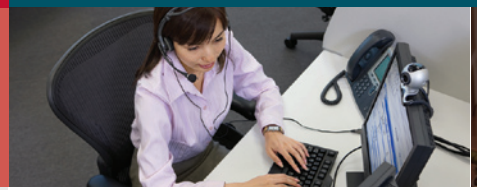
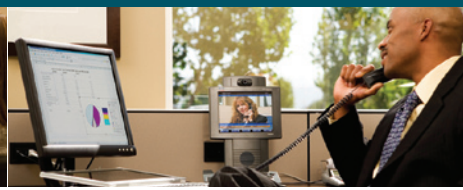
Cisco 2009 Midyear Security Report





An update on global security threats and trends

CISCO

Introduction

The Cisco® Midyear Security Report presents an overview of Cisco security intelligence, highlighting threat information and trends from the first half of 2009. The report also includes recommendations from Cisco security experts and predictions of how identified trends will evolve.

As the global economy struggles to regain its footing, one moneymaking sector remains healthy—online crime. This sector embraces technical innovation, collaborates with like-minded enterprises to develop new strategies for generating income, and continues to demonstrate adoption of the best legitimate business strategies to maximize profits.

Criminal sophistication and business acumen have increased since the publication of the *Cisco 2008 Annual Security Report*. For instance, criminal enterprises are innovating new business models with the creators of botnets—networks of compromised computers that can carry out the bidding of online scammers. These innovations include "botnets as a service," a sobering spin on the software-as-a-service trend that has spread across the technology sector.

"We see many signs that criminals are mimicking the practices embraced by successful, legitimate businesses to reap revenue and grow their enterprises," said Tom Gillis, Vice President and General Manager of Cisco Security Products. "It seems the best practices espoused by *Fortune* magazine and Harvard Business School have found their way into the online underworld."

Cause for Concern: Technical Innovation of Online Criminals

The technical innovation and capabilities of online criminals are remarkable. The Conficker worm, which began infecting computer systems in late 2008 and early 2009 (and is still infecting thousands of new systems daily), provides the best example. Several million computer systems have been under Conficker's control at some time as of June 2009, which means the worm appears to have created the largest botnet to date. (Read more about Conficker on page 4.)

Security industry watchers also point to the methods used by Conficker to propagate and create the botnet. Instead of using newer approaches that involve social engineering, or delivering the payload via email or the Internet, Conficker's creators exploited a vulnerability in the Windows operating system. This was an "old-school" method that may not have seemed threatening, given the preponderance of new tactics for online scams. Conficker's creators appear to have recognized that their entry point into computer systems might yield more satisfying results.

It's safe to say online attacks will continue to showcase the most cutting-edge technology—and criminals will try to use older tactics in new ways. Criminals are also closely watching security researchers and learning from their methods for thwarting attacks, putting the "good guy" knowledge to use so their next attack can evade existing protections.

Cause for Concern: Criminal Sophistication and Collaboration

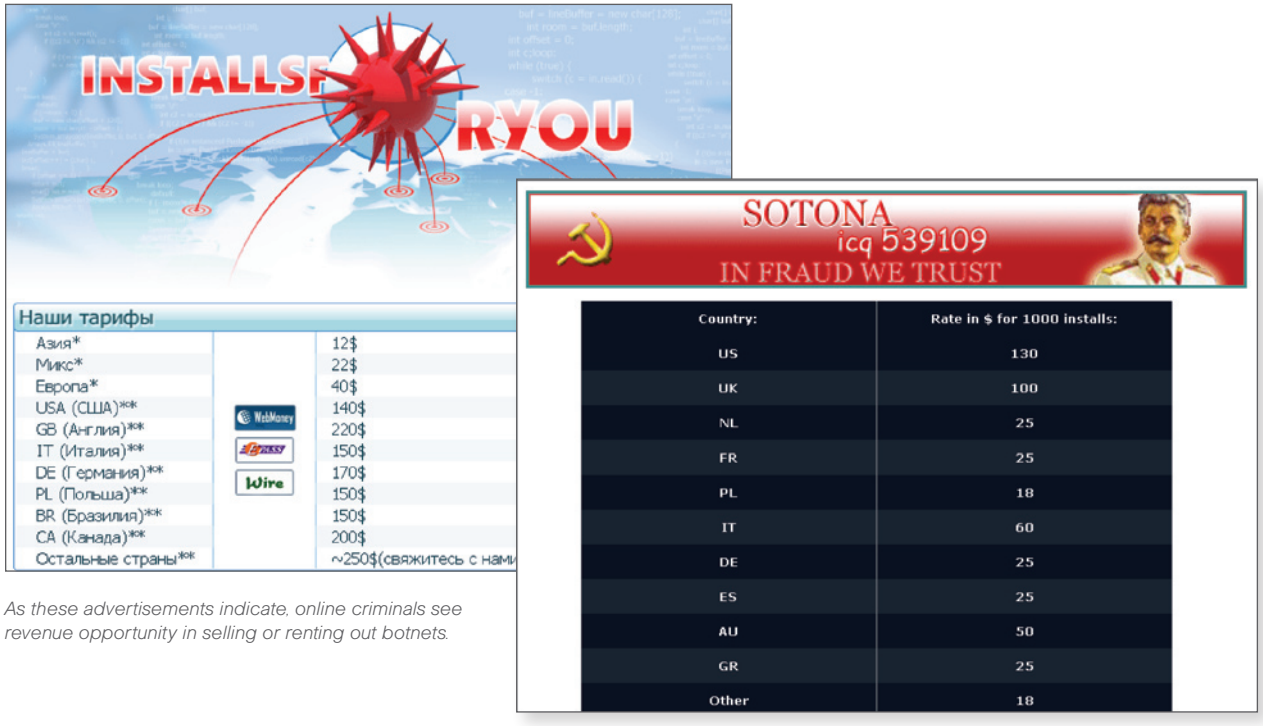
"Bad guys" are aggressively collaborating, selling each other their wares, and developing expertise in specific tactics and technologies. Specialization makes it tougher to shut down illegal activity, because there are many players in this ecosystem.

Consider the collaboration between the creators of two large botnets, Conficker and Waledac (see page 10). In April, the Conficker botnet monetized itself by delivering the Waledac malware via Conficker's own hosts, along with scareware—scam software sold to consumers based on their (often unnecessary) fear of a potential threat—to generate revenue from victims. In other words, Conficker served as a large-scale distributor for Waledac's wares.

The Conficker-Waledac collaboration is an example of the networked and persistent threats that will likely become more prevalent. The threats are networked because they involve at least two enterprises collaborating with each other for illegal purposes, and they are persistent because the same attacks are launched from the same hosts over a long period of time—which means they can inflict greater damage.

Cisco security experts expect to see cyber criminals engaging in similar joint ventures in the coming months. In fact, they have located online advertisements that offer other criminals the ability to access existing botnets. In a recent online conversation with a botmaster, Cisco researchers learned that botnets can be sold off at a given price per "node" or infected system. As botnet creators become more capable of operating in stealth mode for longer periods of time, they will be able to earn more money before the botnets are detected and dismantled.

Depending on situation and opportunity, those who engage in online attacks have also been known to both collaborate with, and target, each other. One security researcher discovered that a major botmaster used an online forum to ask other criminals for help after his own botnet was hacked.



As these advertisements indicate, online criminals see revenue opportunity in selling or renting out botnets.

Cause for Optimism: Organizations Collaborate to Shut Down Online Threats

As online criminals constantly adapt and refine their techniques for reaping illegal revenue, security professionals and individual computer users must become even more sophisticated in their own approaches to combating security threats. There are encouraging signs that aggressive "good guy" collaboration can succeed.

The Conficker Working Group is an excellent example. The group was founded in early 2009 as the Conficker botnet continued to spread, and now boasts more than 100 security organizations (including Cisco) as members. The group's website (www.confickerworkinggroup.org) publicizes news about recent Conficker infections, the latest patches to block the Conficker worm, and tests to check for infection. The collaborative efforts of Conficker members helped disrupt most of the worm's activities earlier this year (see page 5).

Another positive example is the crippling of the Srizbi/Reactor Mailer botnet (see page 9). One Internet hosting company, McColo, hosted the Reactor Mailer command and control infrastructure that controlled Srizbi/Reactor Mailer. After an aggressive campaign documenting McColo's activities, the company's upstream Internet providers terminated McColo's service. Once McColo was shut down, worldwide spam volumes plummeted.

However, Srizbi/Reactor Mailer was able to shift its operations to a hosting company based in Estonia, and spam volumes originating from the botnet rose until Microsoft's Malicious Software Removal Tool (MSRT) disabled the majority of the bots. The availability of the MRST demonstrates how coordinated action can thwart such attacks for prolonged time frames.

In addition, there has been a greater focus from both government and international law enforcement on combating cybercrime and improving cybersecurity. Increased cooperation of law enforcement in the tracking, arresting, and extraditing of cyber criminals is anticipated —and 2009 has already seen some high-profile arrests (see "Prolific Scammers Caught and Indicted," page 5). Increased compliance requirements and improved vendor response are also expected.

Following a formal "60-Day Review" of cybersecurity in the United States, President Barack Obama announced that he will appoint a "cybersecurity coordinator" to oversee "a new comprehensive approach to securing America's digital infrastructure."[1] The Obama administration is expected to keep the spotlight on making improvements and embracing innovative thinking in both U.S. cybersecurity and technology policy.

According to the *Cyberspace Policy Review* report released by the White House in May 2009, the United States looks to "harness the full benefits of innovation to address cybersecurity concerns . . . [and] develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks." The report also notes that the country "faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights."

The United States is not alone in its desire to improve cybersecurity and prevent cyber criminals from achieving success. Because these are issues of global concern, it is no surprise that other countries are also increasing their efforts to address them.

For instance, the United Kingdom is currently conducting its own cybersecurity review. Results are expected to be published this summer along with an updated version of the country's National Security Strategy. It is anticipated that the United Kingdom will also create a cybersecurity coordinator-type post in its government. Meanwhile, Finland recently announced that it will establish, and activate by early 2011, a round-the-clock "cyberwar unit" responsible for protecting the country's data communications from both civilian and military cyber attacks.

> "We see many signs that criminals are mimicking the practices embraced by successful, legitimate businesses to reap revenue and grow their enterprises."
>
> TOM GILLIS,
> Vice President and General Manager,
> Cisco Security Products

[1] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, transcript released by The White House, Office of the Press Secretary, www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

Online Security Risks and Trends

Malware: Conficker Combines Old and New Threats

The piece of malicious software that may have caused the most chaos in the first half of 2009 used an older method of attack that should have been easy to detect and avoid. Yet when the Conficker worm (also known as Downadup) began exploiting vulnerable devices in the last quarter of 2008, and continued to propagate through early 2009, it quickly spread to millions of computer systems, infecting tens of thousands of new machines daily. Experts agree that Conficker appears to be the largest worm infection since the SQL Slammer attack of 2003. Given that the Conficker worm was detected by security experts in October 2008, and that patches for the exploited vulnerability had been available since that time, this threat should have been easy to mitigate.

The Conficker worm actually has several variants, although Conficker.C (which includes .A and .B variants that downloaded the .C update) has been most successful at infecting large numbers of hosts. The worm infects computers by exploiting a vulnerability in the Microsoft Windows operating system (MS08-067/CVE-2008-4250). When executed, Conficker disables various Windows services such as Automatic Update and Security Center. It also blocks access to websites that would allow users to remove the infection. It then receives instructions through various communications channels, directing it to propagate, gather personal information, and download and install more malware onto victims' computers.

Given the amount of Windows vulnerabilities that require attention, this particular flaw may have been overlooked by IT professionals and individual computer users. In recent years, security has focused primarily on the web and email, and administrators may have neglected to install appropriate patches that would block Conficker's spread. About 150 countries have detected outbreaks of Conficker, with Brazil, China, and Russia showing the highest numbers of infected computer systems.

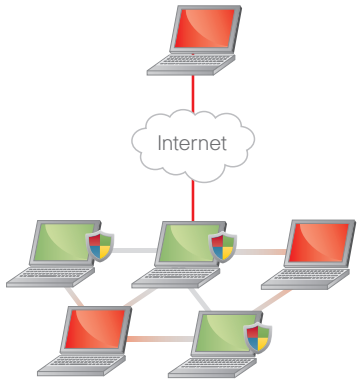
Although there may have been a dearth of attention focused on Conficker at the beginning stages of the infection, the spotlight grew as it became clear the worm's purpose was to build a massive botnet, perhaps the biggest ever. And when researchers realized that on April 1, 2009, the growing botnet would transition to a new method of communicating, media attention grew markedly. That, more than anything else, helped raise awareness of the Conficker problem, and spurred computer users to download the necessary patches. The Conficker botnet remains active, but rates of infection have slowed; as of early June 2009, it's estimated that about 3 million computers are still infected.

As April 1, 2009 (April Fool's Day in the United States) approached, security researchers were able to "dissect" the worm and piece together its plan of attack. On or about April 1, Conficker would begin generating thousands of Internet domain names and attempt to instruct some of them to download updated software. Although the botnet began generating 50,000 domain names per day compared to 500 before the April update, this method of communication was never actually put into place; one of the Conficker variants, an add-on module to Conficker.C, implemented peer-to-peer functionality instead.

The endgame for this activity appears to be the monetization of the botnet. In mid-April, the Conficker botnet was part of an outbreak of spam offering a free trial of software that would allow individuals to read supposedly private SMS messages. The malicious payload delivered via the fake SMS software was the Waledac botnet worm, which Conficker temporarily installed on infected hosts. It appears the creators of Conficker had allowed Waledac and some spyware to transport themselves via the large and well-established Conficker botnet. (Read more about Waledac on page 10.)

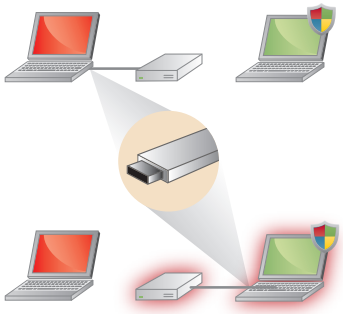
Conficker: A Malware Triple Threat

Network–Based Infection



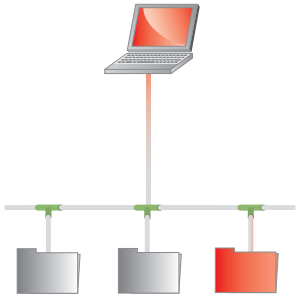
Conficker initially spread by exploiting the MS08-067/CVE-2008-4250 vulnerability. Any unpatched systems with ports 139 or 445 available were vulnerable.

Removable Storage–Based Infection



An infected computer can spread the infection, even to patched systems, if a removable storage device (for example, a USB drive) is shared between them.

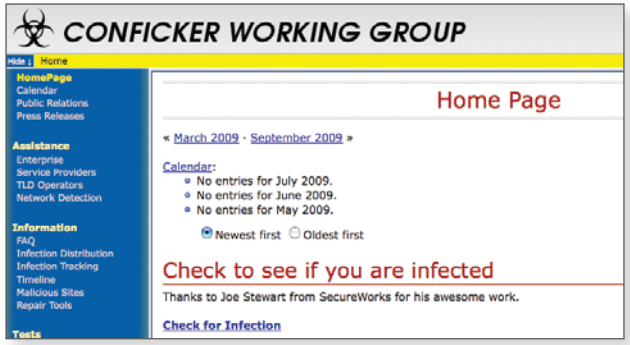
Network Share–Based Infection



Conficker-infected hosts attempt to log into network shares. If successful, any other computers connecting to those network shares will become infected — even if they are already patched.

The rapid propagation of Conficker emphasizes the need for risk and threat management that intelligently determines that attacks can be sourced from anywhere in a network. Even an "old-school" vulnerability may be deployed by criminals—especially if they think corporate security experts and individual computer users are paying minimal attention to these types of threats.

A key takeaway from the Conficker experience is the value of collaboration in fighting back. The Conficker Working Group, composed of more than 100 organizations involved in technology and security (including Cisco), was formed in February 2009. ICANN, the organization that coordinates the Internet's naming systems and a member of the Conficker Working Group, was able to compile a list of the domain names Conficker was attempting to contact,



The Conficker Working Group website includes Conficker removal tools as well as a simple test to determine if a computer is infected.

Prolific Spammers Caught and Indicted

Thanks to collaborative efforts among legal authorities, security researchers, and other institutions, cyber criminals are being identified and prosecuted—and going to jail. In mid-2009, two brothers (Amir Ahmad Shah and Osmaan Ahmad Shah) were indicted by a U.S. federal grand jury for illegally harvesting students' email addresses, and bombarding them with spam messages offering everything from iPods to teeth-whitening services.

The brothers—one a current student at the University of Missouri, one a former student—used the spam to falsely portray themselves as representatives of the university. At the height of their operation in 2003, they were generating and delivering 1 million spam messages every hour to students at nearly 100 educational institutions across the United States.

Using information from the various affected schools, including the University of Missouri, Cisco researchers were able to chart the increases in spam traffic generated by the Shah brothers. The The Cisco SensorBase network, which collects live threat data from over 700,000 globally deployed security devices, provided researchers with a high-level view into the damage this spam was causing to computer networks. The data was shared with U.S. district attorneys, and eventually played a key role in building the government's successful case against the Shahs.

thanks to data provided by security researchers tracking the worm. ICANN then passed this information to top-level domain operators, who could then block these domains. This coordinated effort went a long way toward blunting the impact of the worm.

When Conficker's creators realized the botnet's communications methods had been detected by security researchers, the scammers quickly shifted to a different approach. As criminals seek ways to monetize their activities and work to protect these revenue streams, they will fight back to prevent any tampering with their underground economy.

"Spamdexing": SEO for Online Criminals

As the media reported on the mayhem caused by Conficker, worried computer users took to Google and other search engines to locate patches to block the worm. Unfortunately, some of the most prominent first-page results—which users assumed to be trustworthy, since they were indexed ahead of all other results—were actually for sites hosting fake security software, and often, malware.

When prominent news events drive computer users to search engines—for instance, NCAA basketball tournaments in the United States, major holidays, or threats like Conficker—online criminals employ a technique called search engine poisoning, or "spamdexing," to push their fake websites to the top of search page results. Spamdexing involves overloading a webpage with relevant search terms or keywords so search engines will interpret the sites as good matches for the computer user's query—raising the ranking for the suspect pages.

Spamdexing isn't used solely by online criminals. Although search engine companies disapprove of the tactic, and supposedly employ methods to minimize the impact of spamdexing, many legitimate companies use this strategy to boost their own search rankings. And as discussed elsewhere in this report (see page 10), criminals have been quick to co-opt any practices deemed successful in the legitimate business world. In fact, they can use free online tools like Google Trends to discover the most popular search terms at any given time—and create malware-carrying fake websites accordingly.

User education in the form of security awareness training helps mitigate the threats posed by spamdexing, but enterprises can't assume employees will always make the correct choice about which websites to trust. For more thorough protection, businesses need security solutions that combine traditional URL filtering, reputation filtering, malware filtering, and data security.

Financial Information Targeted by DNS Poisoning

Domain Name System (DNS) cache poisoning has been a threat to online security for quite some time, but recent attacks indicate that criminals continue to use this method to obtain financial information—a key moneymaker for scammers. In April 2009, security researchers recorded what appears to be the first documented DNS cache poisoning attack on a financial institution—in this case, Brazil's Banco Bradesco. As with typical DNS-related attacks, the criminals redirected visitors from the bank's website to their own website, and offered up a fake login screen, presumably to steal login credentials.

There was hope in the security industry that DNS cache poisoning would become less prevalent once word got out about the Kaminsky DNS vulnerability (named after the security researcher who spotted a dangerous flaw in the Internet's DNS). Although exposure of this vulnerability led to development of effective patches, many DNS servers still remain unpatched.

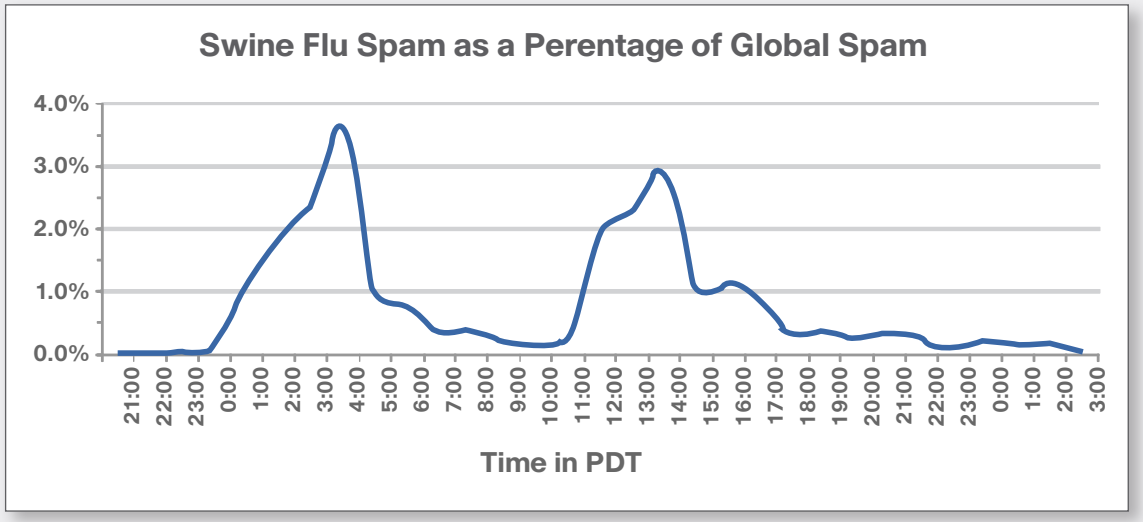
Dynamic, real-time web reputation technology is the answer to the ongoing threat of DNS cache poisoning. By assessing the trustworthiness of all URLs that comprise a webpage—not simply using a URL blacklist or whitelist—attacks can be quickly detected and blocked.

User education in the form of security awareness training helps mitigate threats. But enterprises can't assume employees will always make the correct choice about which websites to trust.

Recent Social Engineering Spam Campaign: Swine Flu

The worldwide outbreak of H1N1 influenza (commonly referred to as "swine flu") that began in April 2009 quickly led to an outbreak of another kind—a barrage of spam emails using swine flu as the bait. In late April 2009, cyber criminals started sending spam messages with subject lines such as "US swine flu fears" and "Swine flu in Hollywood." Recipients who clicked through were rewarded with messages urging them to buy nonexistent swine flu preventive drugs, along with a link to various websites known to sell fake pharmaceutical products.

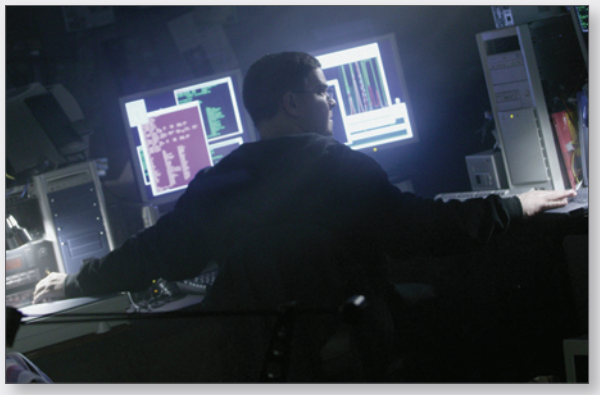
At the peak of the outbreak, swine flu-related spam messages comprised nearly 4 percent of global spam traffic. However, enterprise computer users with robust anti-spam solutions and web reputation filters probably saw very few of the messages because they were quickly blocked. Alert IT departments and computer users should assume that every time a major story like the swine flu outbreak hits the news media, spammers will seize the chance to launch an attack using these social engineering techniques.



As swine flu dominated global news stories, cyber criminals took advantage of its popularity to send more spam. Given the perfect storm of high popularity and low prior knowledge, people turned to the Internet to learn more about H1N1 influenza. Cyber criminals seized the opportunity by sending billions of spam messages—accounting for up to 4 percent of global spam at its peak.

Conversations with a Botmaster

Why does someone go into the business of creating and running a botnet? Not for the glory, discovered Cisco researchers who ended up chatting with a botmaster—but for the money. The botmaster who offered up an insider's look at the world of running botnets pegged a typical botmaster's income at US$5,000 to US$10,000 a week. And today, this income potential only demands a minimal level of technical knowledge, along with a savvy sense of how to con computer users into falling for the right lure.



The online conversation with this particular botmaster took place after Cisco researchers detected and removed a botnet infection. The researchers had noticed a high level of Internet Relay Chat (IRC) traffic over the network on nonstandard ports—usually a good indicator of malicious activity.

One of the researchers, pretending to be a fellow botmaster, posted a polite opening query via IRC. When the botmaster responded, the researcher asked what the botnet would be used for. The botmaster replied that he planned to gain control of several thousand machines, and sell them off to online criminals for their own schemes for 10 to 25 cents per node, or bot. The botmaster said he had recently sold 10,000 infected machines for US$800.

The researcher asked the botmaster how he gained control of so many machines, expecting him to say he'd exploited a known vulnerability using a worm like Conficker (see page 4). But the answer was surprising: The botmaster had sent out thousands of pieces of spam via instant messaging applications, with messages along the lines of "Check out this cool software," and a link to the botnet malware. Even if only 1 percent of the recipients were careless enough to follow on the link, the botmaster gained control of enough machines to make the effort worthwhile.

The researcher then asked the botmaster why he sells bots instead of using them for spam or phishing networks. The botmaster replied that selling bots wasn't usually his goal, since earnings were modest. In this instance, he had sold off 10,000 machines because he needed money for antibiotics for his sick child—but the real money, he said, came from using the bots for phishing attacks, in which personal information, such as banking passwords, is stolen. When the researcher asked how much money could actually be made from phishing activities, the botmaster was evasive about his own income, but said "a guy he knew" was able to earn US$5,000 to US$10,000 a week solely through phishing activities.

Why did the botmaster—someone obviously skilled with technology—choose this type of work instead of seeking a legitimate IT position? The botmaster said that a criminal record and lack of a "decent education" prevented him from obtaining an above-board job. In this faltering economy, one has to wonder if even well-educated IT experts with no criminal record will resort to illegal activities, since jobs are so scarce.

The Cisco researchers were also struck by the fact that neither the botnet nor the method of attracting victims (instant-messaging applications) were overly complex. It is not necessary to understand code, nor is there a need to understand networking.

Given the fact that anyone with a moderate understanding of the technology can bring a botnet to life, the implications for enterprise security are sobering," said Jeff Shipley, Security Research and Operations Manager at Cisco. "Patching to prevent threats against known vulnerabilities is key, but security awareness training about safe online behavior is even more important."

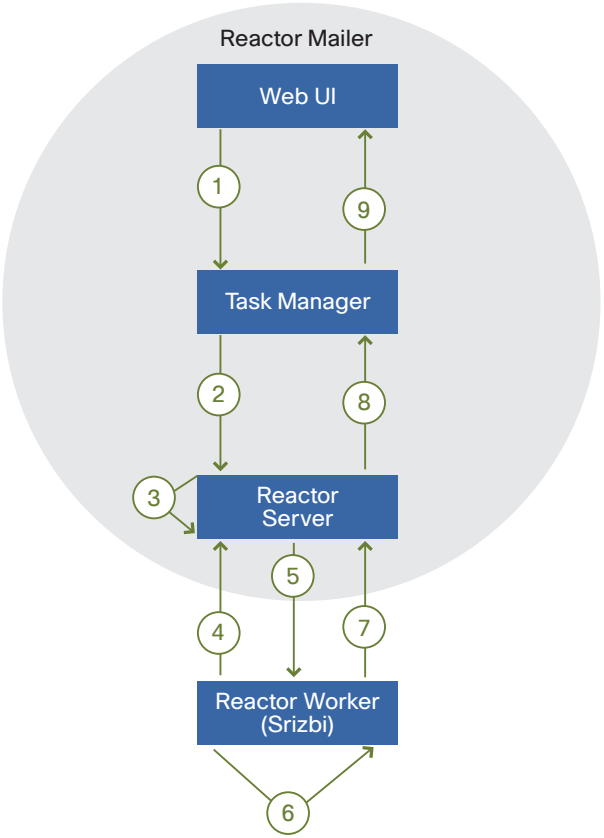
Read the full-length "Infiltrating a Botnet" Cisco report at www.cisco.com/web/about/security/intelligence/bots.html.

Botnets: The Rise—and Fall—of Srizbi/Reactor Mailer

In 2008, one of the biggest stories from the botnet world was Storm, which used innovative social engineering techniques to spread infection. As Storm's power waned, thanks to higher awareness and more effective threat-removal tools, the Srizbi/Reactor Mailer botnet took center stage, and, at its peak, dwarfed Storm in both size and output. By mid-2008, the Srizbi botnet had a stable population of 260,000 host computers and was responsible for the distribution of as much as 60 percent of the world's spam (a staggering 80 billion messages per day). Because it did not draw as much attention as Storm, Srizbi/Reactor Mailer operated unchecked for a longer period of time.

How did Srizbi achieve such success? Although it was initially distributed via "drive-by" downloads, Srizbi later used social engineering tactics to lure spam recipients into clicking through and downloading the malicious software. For instance, emails claimed the sender had a video file "where you look stupid." The unwitting recipient downloaded an executable file that turned the computer into a bot, or node, on the botnet.

This was standard operating procedure for botnet creators, but Srizbi/Reactor Mailer also had a secret weapon: a purpose-built "spam engine" that dramatically accelerated delivery of email messages generated by the individual nodes in the Srizbi botnets. Srizbi/Reactor Mailer was created by a spammer and sold to botnets using a software-as-a-service model—a good example of how online criminals are adopting best practices in business and technology to monetize their activity.



1 Create Task
2 Run Task
3 Create Atoms
4 Request Atom
5 Deliver Atom
6 Transmit 1000 Messages
7 Report Completed Atom
8 Aggregate Results
9 Report Results

The Srizbi/Reactor Mailer botnet was created as software-as-a-service—whereby spammers can create and deliver spam messages (tasks and atoms) through the botnet for a fee.

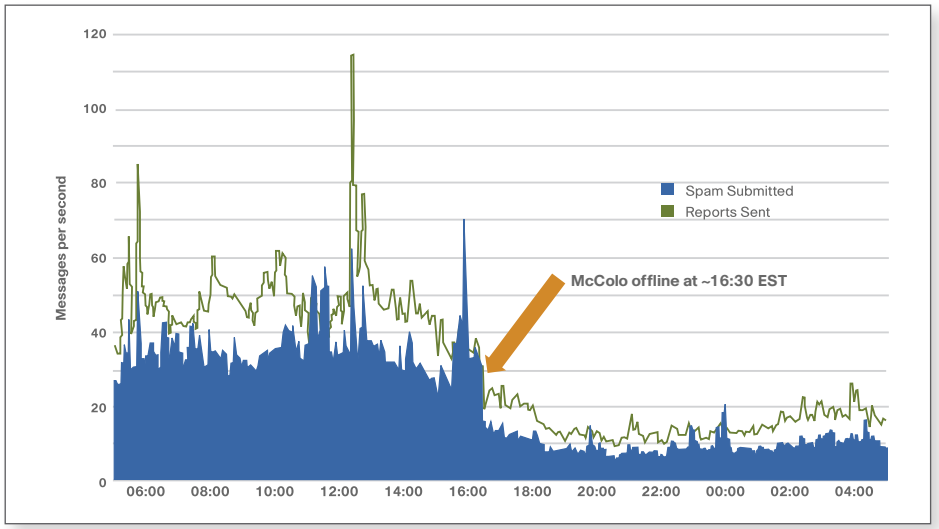
Srizbi/Reactor Mailer proved highly efficient at distributing spam because it eliminated a common bottleneck—that is, the transmission of spam, byte by byte, through a single data center. Srizbi/Reactor Mailer separated spam tasks into individual work units (called "atoms"), each with their own message templates, data files, and email lists. The atoms would then report back to the Reactor server when the work was completed. This process, combined with a large number of infected hosts, allowed Srizbi to deliver an unprecedented level of spam.

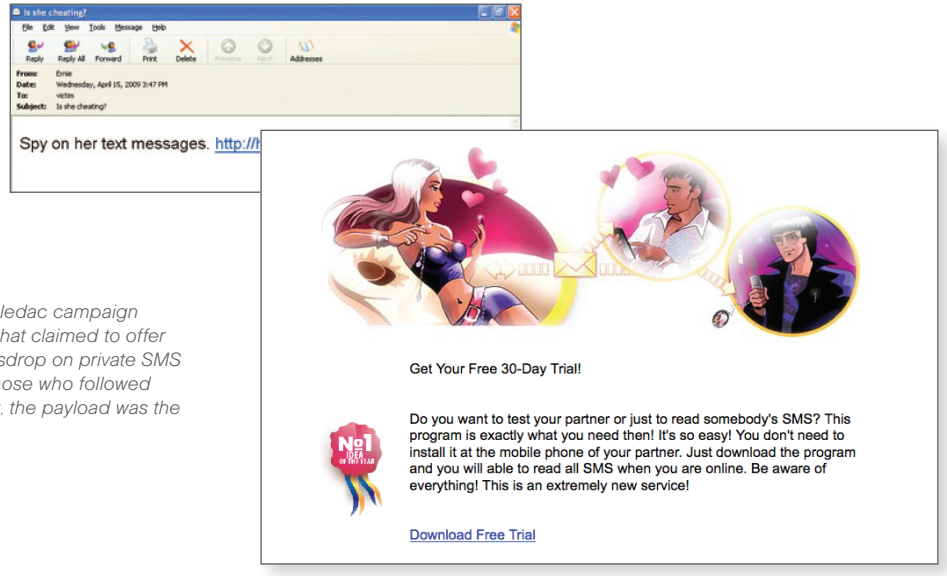
The Takedown of Srizbi/Reactor Mailer

Srizbi/Reactor Mailer fell just as quickly as it became the world's leading distributor of spam. The first salvo against Srizbi occurred when McColo, the botnet's hosting provider, was shut down in November 2008. McColo had a reputation for hosting botnet command and control servers and online pharmacy payment processors. Srizbi/Reactor Mailer appeared to be McColo's largest single customer.

Srizbi/Reactor Mailer's major flaw was that its entire command and control infrastructure was hosted in the same data center on McColo. When McColo was taken down by its upstream providers, worldwide spam volumes immediately dropped by two-thirds, according to the Cisco SensorBase threat-tracking database. Within two weeks, Srizbi/Reactor Mailer was able to relocate its operations to Estonia, and by February 2009, it once again accounted for 60 percent of global spam volume.

Spam Volume Decline Due to McColo Shutdown





A high-profile Waledac campaign delivered spam that claimed to offer software to eavesdrop on private SMS messages. For those who followed the enclosed link, the payload was the Waledac bot.

However, Microsoft dealt Srizbi/Reactor Mailer a crippling blow in February 2009. At that time, Microsoft added a signature for Srizbi to its Malicious Software Removal Tool (MSRT), eliminating most Srizbi infections in just a few weeks. Worldwide spam volumes plunged once again, this time to levels last seen in June 2007, according to SensorBase data. Srizbi has since mutated to a new botnet, Xarvester, in response.

Waledac: Storm 2.0

While Srizbi stole headlines in late 2008 and early 2009 as the spam powerhouse, the Storm botnet was morphing into Waledac—also called "Storm 2.0," because it came from the creators of Storm. Waledac began spreading its malware in earnest in early 2009, using emails referencing U.S. President-elect Barack Obama and the then-upcoming inauguration, as well as holiday-themed spam. Recipients were lured to a fake website and prompted to download an executable file containing the Waledac malware.

Waledac is notable for its use of fast-flux service networks, which both obscure the identity of web servers (often hosting illegal material such as malware and child abuse images), and make it harder to shut them down. The Storm botnet also used fast flux.

Waledac's most recent high-profile campaign, launched in April 2009, delivered spam that claimed to offer software that would allow users to eavesdrop on supposedly private SMS messages. As before, for the unfortunate recipients who followed the enclosed link, the payload was the Waledac bot.

The SMS spyware campaign is significant because the messages were sent through the Conficker botnet. This marked the first time that Conficker monetized itself by allowing Waledac to be downloaded via Conficker's hosts (read more about Conficker on page 4).

Battling the Botnets

In response to coordinated and effective responses to major botnet threats, botmasters see value in trying to stay slightly under the radar. One method seen by Cisco and IronPort researchers is lower-volume but more frequent botnet attacks, which may allow criminals to avoid gaining attention while still yielding enough new bots. In a keynote address at the recent LEET '09 USENIX conference, Cisco IronPort senior security researcher Henry Stern noted that today's malware creators recognize the value of "boring" technologies and tactics that are slow to garner the attention of security experts—and therefore, have plenty of time to wreak havoc.

For instance, the Torpig botnet (which was "hijacked" for 10 days in early 2009 by computer science researchers at the University of California, Santa Barbara) has apparently been in operation for a few years now, stealing login credentials for hundreds of thousands of online bank accounts. The researchers were able to observe the botnet's activity as it accumulated an additional 180,000 infections and collected more than 70 gigabytes of data. Although the researchers gleaned valuable information from their brief takeover of Torpig, the botnet remains active.

There are also signs that botmasters are willing to collaborate—or at least sell or send each other their wares—to make money. The "SMS spying" Waledac attack emanating from Conficker-infected hosts is a good example. The Rustock botnet, another prolific source of spam, appears to be exploiting the same vulnerabilities used by variants of Conficker—a case of criminals "borrowing" strategies from their competitors.

As for how to battle botnets during future attacks: Locating and shutting down hosting providers like McColo had an immediate impact on spam traffic and computer infections, and the release of the MSRT had a slightly longer-term impact.

"These are not permanent solutions to the botnet problem, but they are very effective," said Patrick Peterson, Cisco Research Fellow and Chief Security Researcher. "Naturally, these tactics need to be deployed in tandem with network-based botnet mitigation and spam mitigation solutions."

Mobile Device Threats: Text Message Scams

Text message scams targeting users of handheld mobile devices, such as cell phones and smart phones, are becoming a common fraud tactic. At least two or three new campaigns have surfaced every week since the start of 2009. The spike in frequency can be attributed partly to the economic downturn, but it's also the massive—and still growing—size of the mobile device audience that is making this new frontier for fraud irresistible to criminals.

According to the International Telecommunications Union, there are more than 4.1 billion cell phone subscriptions worldwide. Cell phones have become the communications technology of choice for many individuals—particularly in developing countries. Meanwhile, the number of smart phones in use is expected to outpace cell phones in the near future. A criminal may cast a wide net with a text message scam—targeting, say, 1 million users at a time. But, even if that effort yields only 1000 victims, the scammers are likely to guarantee a decent return on their investment.

Many text message scams rely on social engineering tactics to dupe victims into handing over personal identification information or credit card numbers by purchasing worthless (or nonexistent) products or services or cashing in on a prize. For example, in a recent fake lottery scam, Qatar-based customers of telecommunications company Qtel were targeted by Pakistan-based fraudsters purporting to be from the Qtel headquarters in Dubai. Customers were contacted by either SMS or phone and asked to provide "verification details," such as bank account numbers, to collect a grand prize. Victims were also asked to purchase scratch cards worth QR500 (approximately US$135) and provide those numbers as "security" when they collected their fictitious prize.

More criminals are also taking advantage of the popularity of online banking, and are heading straight for victims' money by specifically targeting their ATM accounts and personal identification numbers (PINs) with well-designed and localized text message scams—and they're leaving virtually no trail.

Because more handheld mobile devices offer Internet capabilities and PC-like functionality, more customers are using them to conduct financial transactions while they are mobile. So, when they receive a text message from their bank alerting them to a problem with their account, they may not view such correspondence as suspect—especially because these campaigns are often very sophisticated. (Note: Generally, financial institutions will not email, call, or text consumers to obtain or confirm passwords, PINs, or other identifying information regarding their accounts.)

To make their schemes even more convincing, scammers will direct recipients of their SMS messages to call a telephone number. When victims follow through, they actually connect with what sounds very much like the real bank's automated customer service line. Through voice prompts, recipients are asked to verify their identity by providing their login ID or account number and PIN. Then, the user is "thanked" by the automated operator and informed their issue has been addressed. Meanwhile, the scammers are already logging into the victim's bank account and transferring money into other accounts.

Recently, smaller financial institutions have been the focus of many text message scams, likely because customers tend to have higher levels of trust and familiarity with local banks. The following are some examples of recent text message scams involving these types of financial institutions:

- Cell phone users in Fargo, North Dakota, received text messages claiming there was an issue with their account at First Community Credit Union and were directed to call an 888 number. Callers were connected to an automated system for the "General Protection Department" and asked to answer three questions to verify their identity and to disclose a credit card or bank account number.
- A "smishing" scam (a phishing attack using SMS) that targeted Buffalo Metropolitan Federal Credit Union customers in New York surfaced in early 2009. The text message included a link that, when accessed, took victims to a phishing site meant to look like a legitimate website associated with the bank. Once on the site, they were prompted to download a program—a Trojan that provided criminals with access to customers' personal information.
- Scammers sent text messages to an undetermined number of Verizon Wireless customers, telling them their BCT Federal Credit Union card had been deactivated and they needed to call a certain number to reactivate the card. Several customers responded and provided their 16-digit card numbers and PINs, according to the bank, which operates in New York and Pennsylvania. The scammers used the information to recreate cards, withdraw money at ATMs, and make purchases.

Not surprisingly, telemarketing scams involving cell phones are also on the rise, and mirror "traditional" landline schemes. For instance, scammers tell victims that their auto warranty has expired and convince them to purchase a worthless insurance policy. Or, hoping to cash in on individuals' hard luck during the recession, they offer to help consumers get out of credit card debt or pay off their mortgage.

Consumers can put their mobile phone number on the United States Federal Trade Commission's (FTC's) Do Not Call Registry, and both the FTC and the United States Federal Communications Commission, which regulates cell phones, have made it clear that telemarketers may not use automated dialers to call cell phone numbers. Of course, scammers ignore such warnings, and because so many cell phones and smart phones are in use today, law enforcement cannot keep pace with the number of complaints they receive about telemarketing and text message scams that target users of these devices.

U.S. Government: A New Administration, a New Focus on Cybersecurity

As a candidate for the U.S. presidency, Barack Obama made it clear that, if elected, his administration would "make cybersecurity the top priority that it should be in the 21st century"[2] and put particular focus on its role in both homeland security and the nation's overall technology policy. He emphasized that information infrastructure, critical infrastructure sectors, and consumer safety were of great importance for the country.

Shortly after his inauguration in January 2009, President Obama launched a "60-Day Review" of the nation's cybersecurity infrastructure. Completed in May, this broad review included government systems, critical infrastructure sector systems, and consumer systems—domestic and global. The "comprehensive, clean-slate review to assess U.S. policies and structures for cybersecurity"[3] was the Obama administration's first major step toward:

- Developing a comprehensive cybersecurity policy for the United States
- Positioning the White House to assume a leadership role in protecting the nation's information infrastructure
- Fostering global cooperation on cybercrime, best practices, and ensuring a safer networking environment

[2] Remarks made by Senator Barack Obama at the Summit on Confronting New Threats, University of Purdue, July 16, 2008. Text of speech available on the Council on Foreign Relations' website: www.cfr.org/publication/16807/barack_obamas_speech_at_the_university_of_purdue.html.

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

Also in April 2009, President Obama appointed Aneesh Chopra, Secretary of Technology for the Commonwealth of Virginia, as the first U.S. Chief Technology Officer. This move underscored the new president's pledge to make cybersecurity and technology priority items for the United States. It also highlighted the administration's intention to help develop a more collaborative and highly interactive relationship between the government and citizens. (It is expected that part of this long-term plan will include the embedding of collaboration technologies into government systems.)

Following the 60-Day Review, the administration issued the *Cyberspace Policy Review* report, which includes key findings from the review and recommendations for improving the nation's cybersecurity. Those recommendations, including 10 near-term actions, were discussed by President Obama during a speech in the East Room of the White House on May 29, 2009. They include:

- A cybersecurity policy official (a "cybersecurity coordinator") responsible for organizing U.S. cybersecurity policies and activities will be appointed. Also, a strong National Security Council (NSC) directorate to coordinate interagency development of cybersecurity-related strategy and policy should be established. This directorate should be under the direction of the cybersecurity coordinator, who will represent both the NSC and the National Economic Council.
- An updated national strategy (for the president's approval) to secure U.S. information and communications infrastructure will be prepared. This strategy should include continued evaluation of the Comprehensive National Cybersecurity Initiative's (CNCI) activities and, where appropriate, build on its successes. (The CNCI, approved by President George W. Bush in 2008, is designed to reduce the vulnerability of federal computer networks and critical infrastructure and mitigate the effects of attacks against those networks.)
- Appropriate, interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process should be convened. In addition, coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the federal government should be formulated.
- A national public awareness and education campaign to promote cybersecurity should be initiated.
- U.S. government positions for an international cybersecurity policy framework should be developed, and the nation should strengthen its international partnerships, to create initiatives that address the full range of activities, policies and opportunities associated with cybersecurity.

According to the Cyberspace Policy Review, innovation should also be leveraged to address cybersecurity concerns. The U.S. government should work with the private sector to "define performance and security objectives for future infrastructure, linking research and development to infrastructure development and expanding coordination of government, industry, and academic research efforts."

While lacking the detailed action plans that no doubt are under development now, the Obama administration's 60-Day Review and *Cyberspace Policy Review* report represent outstanding leadership in improving U.S. cybersecurity. Simply having the president making direct comments on cybercrime creates far more attention and action within government. The report's focus on "leading from the top" and alignment of resources in the executive branch with access to the president will ensure the topic gets the attention it deserves. *The Cyberspace Policy* Review report also offers a level of transparency that was not available in the previous administration's CNCI program.

Although there will always be material the federal government cannot reveal to the public, sharing as much as possible will enable all government employees and industry to participate in the new administration's cybersecurity initiative appropriately. In addition, the emphasis on public/private partnerships—especially international cooperation—is an essential element in reversing cybercrime trends. The Internet is operated and managed by many private, global enterprises. Cooperation with all of them worldwide to address cybersecurity issues is essential.

Through this 60-Day Review process, the Obama administration has put in motion changes that will transform the structure of cybersecurity leadership in the United States. However, the president has emphasized that this more intense focus on improving the nation's cybersecurity will not create new burdens for the private sector, but opportunities. In his remarks on the results of the 60-Day Review, President Obama said, "Let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."

In addition, the president has requested that more than US$400 million be included in the federal budget to support cybersecurity spending for the Department of Homeland Security, to protect critical infrastructure and IT networks from hackers.[4] And as part of the recent federal stimulus package, the American Recovery and Reinvestment Act (ARRA) of 2009, President Obama asked that US$7.2 billion be allocated for new broadband spending to support various projects, such as bringing broadband to rural areas and creating a "broadband map" of the United States.

[4] "Obama's Budget Calls for Shifts in IT Spending," by J. Nicholas Hoover, *InformationWeek*, May 8, 2009.

The President's Smart Phone "Addiction"

The U.S. presidential election in November 2008 ushered in a new generation of leadership in the country—one that is at home with technology. And the man at the top, President Barack Obama, is someone who (like so many other individuals around the world) has wrapped his life around his personal technology use.

Being asked to relinquish his smart phone, the center of his "on the go" productivity and connectivity, would be unthinkable, even for the highest office in the land. So, when President-elect Obama—perhaps the most high-profile member among the legion of worldwide "CrackBerry" addicts today—was informed he would likely have to give up his beloved BlackBerry in the interest of national security, he resisted and asked the National Security Agency (NSA) to find a solution.

This caused a stir, primarily because this was a new issue for the NSA to tackle for the Oval Office. Eventually, President Obama won: It has been reported that the president currently keeps in touch with a select group of family and friends with a BlackBerry 8830 and uses a General Dynamics Sectera Edge smart phone for confidential government business. The Sectera Edge is reportedly one of only two types of smart phones that are approved to access the highly classified Secret Internet Protocol Router Network (SIPRNet).

According to media reports, President Obama will likely shift back to BlackBerry-only use once the appropriate security software is installed on the BlackBerry 8830 by the NSA—a day that may come very soon. Top aides and, of course, First Lady Michelle Obama, are expected to be issued the same devices.[6]

Additionally, US$11 billion will go to support a smart energy grid project that will modernize the way electricity is distributed throughout the country by integrating computer technology to help balance supply and demand from various energy sources. Recent events underscore the need for updating critical infrastructure, such as the U.S. electrical grid, in the interest of national security. "We know that cyber intruders have probed our electrical grid, and that in other countries, cyber attacks have plunged entire cities into darkness," said President Obama in his May 29, 2009, speech on cybersecurity.

While no such disruption has been reported in the United States to date, the grid-probing incident does point to the need for enhanced monitoring and control over such vital services. One such strategy is the Cisco plan for a "smart grid" that not only secures both physical and cybersecurity of electrical grids, but also helps utility companies manage power supplies and energy consumption more efficiently.

The ARRA also provides approximately US$20 billion for healthcare information technology. The legislation aims for widespread adoption of the use of electronic health records (EHRs) within the next decade and requires the federal government to develop standards by 2010 for the nationwide electronic exchange and use of health information to improve patient care.

[5] "Inside Obama's Classified Smartphone," by Sascha Segan, PCMag.com, January 23, 2009, www.pcmag.com/article2/0,2817,2339444,00.asp.

[6] "Obama's BlackBerry Getting Final Security Touches," by Roy Mark, eWeek.com, April 23, 2009, www.eweek.com/c/a/Mobile-and-Wireless/Obamas-BlackBerry-Getting-Final-Security-Touches-475999/, and "Obama to Ditch Sectera Edge for BlackBerry?" by Sascha Segan, PCMag.com, April 24, 2009, www.pcmag.com/article2/0,2817,2345908,00.asp.

Technology: An Engine of U.S. Growth for the Next "New Economy"

Aside from the increased emphasis on improving U.S. cybersecurity, the Obama administration has shown a strong interest in defining and refining the nation's technology policy. It is becoming increasingly clear that the president views technology as playing a vital role in the nation's overall economic recovery and defining America's place on the global stage in the next "new economy."

The Obama administration's actions during its first 100 days in office indicate that the president believes investing in the nation's technology in the short term—whether for improving national defense, healthcare, power transmission, or other areas—will pay long-term dividends for the country and its citizens. In a way, what will happen over the next few years is not unlike the national highway system construction supported by President Dwight D. Eisenhower in the 1950s that continues to benefit us today. Instead, the bridges and highways being built or improved include those that make up the nation's IT infrastructure.

Whether it is the priorities of economic recovery, healthcare (and healthcare IT), climate change and moving to a low-carbon economy (smart grids, smart buildings, smart transportation, and travel substitution), and education (technologies and schools, distance learning, and collaboration), it is obvious the new administration views technology as an engine of U.S. competitiveness and growth.

Geopolitical: Twitter Users Are Broadcasting the Revolution

Twitter, the microblogging service whose popularity skyrocketed in the first half of 2009, has been playing a starring role in political uprisings and demonstrations around the world. Although microblogging is legal and currently low-risk in terms of online security, the lightning-fast speed at which social networking services like Twitter can spur mass action is worth noting.

In response to allegations of voting fraud during Communist Party elections in the country of Moldova, students and other individuals protested on the streets of Chisinau, the capital, and learned of upcoming demonstrations via Twitter and other social networking vehicles. The government had shut down SMS texting and television stations. On one particular day of protests in early April 2009, Twitter posts meant to generate support for demonstrations were being delivered at a furious rate—new posts would appear every few seconds.

The same tactic was used by protestors during the G20 economic summit in London in April 2009. Protestors not only used social networking services (frequently from their mobile devices) to assure heavy turnout at demonstrations, but they also traded messages about evading the police. Of course, because many social networking posts are public, authorities could visit the same service to locate protesters and learn about planned activities.

Social networking's ability to summon crowds is also evident in the rise of "flash mobs," where individuals gather in large crowds—sometimes for a serious purpose and sometimes just for fun—to conduct some action, and then quickly leave the scene of the demonstration. Alerts about impending flash mobs are usually spread via social networks like Twitter. In May 2009, flash mobs appeared at several European airports, including London's Heathrow, to protest airport expansions.

The power and reach of social networking to bring about societal change is fascinating to watch, but also somewhat sobering because these tools won't always be used by the "good guys." All types of political activities—demonstrations, coup attempts, and general unrest—can take place at a far more rapid pace than ever before, posing a greater risk of instability for emerging markets and governments.

Economic Instability and Online Security

As worldwide unemployment rises and the job market tightens, security watchers assume that online crime may also be on the upswing. Employees who have been laid off, particularly those with IT skills, may see no option but to turn to online scams or other criminal activity. A subset of disgruntled employees without jobs may also be tempted to earn money by targeting former employers through network attacks or the theft and sale of intellectual property. (See "Conversations with a Botmaster" on page 8 for insights on why individuals with IT talent might choose illegal work over a legitimate job.)

In May 2009, the *Financial Times* reported that fraud committed by employees against their own companies may be on the rise, owing to the weak economy. The newspaper cited statistics from "whistleblower" hotlines, showing an increase in tips about insider crime. And in April 2009, the Association of Certified Fraud Examiners, the world's largest anti-fraud organization, released its report, *Occupational Fraud: A Study of the Impact of an Economic Recession.* According to the report, 90 percent of surveyed fraud examiners said they expect to see a rise in fraud over the next 12 months.

Vulnerabilities

The Weak Links in Social Networking

Web 2.0, the name for the collection of technologies and applications that make the Internet more collaborative and interactive, helped create the revolution in social networking. However, these lightweight, easy-to-use technologies aren't usually robust enough to block attacks from online criminals. The open, simple communication structure of Web-2.0-based applications is also its key weakness: Scammers who can exploit weaknesses in social networking sites can reach millions of potential victims with a single click.

Users of social networks place an undue amount of trust in members of their friend or contact lists. Criminals rely on this assumption to engage in social engineering-based scams—that is, they prey on computer users' assumptions that individuals in their communities won't send them malware-laden messages. So when a known community member sends friends a message with a link, recipients are far more likely to click through—inadvertently downloading malware, or ending up at a malicious website.

With a worldwide membership of 200 million as of May 2009, the social networking site Facebook has become a popular target for phishing attacks. According to phishtank.com, a website devoted to tracking phishing activity, about three separate phishing attacks were launched against the site on a daily basis in March 2009.

Microblogging service Twitter has also been susceptible to worm attacks. In April 2009, worms identified as "Mikeyy" or "StalkDaily" were spread by scammers who hacked into Twitter accounts and replaced the users' legitimate status updates with a link to a supposed celebrity website, StalkDaily.com. Each Twitter user who saw what they believed to be a friend's update and clicked on this link would then infect their own Twitter accounts, and cause the malicious link to be sent to their entire network. The 17-year-old hacker who created the "Mikeyy" worm said he did so "out of boredom"—an exception to most of today's malware attacks, which are launched to make money.

These worms were able to exploit a cross-site scripting vulnerability on the Twitter website. The attack had the potential to be far more malicious than it was, because it could have infected users' computers with malware instead of simply changing their Twitter status updates. This worm attack, like others aimed at social networks, demonstrates the need for more robust protection mechanisms built into the networks themselves.

Mac OS: Online Criminals Move Beyond Windows

In one of Apple's well-known "Mac vs. PC" commercials, "PC" laments the fact that his Windows-based computer is prone to security threats, while "Mac" stands complacently by. The implication is that the Mac operating system (OS) is far less vulnerable to security threats than Windows—so Mac users are more protected against online criminals.

Today, there are signs that criminals want to debunk the widely held assumption that the Mac OS is less prone to online attacks. Criminals are not targeting Macs because they perceive them to be less secure than they used to be, but rather because they offer greater opportunity for profit than before. Gartner Inc. has predicted that Apple will double its share of the computer market in the United States and Western Europe by 2011.

The first botnet that seems to be specifically aimed at Macs was identified by security researchers in mid-2009. A malicious file appears to have been placed in pirated copies of Apple's iWork software and Adobe Photoshop for the Mac OS. That malware infected the computers of users who downloaded the pirated software and turned the systems into nodes for the botnet. There are signs the botnet is being used to launch distributed denial of service (DDoS) attacks.

In short, while "Mac" in the Apple commercial may have a relaxed attitude toward his ability to ward off online scammers, businesses and individuals relying on Macs should not adopt a similarly laid-back stance. Much like forward-thinking businesspeople, online criminals look for markets to exploit.The popularity of Macs presents the chance for criminals to launch new attacks in more places and grow botnets with more infected computers. Security policies should be applied regardless of the operating system or device that is used to access and share corporate data—whether it's a Microsoft Windows or Mac system, Apple iPhone, Palm or BlackBerry, protection needs to reside in the network.

According to a recent study, 45 percent of surveyed privacy and security professionals said they had purchased cloud computing services for their companies, and an additional 22 percent are considering such a purchase.

Cloud Computing: Protecting Data in the Cloud

According to a recent study from Deloitte & Touche and the Ponemon Institute, 45 percent of surveyed privacy and security professionals said they had purchased cloud computing services for their companies (for such key services as data storage, email, and financial applications), and an additional 22 percent are considering such a purchase.

However, for the most part, these same professionals have not established plans for managing the security risks associated with ceding so much valuable corporate data to a third party. The Deloitte/Ponemon Institute study also reported that 82.6 percent of surveyed businesses had no formal plans in place to protect data they were entrusting to cloud providers. And in a recent IDC survey of companies' views of cloud services, respondents indicated that security was the greatest cloud-computing challenge they faced.

The cost-savings potential of cloud computing solutions could make them alternative models for some business operations, especially in challenging economic times. However, positive attention about the benefits of cloud computing may overshadow the possible risks that the solutions pose. At worst, security experts imagine scenarios wherein a hacker is able to compromise a single cloud system and access information or gain control of networks for hundreds of companies at once.

Cloud computing is one of the factors behind "deperimiterization," or the blurring of the lines of defense between corporate networks and the outside world (including online criminals). As such, cloud computing requires greater scrutiny in terms of security.

Businesses may lag in their understanding of the security implications of cloud computing. Any enterprise using cloud solutions must ask service providers about the type of security levels and controls stated in their service-level agreements, where and how their data is physically and logically stored, and compliance and regulatory documentation for the countries over which cloud services may travel.

Productivity Applications: Targets of Zero-Day Exploits

Online criminals continue to seek ways to launch exploits that are less suspect than, say, malware-laden spam. Vulnerabilities in popular productivity applications—such as Microsoft Word and Excel, and Adobe Reader and Acrobat—may be ripe for attack by scammers for the same reason popular social networking applications have become attractive. Users of these productivity applications perceive them to be safe environments and therefore are more likely to open documents provided by attackers. Additionally, targeted attacks against unknown vulnerabilities—known as zero-day attacks—allow criminals to continue to hide vulnerabilities from software vendors, preventing software fixes from becoming quickly available.

In early 2009, Adobe identified buffer overflow vulnerabilities that could cause some of its programs to crash, and possibly allow a hacker to take control of the user's computer. The company made appropriate patches available within a few weeks. Security researchers

Top Alerts: January–June 2009

Adobe Acrobat Products PDF File Buffer Overflow Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=17665
Adobe Reader Function Buffer Overflow Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=18088
Worm: Conficker	http://tools.cisco.com/security/center/viewAlert.x?alertId=17121
GhostNet Spy Network Infiltrating Government and Private Systems	http://tools.cisco.com/security/center/viewAlert.x?alertId=17938 http://tools.cisco.com/security/center/viewAlert.x?alertId=17924
Gumblar Malicious Code Manipulates Search Engine Results to Increase Advertising Revenue	http://tools.cisco.com/security/center/viewAlert.x?alertId=18286
Worm: Koobface	http://tools.cisco.com/security/center/viewAlert.x?alertId=17240
Microsoft Office Excel Invalid Object Arbitrary Code Execution Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=17689
Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=17519
Microsoft Office PowerPoint Arbitrary Code Execution Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=17966
Malware Distributors Employ Search Result Poisoning to Target Unsuspecting Users	http://tools.cisco.com/security/center/viewAlert.x?alertId=18034
Worm: Waledac	http://tools.cisco.com/security/center/viewAlert.x?alertId=17327

detected exploits related to this vulnerability, so it was apparent that criminals were intending to make use of it. In May 2009, there were additional announcements about vulnerabilities in Adobe products. A similar flaw was identified by researchers in the Excel spreadsheet program in February 2009, but only after hackers used the vulnerability to take control of computer systems at businesses and government offices in Asia.

Since these exploits are often delivered via emailed files (for instance, Word or Excel documents or Adobe PDFs) that are commonly used in business environments, the best defense is user education. In years past, computer users were advised to exercise caution about opening executable (.exe) files; they should learn to apply the same level of skepticism to common productivity files that are coming from unexpected sources, or that raise suspicion because of the nature of the email message.

Barring user education, organizations can protect themselves against these threats with network-level signature and reputation systems. In addition, security solutions that monitor content of email messages (not just attachments) identify trends that indicate threat outbreaks and block email messages accordingly.

Web 2.0 Security: Filtering Dangerous Content

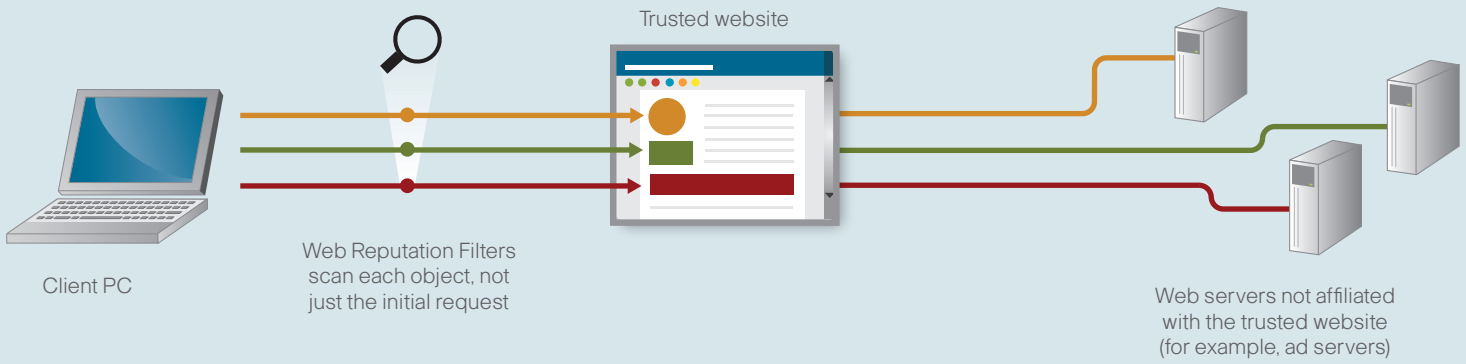
Dynamic Web 2.0 websites gather material from many sources, creating a richer experience for the website visitor—and a security headache. Online criminals intent on spreading malware now have many points of entry into websites, increasing their chances of success.

To the online visitor, who may only see the URL of a reputable site in the web browser, a malware attack can be impossible to spot. When a site is drawing its content from many third-party providers, there is no way to guarantee all of the component information is safe and free of malware.

Gumblar malware, which was racking up a number of hacked high-profile websites as of mid-2009, makes use of this Web 2.0 weakness. Gumblar begins its attack by exploiting legitimate websites through stolen FTP credentials and by leveraging vulnerable web applications through JavaScript. Visitors to these compromised websites are then exposed to malicious code that diverts search engine results to malware and phishing websites.

Preventing these kinds of attacks has become a key security requirement, as more and more websites pull content from third parties (a typical webpage can draw content from as many as 150 sources). URL filtering, one of the most common methods of blocking malicious content, is not effective; rather, a solution that examines every request for information made by a web browser as it loads content is necessary.

Protection For a Dynamic Web 2.0 World: Visibility Beyond the Initial Threat



Data Loss and Compliance

Data Loss

Identity Theft

The recession has created new moneymaking opportunities for at least one group of "entrepreneurs": identity thieves. As predicted in the *Cisco 2008 Annual Security Report*, spam, phishing, and text message scams are on the rise and growing in sophistication. Many of these campaigns are designed and deployed for the purpose of stealing identities to open new financial accounts or misuse existing ones.

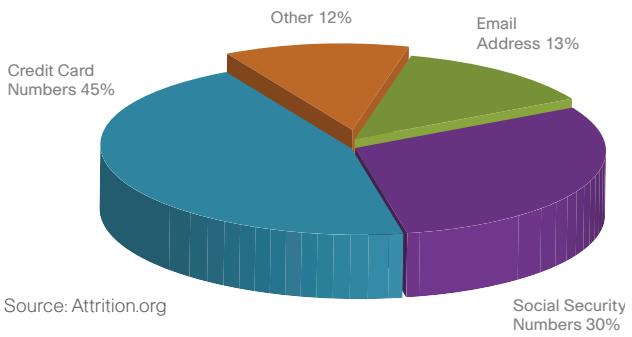
Of even greater concern is the role that "carding" (large-scale theft of credit card account numbers and other financial information) plays in funding terrorism and drug trafficking. According to a recent U.S. Department of Justice report, *Data Breaches: What the Underground World of Carding Reveals*, the "connection between identity theft—in particular as it relates to obtaining fraudulent identification documents—and terrorism is well established. In addition, links to drug traffickers engaging in identity theft for purposes of funding drug addictions is also well known."

The FTC reports that more than 9 million identities are stolen annually in the United States alone. Thirty-seven percent of complaints to the FTC deal with identity theft—by far the largest category of complaints the agency must field.

Researchers say that individuals ages 18 to 25 are at the highest risk for experiencing identity fraud today. This is primarily due to Generation Y's fondness for social networking. Identity thieves and hackers are trolling these sites regularly, searching for the keys to a user's identity—and finances. Users' profiles can provide a wealth of personal information—names, date of birth, hometown, and even phone numbers—that provide just enough detail for clever criminals to successfully commit fraud. Some have even gone so far as to contact a victim's friends and family members directly to request money.

Meanwhile, criminals continue to hack into personal email accounts to locate sensitive financial data or login information for websites. Or, they deploy social engineering techniques designed to lure unsuspecting victims to fake *and* legitimate websites, where they either willingly provide personal identification information, or unwittingly download keylogging malware that surreptitiously collects all the authentication details required for a criminal to gain access to their money. And with more botmasters looking to monetize their botnets, keylogging software is now being used to gather sensitive personal information from victims on a massive scale—stealthily.

Lost Record Types



Consistent with the greatest regulatory concerns, security professionals are most sensitive to data loss when credit card numbers, Social Security numbers, and private employee and customer records are lost.

Data Breaches

Data loss is a common problem for organizations, and it can be very costly: The Ponemon Institute estimates that in 2008, data breaches cost U.S. companies, on average, US$6.65 million, with the largest cost increase being lost business; this is an increase over 2007 at US$6.2 million. The Ponemon Institute also estimated the cost per record to be US$202.

According to the Privacy Rights Clearinghouse, which maintains a "Chronology of Data Breaches," 260 million personal records have been reported lost or stolen since January 2005—just in the United States. And the Identity Theft Resource Center (ITRC) says reported data breaches nearly doubled in 2008 from 2007. ITRC also says financial institutions were responsible for more than half of the 35 million personal records known to be lost or exposed during 2008.

The first major data breach reported in January 2009 involved a leading credit card processor. The company announced it had discovered—and had taken actions to resolve—a malware infection in its processing system that caused a 2008 breach, and that the incident may have been the result of a widespread global "cyber fraud" operation. The company processes cards for approximately 250,000 businesses in the United States, which means millions of credit and debit card transactions may have been compromised. The company reported a quarterly loss of more than US$2 million as a result of spending more than US$10 million in legal bills, fines from MasterCard and Visa, and administrative costs.

Insiders

Fraud, hacking, and identity theft by insiders are very real security threats, and they can be especially damaging for an organization because insiders know security weaknesses and how best to exploit them. Given the current economic downturn, in which many individuals have lost their jobs or become disgruntled—or set traps in advance to retaliate against an employer—insider threats can be expected to increase in the months ahead.

The Identity Theft Resource Center estimates that insiders were responsible for nearly a quarter of all known incidents involving financial institutions in 2008. That trend appears to be continuing in 2009. In April, a former employee at the Federal Reserve Bank of New York and his brother were arrested on suspicion of obtaining loans using stolen identities. According to the U.S. Federal Bureau of Investigation, one brother worked as an IT analyst for the bank and had access to sensitive employee information. Investigators found a USB flash drive attached to his computer with applications for US$73,000 in student loans using two stolen identities. They also found a fake driver's license with the photo of a bank employee who wasn't the individual identified in the license.

In a separate investigation, the U.S. Postal Inspection Service discovered that the fraudster's brother had opened a mailbox in New Jersey using a fake driver's license with a photo of a former or current employee of the Federal Reserve Bank of New York. He allegedly used the mailbox to receive documents for a boat loan obtained through the use of a stolen identity. He also is suspected of using a fake driver's license with another bank employee's photo in connection with the boat loan, and with using a bank employee's information for a phony income tax return.

Also in April 2009, a former employee of New York's Department of Taxation and Finance was arrested on charges that he illegally possessed sensitive personal data of thousands of New York residents and used the information to apply for and obtain credit cards. According to the office of State Attorney General Andrew Cuomo, the thief (who allegedly opened 90 fraudulent credit cards and other credit lines at more than 20 banks) had unpaid charges on accounts totaling more than US$200,000.

Among the fraudster's identity theft victims were a 4-year-old boy and at least four dead people, including his mother and sister. While employed for the Department of Taxation and Finance, he worked in a unit that scans identification documents, including birth certificates, submitted in connection with routine audits. Investigators found copies of more than 700 New York State tax forms; copies of more than 300 birth certificates and more than 1000 Social Security cards; and hundreds of pages of credit card statements, inquiry letters, applications, and cards in the criminal's and others' names.

In addition, as companies continue to look for ways to cut costs, they may increase their dependence on short-term staff, teleworkers, consultants, and third-party resources. Organizations will be wise to implement additional security policies regarding these resources and be particularly vigilant about the level and term of their access to sensitive data. One recent case: A disgruntled software engineer contractor who had worked for Fannie Mae for three years and had access to 4000 of the company's servers was indicted in January 2009 for allegedly planting a "logic bomb" in the mortgage lender's computer network. The embedded code was discovered by another engineer before it caused any damage, which would have been monumental, as the malicious script was designed to wipe out all data across Fannie Mae's network on January 31, 2009.

Web 2.0 Collaboration Quandaries and Mobile Device Dilemmas

In today's highly collaborative Web 2.0 environment, information is being shared between individuals inside and outside of an organization more often—and frequently in an insecure fashion. For example, according to a 2008 Cisco report titled, *The Challenge of Data Leakage for Businesses and Employees Around the World*, 44 percent of employees share work devices with others without supervision. Meanwhile, 18 percent share their passwords with coworkers.

Most organizations today have policies that provide clear guidelines about the devices and applications that employees are permitted to use while on the job. However, many workers find the rules constraining, and in the interest of conducting business more quickly and efficiently, ignore the rules that protect them and the organization. And until something costly or embarrassing happens, most users think nothing of the threat their carefree use of technology may pose to their employer.

Using technology that is not supported or approved by an organization can even compromise national security. In early 2009, Internet security firm Tiversa revealed that sometime during the summer of 2008, an unauthorized peer-to-peer file-sharing program installed on an employee's PC had led to a security breach in which blueprints "including planned engineering upgrades, avionic schematics, and computer network information" for the U.S. president's helicopter, Marine One, had been transferred to an IP address in Tehran, Iran. Tiversa reported that the address belongs to an "information concentrator," someone who searches peer-to-peer networks for sensitive information.

Mobile and handheld devices also create security headaches for organizations. Of course, with more of these devices on the work scene, there are more opportunities for employees to lose equipment containing sensitive data or login information. But there's more to the story: These devices, just like collaborative Web 2.0 applications, are playing a key role in stretching the traditional security perimeter.

Many workers—regardless of the policies their employers set—are using handheld devices, such as smart phones or netbooks, for both work and personal use. As more handheld devices are designed to offer PC-like functionality and a richer computing experience, users are expected to rely on their handheld devices even more to access business-critical information, including financial data and sales reports. Therefore, companies and their IT departments can expect mobile device security to remain a concern.

Collaborative applications and mobile devices can enhance workforce productivity and create cost savings. But businesses today face the challenge of balancing that productivity opportunity with the security risks it brings, and finding the right mix of policies and technologies to mitigate those risks. Going forward, companies will need to create policies and deploy solutions that protect sensitive data and prevent security threats, but that are also relevant for a Web 2.0 work environment where handheld devices are becoming the computing tools of choice.

Organizations must also take care when removing access rights after terminating any type of employee: A recent survey of laid-off workers conducted by the Ponemon Institute revealed that many companies are not doing enough to protect against data theft when they trim their workforce. Eighty-two percent of respondents said their employers did not perform an audit or review of documents before employees departed the company. Meanwhile, nearly a quarter of respondents said they still had access to the corporate network of their former employer after being laid off. According to the same study, more than 60 percent of those who purposefully took confidential data from a former employer also reported having an unfavorable view of the company.

Compliance

Around the world, there is an increase in legislation and industry initiatives around making data on networks more secure and informing those affected by data breaches. Today, there are many laws, regulations, and standards just in the United States related to data management. In fact, individual states are becoming much more aggressive about protecting their citizens from identity theft and other fraud; more than 40 states have already enacted data breach laws.

Nevada, for example, implemented a privacy law in 2008 that prohibits businesses from electronically transferring customers' personal data—such as first and last names, Social Security numbers, and bank account numbers—outside their organization, unless the data is encrypted. The law applies to data in motion and not "at rest."

Massachusetts also passed a regulation in 2008 that requires all persons who own, license, store, or maintain personal information concerning the state's residents to protect that information from unauthorized access, disclosure, or misuse. Companies affected by the legislation must assess the risks to such information and develop written, comprehensive security programs that address them.

The Massachusetts regulation also requires affected entities "to the extent technically feasible [to implement] encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly" as well as "all personal information stored on laptops or other portable devices."

Massachusetts' encryption requirement proved to be a major hurdle for compliance by the initial deadline of January 1, 2009, particularly for smaller organizations. Ultimately, the state extended the deadline for encryption of non-laptop devices twice, and it is now set for January 1, 2010. (The compliance date for encryption of laptops and data sent over public networks and wireless systems, however, is the new general compliance date of May 1, 2009.)

HIPAA Gets HITECH

On the healthcare compliance front, U.S. President Obama's 2009 American Recovery and Reinvestment Act (ARRA) stimulus package gave a boost to the Health Information Portability and Accountability Act (HIPAA): the Health Information Technology for Economic and Clinical Health Act (HITECH Act). This measure substantially raises the penalties for noncompliance for healthcare companies. It also contains regulations that expand the security and privacy provisions of HIPAA. More significantly, perhaps, it also generally extends some of those regulations to non-HIPAA-covered vendors of personal health records and their business partners.

The HITECH Act, like HIPAA, preempts any contrary state laws, but leaves intact any state laws and regulations that impose stricter requirements on the handling of patient information. Two examples of strict laws on the books: United States Senate Bill 541 (SB 541) and Assembly Bill 211 (AB 211), which California Governor Arnold Schwarzenegger signed in September 2008. These laws, which went into effect on January 1, 2009, are designed to improve patient privacy laws, address confidential health information leaks, and give the state the ability to assess and enforce fines for unauthorized disclosure of patient information.

AB 211 created a new State Office of Health Information Integrity (OHII) to oversee data issues and enforce statutes regarding confidentiality of healthcare data. OHII also is responsible for administering fines ranging from US$25,000 to US$250,000 on noncompliant entities. Meanwhile, SB 541 outlines the fine scale for healthcare organizations that commit data privacy and security violations that put patients at immediate risk of injury or death. The fines can run as high as US$50,000 for the first administrative penalty, up to US$75,000 for a subsequent administrative penalty, and up to US$100,000 for the third (and every subsequent) violation.

An organization that is covered by HIPAA and the HITECH Act must meet new minimum standards while continuing to monitor and comply with the growing number of laws governing patient information in every state in which the company operates. The HITECH Act's security breach notification requirements specify the timing, manner, and substance of any breach notification, among them:

- Notifying the Secretary of Health and Human Services "immediately" if the breach affects 500 or more individuals
- Notifying each individual whose unprotected health information is reasonably believed to have been accessed, acquired, or disclosed as a result of the security breach
- Providing notice to prominent media outlets in each state where the unsecured protected health information of 500 or more residents is reasonably believed to have been accessed, acquired or disclosed as a result of the breach
- Specifying in each notification to an individual a description of what happened, the types of information believed to have been accessed, and contact procedures for affected individuals to ask questions or learn more information

New "Red Flags" Rules

Because the concern around identity theft is escalating, it is driving more restrictive regulations both at the federal and state levels in the United States. This is creating additional burdens—in terms of money, time, and human resources—for businesses already working to be compliant with other existing laws, standards, or best practices, such as the industry-led Payment Card Industry Data Security Standard (PCI DSS), HIPAA, Gramm-Leach-Bliley Act (GLB), and Sarbanes-Oxley Act (SOX).

Of note are the new "Red Flags" Rules issued by the FTC, federal bank regulatory agencies, and the National Credit Union Administration. These rules—already delayed once before—were supposed to go into effect on May 1, 2009, but businesses now have until August 1, 2009, to develop their written programs. However, enforcement of the rules is scheduled to begin as planned on November 1, 2009. Examinations on financial institutions began in November 2008, and examinations for credit unions began April 2009.

In short, the rules require financial institutions and creditors to implement written identity theft programs for detecting, preventing, and mitigating instances of identity theft. Creditors that must comply with the rules are businesses that provide goods or services before billing, including industries such as telecommunications, utilities, and healthcare. The "red flags" to be monitored are patterns, practices, and specific activities that may indicate identity theft; for example, unusual account activity or attempted use of suspicious account application documents.

The program must also describe the appropriate responses that would mitigate the crime and detail a plan to update the program. (For more information on the "Red Flags" Rules, go to www.ftc.gov/opa/2008/10/redflags.shtm.)

Securing Data

More businesses are realizing their data is a vital asset, and are working to be more proactive about protecting it. As was recommended in the *Cisco 2008 Annual Security Report*, organizations must identify the data that they need to keep safe and place stronger controls where necessary. In short, they must let go of the view that they should try to protect everything, as that is an impossible task.

Companies also should strive to educate their employees and continually monitor email and web traffic to ensure sensitive information is not being shared inappropriately. Many organizations have implemented formal data loss prevention (DLP) programs to help secure their data—whether it is stored, in use, or moving around the network.

PricewaterhouseCoopers' *2008 Global State of Information Security Study* reports that many organizations are also paying more attention to protecting sensitive data on mobile devices such as laptops—primary contributors to data loss because they are easily lost or stolen—as well as on databases, file shares, backup tapes, and removable media. Cisco advises its customers to deploy methods (preferably automated) to maintain the confidentiality of information on mobile devices, such as access controls, encryption, remote data removal, data association, redaction, truncation, or other methods that effectively render data unusable to unauthorized users.

Policies

Policies are a must-have for compliance audits. This is a primary focus for auditors—most compliance and industry best practices or regulations, such as HIPAA, the "Red Flags" Rules, PCI DSS 1.2, SOX, and GLB, require policies, which are thoroughly reviewed during audits.

Increasingly, companies are also realizing that these policies are important in the event that something does go wrong—such as a data breach that compromises customers' credit card numbers—so they can show victims, attorneys and legal departments, shareholders, and law enforcement that they took clear steps to prevent such an event from happening.

While regulatory standards are designed to help protect user data, organizations should never view compliance as a security guarantee. In fact, as stated in the *Cisco 2008 Annual Security Report*, multiple security incidents in the previous year involved organizations considered to be "compliant." However, compliance procedures are specific by design; they are intended to help organizations achieve only very specific objectives that mitigate only particular security risks.

Conclusion and Recommendations

Conclusion

Cybercrime, fueled by the global recession, is costing global businesses and individuals billions of dollars, according to recent industry estimates. It is a complicated world, with players big and small, organized and fringe, sharing a common desire to secure their own profits. Some players are just the guy or girl down the street—like the botmaster discovered and interviewed by Cisco researchers—who is content to scrape out enough to ensure a comfortable lifestyle. However, many other players are doing whatever possible—and more often now by pooling their resources and knowledge—to maximize their profits.

As predicted in the *Cisco 2008 Annual Security Report*, attacks are only going to become more sophisticated and targeted as we move through 2009. Social engineering is, and will remain, the technique of choice for criminals devoted to mastering the arts of trust-breaking and reputation-hijacking. To launch an attack, a social engineer might seize upon the hot topic of the day, such as swine flu or a major sports championship, or pose as someone (a friend or family member) or something (a local bank or a well-known company) to lure unsuspecting victims into handing over their personal information and ultimately, their identity and money.

Users, in droves, are also being convinced to install software that infects their systems and then harvests their personal information—or hijacks the machine so it will spam, infect, or con other users. Worse, users seeking protection from common cybercrime ultimately become victims anyway by turning to the Internet for help: They are duped into buying bogus anti-malware software to "clean up" their infected systems.

Meanwhile, there is increasing investment, focus, and success in malware used to infiltrate a computer and make it part of a botnet. Increasingly, botmasters are working to monetize their botnets, by renting them out, forming alliances, or blatantly exploiting each other—all at rapid speed. Many botmasters are borrowing the best practices and strategies of competitors, and even the real business world, to make their own attacks as high-impact as possible. These activities are all signs of the maturing online criminal economy, where tools and techniques can be easily assembled to quickly and quietly launch an attack affecting millions of people.

Security Community Making Strides

Although it's true that cybercrime is only becoming more pervasive, this year's positive news clearly illustrates the growing effectiveness of the means for fighting back. The unprecedented level of cooperation and participation by the security community and industry in response to the Conficker threat earlier this year marked an important turning point in the ongoing battle against cybercrime and fast-moving and far-reaching Internet security events.

The Conficker Working Group established for this strategic fight-back effort will no doubt serve as a model for the future. Conficker's impact—while significant and still playing out worldwide—has been dramatically reduced because multiple entities combined their knowledge, best practices, and technology to strategically, and as proactively as possible, hinder the spread of the worm.

It is obvious that those bent on committing cybercrime are taking advantage of the fact that many aspects of their targets (desktop operating systems, enterprise network infrastructure, DNS, hosting providers, and so on) are under the control of many different vendors, operators and entities. But the Conficker Working Group demonstrates that the industry can adapt and respond to a significant weakness rapidly and effectively. Thus, when the next major security threat emerges, the security community will know how to assemble and take action swiftly—together.

Through the Conficker experience, the security community also learned that although it may not be possible to clean up every infected computer in the world, it is possible to prevent infected computers from receiving new attack instructions, software binaries, and malware. Unfortunately, however, many of today's security threats are like the Hydra from Greek mythology: One head is cut off, and another grows back in its place. And as the underground economy grows and becomes easier for would-be criminals or simple opportunists to participate in, the Hydra becomes even more difficult to thwart.

One bright spot is that vulnerability and threat activity has been off to a slower start this year compared to 2008, according to Cisco research. This could indicate the security community is succeeding in making it more difficult for attacks to take root and grow.

There is even greater cause for optimism, as well: More cyber criminals—like the Shah brothers (see page 5)—are being identified and prosecuted. Many are going to jail. Security watchers are cautiously optimistic that future efforts to shut down online criminal activity will be increasingly supported by law enforcement. And President Obama has made it clear that improving cybersecurity is a front-burner issue for the United States, and the U.S. government is eager to work with the international community and the private sector to make the Internet safer for everyone.

2009 Threats and Vulnerabilities:
25 Percent Decrease From 2008 Activity Levels

Month	New Alerts	Updated Alerts	2009 Total	2008 Total
January	148	392	540	630
February	227	249	476	695
March	222	335	557	659
April	164	206	370	639
May	218	175	393	528
Totals	**979**	**1357**	**2336**	**3151**

Trends to Watch

Spam to Return to Record High Levels

Even actions that produce dramatic results provide only short-term relief, as has been the case with the takedown of Srizbi/Reactor Mailer. When hosting company McColo was shut down by its own Internet providers, worldwide spam volumes dropped dramatically and immediately. But it didn't last. Ever since the botnet's operators got back in the game with an Estonia-based hosting company, spam volumes have been climbing.

In addition, following the "noise" that helped to expose Conficker last year, botmasters have been working harder to conceal their activities for as long as possible so they can quietly grow their botnets to desired size. Thus, there has been a rise in lower-volume and more frequent botnet attacks recently.

In the months ahead, expect spam volumes to continue to rise to record levels. In May 2009, increases as high as pre-McColo levels were reported. In a 24-hour period around the U.S. Memorial Day holiday (May 25, 2009), just over 249 billion spam messages were sent—the third-highest volume day ever.

More Attacks on Legitimate Websites

Compromising legitimate websites for the purpose of propagating malware remains a popular and highly effective technique. Recent Cisco data shows that exploited websites are responsible for nearly 90 percent of all web-based threats.

Users expect websites from reputable organizations that they know or conduct business with to be safe, and therefore, are not likely to have their guard up when visiting these sites. Infecting legitimate websites also allows for precision targeting of certain groups, such as sports fans or students—an approach that has been very lucrative for cyber criminals. (And removes a great deal of their legwork.) Criminals are expected to maintain their aggressive targeting of legitimate websites, especially to distribute malware for creating botnets.

Social Networking Attacks to Continue

Cyber criminals go where the users are, which means social networking sites are becoming more popular haunts for attackers. In particular, identity thieves are finding great success on these sites, which can provide them with just enough information about a user to take advantage of that person, as well as their friends and family.

Criminals prey on a user's trust in their online community, and on their assumption that the people, companies, and organizations they interact with do not pose a threat to their security. This is why a user is likely to click through a link or download content that was sent to them by a trusted source, and in the process, inadvertently download malware or end up on a fraudulent or malicious website.

Worms have also been a problem for many popular social networking sites recently—and until these sites start featuring more robust protection that is built into the network, expect social networking communities to remain favorite hunting fields for many cyber criminals.

Recommendations

Security must move at the speed of crime. Organizations and users must not wait to patch their operating systems and applications. The list of vulnerabilities grows every day, as does the number of new applications (and versions of existing applications). Meanwhile, the complexity of attacks is increasing. Thus, businesses and users have no choice but to become more agile in deploying countermeasures and working with appropriate parties to respond to attacks.

In addition, security solutions need to be built to react rapidly. Anti-spam systems have become the blueprint for this model. For years now, new attacks have been developed and new techniques have been deployed to meet those threats effectively. All threats are heading in this direction and solutions must do the same.

History shows that many attacks and threats use the same vectors to exploit a vulnerability or compromise victims. Understanding the "anatomy" of an attack, and using multiple solutions and techniques that complement one another to prevent the threat from moving to the next phase, will help to disrupt and prevent the resulting infection quickly.

User education and security awareness training are critical. As was recommended in the *Cisco 2008 Annual Security Report*, employees should be expected to play a vital role in safeguarding their own online identity and understanding the risks that go along with their use of technology.

Particularly, today's users must be educated as to how their growing reliance—and affinity for—Web 2.0 collaborative tools and applications and mobile devices that are not approved or supported by the enterprise pose significant security risks. Ongoing user education on security policies, technologies, and online threats, as well as clear guidance for meeting compliance measures, are essential.

Keep an eye on "old problems" while being vigilant about new risks. Unpatched or forgotten machines are those that will be infected first, giving attackers an "agent behind enemy lines" that can conduct inside-the-firewall attacks. Organizations must remember that a risk is a risk, and as criminals become more sophisticated and bold in their approaches, they will leverage an arsenal of techniques to carry out their attacks—even if the probability of any particular one being successful is low or remote.

Never underestimate the insider threat. The global recession has caused many individuals to lose their jobs—or face the prospect that they could be in the unemployment line soon. Meanwhile, employees who are spared layoffs may become disgruntled due to increasing workloads—and little or no relief or extra compensation for their stepped-up efforts or loyalty to their employer.

As a result, insider threats will be of increasing concern for organizations in the months ahead. Insiders not only could be current or former employees, but contractors or other third parties. Insiders pose a very serious threat, as they know how to exploit an organization's weaknesses, security policies, and technologies to steal data, intellectual property, or money—or simply, disrupt operations.

The importance of strong (and realistic) policies for protecting sensitive data. Today's organizations need to create progressive policies that encompass anti-malware, acceptable use policies, and data loss prevention, and that are designed to help ensure regulatory compliance.

IT must work directly with management and employees to create and implement relevant, flexible, user-friendly policies that can be practiced and enforced throughout all levels of the organization.

Cisco Security Intelligence Operations

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 that meet individual security threats or protect individual products do not provide sufficient security 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 assess and correlate Internet threats and vulnerabilities continuously. As threats continue to evolve, Cisco SIO will enhance the 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.

Cisco Security Intelligence Operations provides the highest level of threat correlation—enabling users to collaborate with confidence.

Report available for download at

www.cisco.com/go/securityreport

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

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

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**.

C02-512160-02 6/09