private partnership approach to security might provide a discussion framework for building out these international norms.

In 2009, in response to complaints about "American dominance" of the Internet, the United States relinquished some of its control over how the network is run, thereby clearing the path for other governments to play a more significant role in shaping the Internet's future. California-based Internet Corporation for Assigned Names and Numbers (ICANN), which is the official body controlling development of the Internet—and is responsible for overseeing the .com, .net, and .org domains—announced in September that it was ending its agreement with the U.S. government. This move helps to position ICANN as an international body and will allow for more involvement from organizations worldwide.

There also have been positive signs recently that U.S. authorities can expect to have greater international cooperation in the fight against cybercrime. For example, in October 2009, the Federal Bureau of Investigation (FBI) announced that U.S. and Egyptian authorities had charged nearly 100 people involved in an identity theft ring—the largest number of defendants ever charged for a cybercrime case. The bust was nicknamed "Operation Phish Fry."

More than 50 people in the United States were charged with running a phishing scheme; nearly the same number of criminals were arrested in Egypt. According to the indictment, Egyptian hackers used emails to direct victims to phony bank websites, where they were asked to update account numbers and passwords. The FBI reported that the scammers had compromised thousands of bank accounts.

Data Loss: A Few Ounces of Prevention ...

It's not glamorous. It doesn't have the panic-fostering ability of a massive worm or the intrigue of online espionage, but data loss is a very real and significant risk for any business organization. And if a data loss incident is serious and far-reaching enough, it can certainly grab and hold on to headlines. However, for many organizations, data loss prevention has typically been a "we'll-get-around-to-it" item, at least beyond protecting any data that relates to a compliance measure, such as PCI DSS or HIPAA.

But that's changing: After watching other well-known companies suffer embarrassing (and preventable) breaches that have affected millions of customers and damaged brand reputations, more organizations are beginning to understand the importance of proactively protecting their data.

The thought of insiders making mischief, particularly during the recent financial crisis, has many executives feeling nervous. They wonder what intellectual property and other sensitive data have slipped away with former employees because no one removed access rights or paid attention to whether employees had been collaborating via unsecure, online applications.

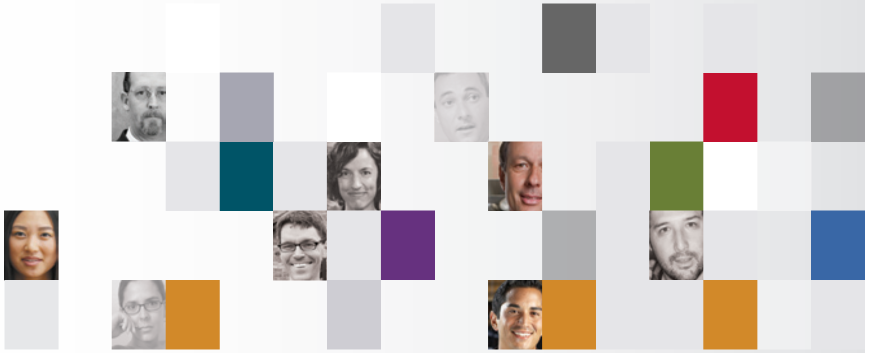
And what about mobile devices, like smartphones and laptops? Are employees using equipment supported or allowed by the enterprise strictly for business purposes? (The answer: probably not.) Add the cloud to this list and consider the fact that large portions of critical data are being sent outside of the organization—and out of its control.

As businesses make data loss prevention (DLP) a higher priority, they are quickly realizing how complicated the process can be, let alone making it a matter of policy. There's the challenge of data classification—figuring out what needs to be protected, as well as recognizing that securing data in the name of compliance is only the tip of the iceberg. Then the various "silos" in an organization must be convinced to coordinate and communicate for the sake of DLP—an often-frustrating exercise. Organizations must also determine who or what function will be responsible for managing DLP efforts, as well as what technology solutions are available for protecting data and helping to enforce policy.

Protecting sensitive information is a complicated undertaking. Effective DLP requires dedicated resources, the active involvement of many stakeholders in the organization, and the support of technology. But it is a necessary process, and in the long term, could save your organization from brand damage, loss of business, and legal and financial repercussions brought on by a security breach committed by just one insider or hacker.

Many executives are wondering what intellectual property and other sensitive data may have slipped away with former employees during the financial crisis.

2010: The Cybersecurity Landscape



If the past year's cybercrime activity is any indication of criminals' industriousness and earnestness, the cybersecurity landscape for 2010 should prove to be rough terrain for many users.

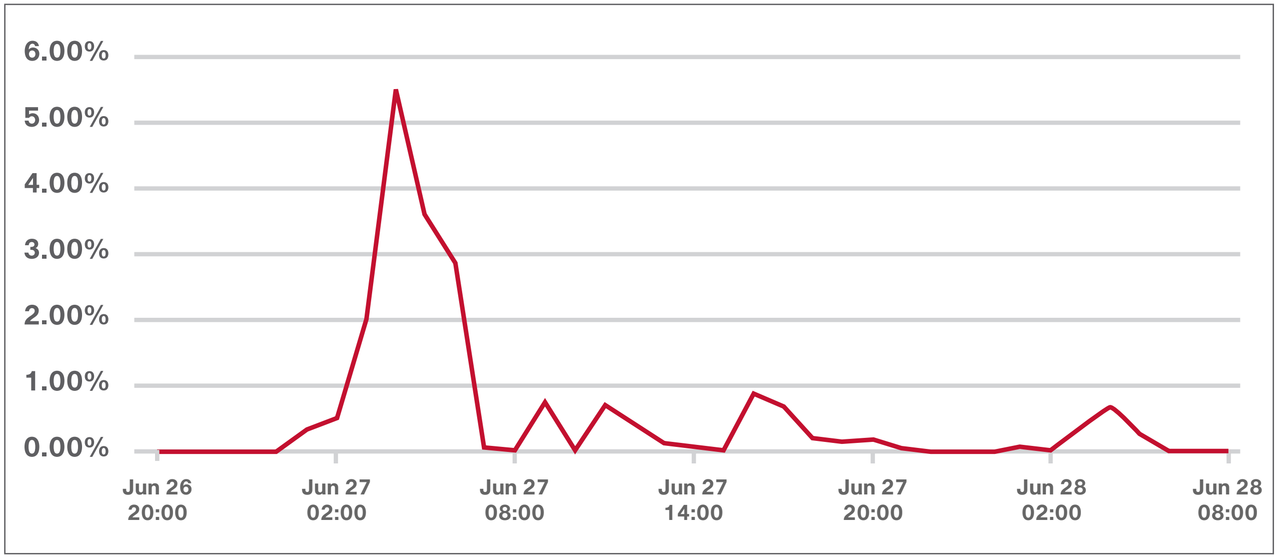
Although there has been good news to report in 2009, including a ramp-up in vulnerability patching by leading software vendors, unprecedented cooperation and collaboration by the security community and industry in response to the Conficker threat, and more arrests and prosecution of cybercriminals worldwide, the Internet is more dangerous for users than ever before.

In the *Cisco 2008 Annual Security Report*, it was predicted that during 2009, cybercriminals would only become more sophisticated in their exploits. They were expected to rely on smaller, more frequent, targeted attacks; more cross-protocol attacks; and reputation hijacking to take advantage of users' trust. This has all been true.

More than that, as the exploits described in this report reveal, the innovation and creativity of cybercriminals are limitless. For users, it is not easy to discern whether a website, an instant message, an email, a PDF, or other files or content are "safe" or a "threat." Even the most cautious and educated Internet user can be fooled. Consider that FBI director Robert Mueller fell prey to a phishing scheme in 2009, after responding to a legitimate-looking email purporting to be from his bank and requesting that he "verify" some of his personal information.

According to the Anti-Phishing Working Group, the number of fake anti-virus programs grew by 585 percent from January to June 2009. Banking Trojans, like Zeus and Clampi, increased by nearly 200 percent. And the number of phishing websites was hovering near 50,000, the most since 2007. Internet users should be prepared to encounter the same type of cybercriminal activity in 2010.

Michael Jackson Spam as a Percentage of Global Spam



Within hours of the first report of pop star Michael Jackson's death last June, a wave of email spam was unleashed worldwide in an effort to take advantage of both grieving fans and the curious.

Cybercriminals are continually refining their "craft" so they can move swiftly to seize their share of the next moneymaking opportunity. Manipulating search engine results is one example of where criminals are showing increasing "mastery" of skills. When a big news event—a devastating earthquake, a flu pandemic, a celebrity scandal—sends information-hungry users to the Internet in droves, cybercriminals are ready and waiting to serve up malware or lure users into handing over their cash for nonexistent goods or causes.

When pop star Michael Jackson passed away in June, for example, many of the highest-ranking search results related to his death on major search engines were actually malicious websites. Internet service actually slowed down on the day of Jackson's death because so many people were online searching for the same information at the same time—whether or not it was true that he had died, and how it happened.

Within hours of the first report of Jackson's untimely demise, a wave of email spam with subject lines such as "Confidential—Michael Jackson" was unleashed worldwide in an effort to take advantage of both grieving fans and the curious. Cisco researchers identified eight different botnet organizations using the Michael Jackson lure, including the Zeus Trojan.

There is no doubt cybercriminals will only continue to take advantage of these prime opportunities for social engineering campaigns. The law of averages works in the criminals' favor too. The Internet is vast and there are millions of users—and millions of webpages are added to the Internet every day. This means there are seemingly limitless opportunities for attackers to set their traps and collect the spoils.

Remote Working: Are You Ready for a Crisis?

The H1N1 flu epidemic has prompted management at many organizations to take a hard look at their business continuity plans. Specifically, what would happen if a major event, such as a pandemic or natural disaster, forced them to require all employees to work from home for an indefinite period? Many are discovering they don't support remote working to the extent that "business as usual" could be maintained in an emergency.

In a Cisco-commissioned survey of security decision-makers at more than 500 companies across the financial, retail, healthcare, government, and education sectors, less than 25 percent of respondents said they felt their current remote-access solutions enhance their pandemic or disaster preparedness.

Fifty-three percent of respondents said that less than half of their employees were set up to work remotely. Meanwhile, only 13 percent have 76 to 100 percent of employees enabled to work remotely. The top two reasons cited for not supporting a remote workforce: "Business requirements do not necessitate any or additional remote/mobile workers" and "budget constraints." The latter response is interesting, considering most respondents noted that a remote workforce creates positive benefits, such as increased productivity and enhanced efficiency.

Even though more than 40 percent of survey respondents said remote workforce security has increased in priority for their organization in the last 12 months, just 36 percent currently provide SSL or IPsec VPN capabilities to their remote workforce. Sixty percent intend to increase those capabilities in the year ahead, but primarily for reasons such as lowering administrative costs.

Among organizations that support remote working at this time, 63 percent issue company-owned laptops to their employees. Forty-six percent currently provide smartphones, and 36 percent plan to commit budget for these devices in 2010.

Social Networks: A Cybercrime Hotspot in 2010

In 2009, social networking sites became the new playground for cybercriminals. And how can they resist? The Nielsen Company reported in March 2009 that social networks and blogs are the fourth most popular online activity—and more than two-thirds of the global online population are participating in these "member communities."

The social networking trend shows no signs of slowing, especially as more businesses start using these sites, users join multiple communities based on their various interests, and more people worldwide gain Internet access. Thus, it is likely that social networks will be gaining the membership of many more cybercriminals in the year ahead.

However, at least in one case, it was positive for U.S. law enforcement that a criminal had a penchant for social networking. In September 2009, a burglar in Pennsylvania was arrested after police tracked him via Facebook. The thief, after stealing some jewelry, stopped to check his Facebook account on the victim's computer. But he forgot to log out—making it easy for police to find him.

Social Media: Political Tool, Newsmaker

An interesting twist for social media in 2009 that will carry into 2010 is how it has become a vital tool in the political process, and for informing the world about dramatic events as they unfold. Microblogging service Twitter and video-sharing service YouTube, for example, both played integral roles in organizing and broadcasting political uprisings and demonstrations throughout the globe this year. From Eastern Europe to the Middle East to Asia to the United States, major news events are being transmitted in real time by everyday people.

Some governments have responded by trying to block access to these services, ignoring the fact that to other parts of the world, they may appear as censors and oppressors—and that people will inevitably find ways to circumvent such restrictions. But it will become increasingly difficult for governments to suppress this form of communication among citizens even temporarily as the number of mobile phones, particularly those with Internet capabilities, continues to skyrocket. In 2009, developing countries accounted for 75 percent of the more than 4 billion mobile phones in use worldwide.[5]

Hello? Cybercrime is Calling

In 2009, several successful text message scams targeted the users of handheld mobile devices, such as cell phones and smartphones. Many users were contacted by scammers via SMS or phone and duped into revealing sensitive information, such as bank account numbers. The scams relied on social engineering tactics and often targeted just a specific group of users, usually by area code. As reported in the *Cisco 2009 Midyear Security Report*, individuals who bank with smaller financial institutions, such as local credit unions, have been favorite targets.

[5] "Mobile Marvels," *The Economist*, September 24, 2009.

Expect to see even more “smishing” scams (phishing attacks using SMS) in 2010. In addition, attackers will no doubt be looking to find and exploit vulnerabilities in smartphone operating systems—and even netbooks—as some leading companies, including Nokia and Apple, move to put smartphone operating systems on these devices. As handheld mobile devices act more like traditional computing platforms, it is likely that individuals will need to update the security of their mobile devices regularly, just as they do their traditional computers.

And as more individuals worldwide gain Internet access through mobile phones (because, in many parts of the world, it’s faster than waiting on the availability of broadband), expect cybercrime techniques that have gone out of fashion to re-emerge in many developing countries. Cybercriminals will have millions of inexperienced users to dupe with unsophisticated or well-worn scamming techniques that more savvy users grew wise to (or fell victim to) ages ago.

Voice over Internet Protocol (VoIP) network hacking and “vishing” (voice and phishing) scams are also becoming more popular with criminals, particularly because these methods can be difficult for authorities to trace. Hackers break into a VoIP network to eavesdrop, make “free” phone calls, spoof caller IDs, and engage in other exploits.

As for vishing, here’s just one example: A so-called “terrorist” calls a cell phone (often in another country) and threatens to do harm to the victim’s family if he or she doesn’t send money. The victim—understandably frightened—may believe the threat is legitimate since the caller has their phone number and appears to know who they are. Therefore, they agree to meet the scammer’s demands.

U.S. Toppled as #1 Spam Sender

Emerging countries face a growing challenge in fighting spam, and they must devote greater resources to halting the spread of the botnets that generate malicious or unproductive email. Meanwhile, spam- and botnet-fighting efforts in developed economies appear to be paying off, according to exclusive data from Cisco.

Spam data gathered from Cisco Security Intelligence Operations reveals that several of the world’s economic leaders, including the United States, the European Union, China, and Russia, all experienced a decline in spam volume between 2008 and 2009. However, most of the world’s developing economies, including Brazil, India, Korea, and Vietnam, show rising spam levels during the same time period. Brazil experienced the largest year-over-year increase of countries examined by Cisco researchers: Brazil’s spam output tripled between 2008 and 2009. In fact, the world’s emerging economies (as defined by membership in the G-20 developing nations group) are responsible for output of 55 percent of the world’s total global spam.

“It’s clear that Internet service providers in developed nations are making great strides in combating spam,” said Russell Smoak, director of technical support for Cisco. “That knowledge needs to be shared with their counterparts in emerging economies, so that these growing countries can avoid the problems associated with high levels of botnets and their related spam—including reduced productivity and increased threats of crime.”

Growing Spam Problem in Emerging Economies

Country	2009 Volume	2008 Volume	Volume Change
Brazil	7.7	2.7	192.6%
United States	6.6	8.3	-20.3%
India	3.6	1.6	130.4%
South Korea	3.1	1.7	81.2%
Turkey	2.6	3.8	-31.3%
Vietnam	2.5	0.5	367.7%
China	2.4	3.2	-24.3%
Poland	2.4	1.6	43.4%
Russia	2.3	3.7	-38.2%
Argentina	1.5	1.3	16.0%

Volume in trillions per year *Source: Cisco Security Intelligence Operations*

Several of the world’s economic leaders all experienced a decline in spam volume between 2008 and 2009; however, most of the world’s developing economies show rising spam levels.

Introducing the Cisco Global ARMS Race Index

There is a tremendous amount of information on cybercrime, yet organizations lack a measurement of the overall effect of cybercrime and how it changes over time. To address this need, Cisco has developed the Global ARMS Race Index.

Inspired, in part, by the Richter Scale to measure earthquake magnitude, the Cisco Global ARMS Race Index measures "Adversary Resource Market Share" (ARMS) and provides a way to track the overall level of compromised resources worldwide—the networks and machines currently under "adversarial control."

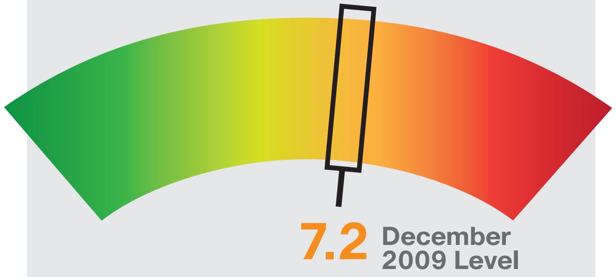
The goal is to gain a better understanding of overall trends based on the global online criminal community's activities, and on their rates of success at compromising both enterprise and individual users. Cisco will track the resources controlled by cybercriminals over time, using a similar methodology and data for comparison and trend analysis. The aggregate number that represents the level of compromised resources at the end of 2009 (7.2) is highlighted in the chart at right.

To arrive at this year's measurement on the 10-point index, Cisco relied on leading botnet-tracking estimates of total bots and other data points derived through internal research, third-party independent security research, and other expert sources. The methodology for the Global ARMS Race Index is based on:

- Current aggregate botnet size and infection-level estimates
- Statistics used to estimate the total number of Internet-connected systems in the world
- Estimates on home and work infection rates, which measure factors like resource availability (such as bandwidth, computing power, and other networked systems)

According to the data on the Cisco Global ARMS Race Index, as of December 2009, enterprise infections are common worldwide, and between 5 and 10 percent of consumers' computers are infected.

The Cisco Global ARMS Race Index



9.5+: More resources are under rogue control than legitimate control. Inability to trust any connection or application, all services readily deniable.

9-9.5: Nearly every network, every machine type, every user type, in all regions is infected at significant levels. Widespread resource abuse is common.

8: Enterprise networks are widely and continuously infected. Consumer systems are heavily infected, with traditional security programs proving ineffective. Large simultaneous attacks on many high-visibility targets are possible.

7: Enterprise networks are experiencing persistent infections. Consumer systems are infected at levels capable of producing consistent and alarming levels of service abuse.

6: Enterprise networks are infrequently infected. Consumer systems have significant infection levels and are capable of broad (but not sustained) high-level service abuse.

5: Enterprise networks are rarely infected. Consumer systems are experiencing annoying but not alarming infections; targeted service abuse is possible.

1-4: Enterprise networks are virtually not infected. Consumers have nominal levels of infection and barely noticeable abuse.

According to the Cisco Global ARMS Race Index, the level of resources under adversarial control worldwide was 7.2 at the end of 2009—meaning enterprise networks are experiencing persistent infections and consumer systems are infected at levels capable of producing consistent and alarming levels of service abuse.

User Education and Realistic Policies: Not for the Back Burner

Previous Cisco security reports have emphasized that "user education" is an essential component to security. Users should be expected to take measures to protect their online identity and to be aware of the risks that accompany their use of technology.

In the Web 2.0 world—where networks lack clear boundaries—organizations have little excuse for not formally educating their employees about what the enterprise considers to be "acceptable use" of social media, collaborative tools and applications, and mobile devices. Internal hosting of these types of applications, which more companies are doing, can also reduce risk.

Organizations need to embrace new technologies to stay competitive and retain their employees—particularly those from ultra-wired Generation Y. However, they must first take time to create enlightened security policies and to embrace a new breed of security tools that are capable of enforcing them. The good news is that these tools are emerging.

Reputation and Global Correlation: More Critical Than Ever

Since today's security threats are often launched via social media, they are tougher to block using traditional perimeter-based tactics. Criminals are often merely delivering the URL that links to malware or a scam website, not the malware itself. And since computer users have repeatedly shown their willingness to respond, a link in a social media message is all that is needed.

One defense against these threats is to incorporate real-time intelligence about the source of Internet traffic, instead of local inspection of network threats only.

To halt attacks that might otherwise evade anti-virus protection or URL filtering technologies, security professionals need a way to gauge the reputation of sources of traffic, and they must stop suspect traffic sources before they cause problems. In many cases, attacks are multipronged—for example, via email, the web, and the network. Therefore, the ability to view traffic across protocols and networks can improve an organization's ability to detect and block these attacks.

In the year ahead, expect more businesses to embrace the concept of the borderless enterprise as they look to increase workforce productivity while achieving greater cost savings.

The Borderless Enterprise: Anywhere, Anytime Architecture

With all of the recent advances in technology, from cloud computing to online collaborative work tools to handheld computing, there has been a significant acceleration of "borderlessness"—an absence or removal of boundaries in the way we work, interact, and share information.

The idea of the "borderless enterprise" that is now emerging is defined by Cisco as "the delivery of business capabilities on demand through an architecture of virtualized resources and services that optimally provides secure, context-aware, rich media information to mobile, seamless communities of employees, partners, and customers."

In the year ahead, expect to see more businesses embracing the concept of the borderless enterprise as they look to increase workforce productivity while achieving greater cost savings. They will embrace new approaches and emerging technologies, such as virtualization and data center optimization. With accelerating globalization trends and the proliferation of mobile devices with expanding capabilities, the shift toward cloud computing and outsourcing of business and IT services will only increase.

However, the borderless enterprise may not be the appropriate choice for every environment today—or even in the near future. Enterprise and government agencies, for example, are likely to continue to require architecture solutions and capabilities designed for the bordered enterprise.

Borderless Demands a New Approach

The rise of the borderless enterprise is a call to action for the security community, which must start thinking differently about how to approach security. The time has come to start disassociating the things a corporation cares most about, such as intellectual property, from the endpoint while compensating for the loss of control of the end device with greater control, depth, and visibility in the network and data center. It is also important to consider the possibilities of integrated forms of commoditized security services—many of which may live in the cloud.

Security Community: Maintaining a United Front

There is another call to action for the security community: working together, regularly, to make the Internet a safer place. One of the most positive developments of 2009 was when the security community and industry united to rally against the Conficker threat. The success of the Conficker Working Group (see the "Sign of Hope" category in the 2009 Cybercrime Showcase section on page 5) proved that multiple entities can put aside their own priorities in the interest of the greater good.

Several organizations recognize the importance of sharing information and best practices to improve Internet security. Carnegie Mellon University's Computer Emergency Response Team (CERT: www.cert.org); the Forum of Incident Response and Security Teams (FIRST: www.first.org); and the Industry Consortium for the Advancement of Security on the Internet (ICASI: www.icasi.org) are just some examples. But will we have to wait for another major security threat like Conficker to emerge for the security community and industry to cooperate closely? Hopefully not, as undermining the efforts of cybercriminals is an ongoing responsibility for the entire security community.

With the Obama administration emphasizing innovation as the key to enhancing U.S. cybersecurity—and countries worldwide taking important steps toward protecting their interests and their citizens from cybercrime—it is clear that collaboration among government, private industry, and the security industry will be expected, and essential, in the effort to improve global cybersecurity in 2010 and beyond.

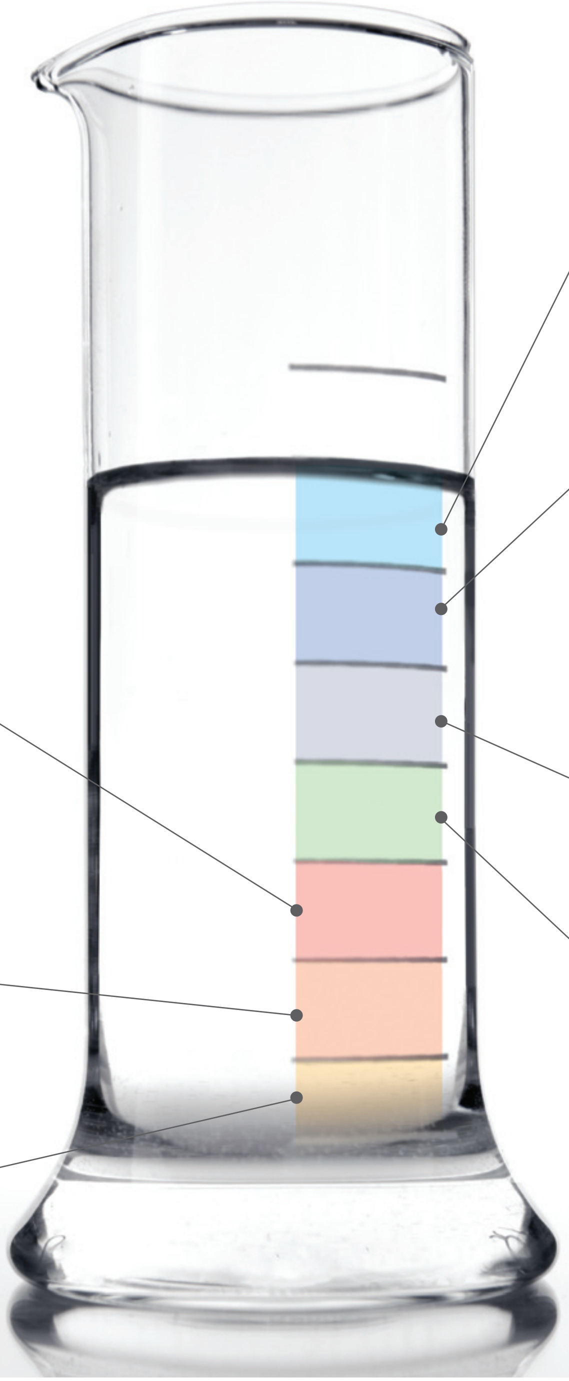
A Recipe for Trouble: The Security "Nightmare Formula"

Minor vulnerabilities, poor user behavior, and outdated security software—they all add up to a big headache for IT and security professionals. Small errors on the part of computer users or their IT departments may not wreak havoc on their own, but in combination, they dramatically increase security challenges. Here's a recipe for the "nightmare formula" that organizations need to avoid or mitigate.

Easy-to-guess passwords and password reuse: Obvious strings of numbers (like "123456"), mothers' maiden names, or simply using the word "password" as a password make it easier for criminals to break into accounts and to reset passwords. Even more problematic is the reuse of the same or similar passwords, or the same answers to password recovery questions, from site to site. (See page 14 for more on password security.)

Inconsistent patching: Conficker, the big botnet of 2009, gained traction because computer users failed to download a patch that was readily available from Microsoft. Although most of today's attacks are launched via social media networks, criminals still look for ways to exploit these old-style vulnerabilities.

Getting too personal: By disclosing information, such as birth dates and hometowns, social media users make it far too easy for criminals to break into private accounts and gain control by resetting passwords. Corporate users are not immune to this trend, frequently using Twitter to discuss business projects.



Overdose of trust: Social media users are placing too much trust in the safety and privacy of their networks, responding to messages, supposedly from their connections, with malware-laden links. (See page 6 for more about social media.)

Outdated virus protection: Computer users fail to update their anti-virus software or let subscriptions lapse, leaving their systems more vulnerable to attacks that might normally be easy to block. Worse, they may be running fake anti-virus software (see "Fake Anti-Virus Scams" on page 12). In addition, individual users may fail to enable easily available security features built into their operating systems or web browsers, such as firewalls. Ensuring virus software is updated provides some protection, but as noted on page 23, criminals are now hiring services to test their malware and ensure that it is not flagged by anti-virus programs.

Not using available security products: Users often assume anti-virus is all they need to be "safe." Thus, they don't take advantage of simple, tried-and-true security measures, such as personal firewalls and browser security features, which can provide an extra layer of protection.

"It won't happen to me" syndrome: This is perhaps the most potent ingredient in the Nightmare Formula. Users intentionally violate policies and knowingly engage in risky behavior online because they believe they won't be the victim of a cyber attack or compromise their employer's cybersecurity.

Cisco Security Intelligence Operations

Cisco's vision for security is enabling customers to collaborate with confidence. To do so, Cisco champions a holistic, proactive, layered approach to counter existing and emerging security threats.

Cisco Security Intelligence Operations (SIO) is an advanced security infrastructure that enables the highest level of security and threat detection and prevention for Cisco customers. With a team of global research engineers, sophisticated security intelligence, and automated update systems, Cisco SIO allows customers to embrace new technologies—securely—so they can collaborate with confidence.

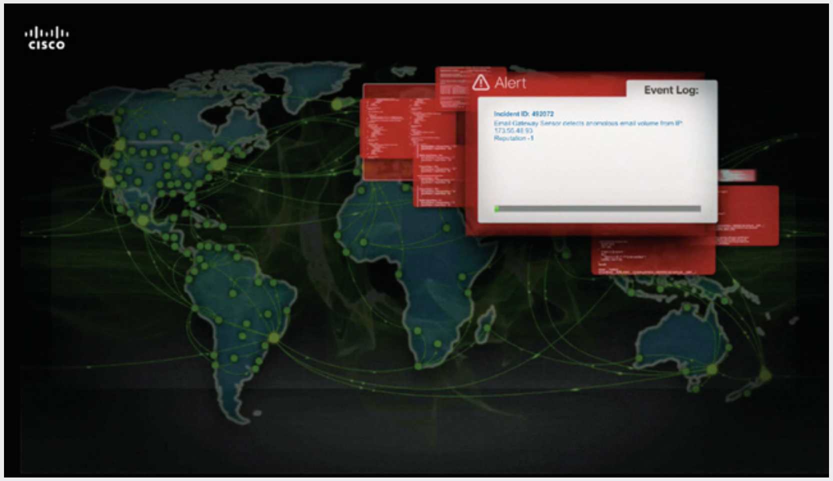
Point defenses to meet individual security threats or protect individual products are not enough in an environment where blended, cross-protocol, and cross-vendor vulnerability threats are increasingly the norm. Instead, integrated security management, real-time reputation assessment, and a layered, multipoint approach are required: a sophisticated security ecosystem that provides a global view across various potential attack vectors.

Cisco SIO relies on tightly integrated data derived from multiple Cisco divisions and devices to continuously assess and correlate Internet threats and vulnerabilities. As threats continue to evolve, Cisco SIO will enhance Cisco's ability to identify global threat activities and trends, and provide expert analysis and services to help protect users from these threats.

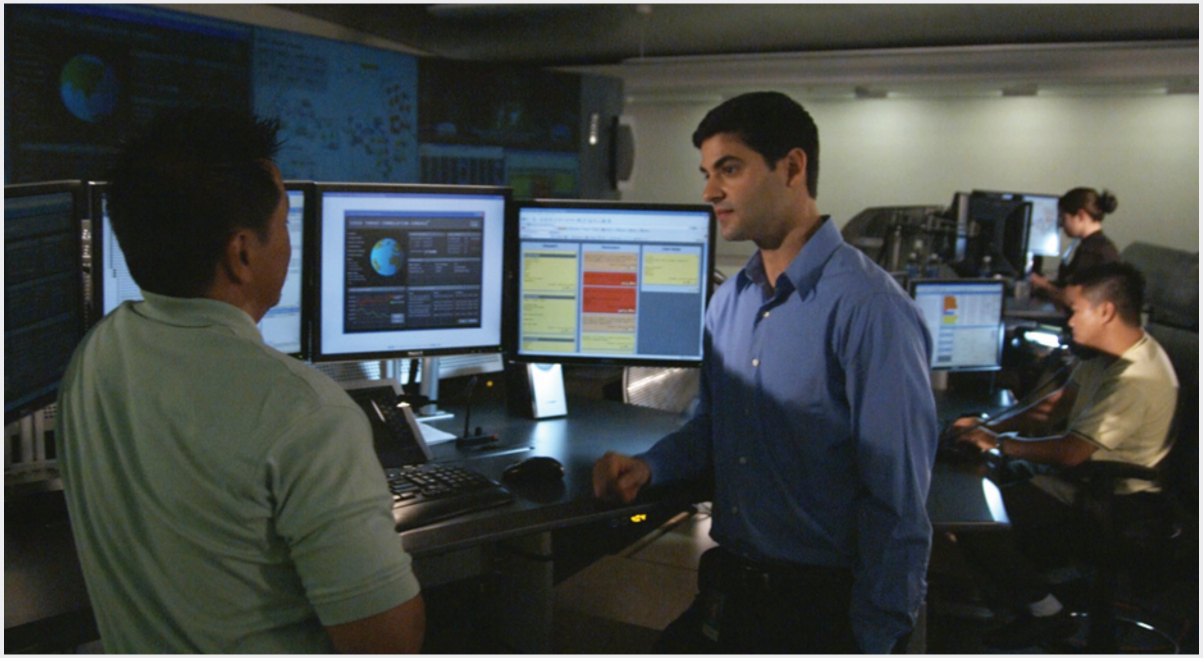
Cisco is committed to providing complete security solutions that are integrated, timely, comprehensive, and effective—enabling holistic security for organizations worldwide. With Cisco, organizations can save time researching threats and vulnerabilities, and focus more on taking a proactive approach to security.

For a look inside Cisco IT, visit the "Cisco on Cisco" blog: http://blogs.cisco.com/ciscoit/comments/welcome_to_the_cisco_on_cisco_blog/.

The Cisco SIO iPhone application is free and available now at the Apple iTunes Store: http://itunes.apple.com/us/app/cisco-sio-to-go/id338613740?mt=8.


Alert
Event Log:
Incident ID: #52072
Email Gateway Sensor detects anomalous email volume from IP:
173.55.48.93
Reputation -1

Cisco Security Intelligence Operations provides the highest level of threat correlation—enabling users to collaborate with confidence. With a sophisticated security ecosystem that provides a global view of potential attack vectors, organizations can save time researching threats and vulnerabilities, and focus more on taking a proactive approach to security.



All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

For More Information

Cisco Security Intelligence Operations
www.cisco.com/security

Cisco Security Blog
blogs.cisco.com/security

SenderBase
www.senderbase.org

Cisco Security Solutions
www.cisco.com/go/securitysolutions
www.cisco.com/go/ros

Cisco Security Products
www.cisco.com/go/security
www.cisco.com/go/intellishield
www.cisco.com/go/ips
www.ironport.com

Report available for download at
www.cisco.com/go/securityreport

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**.