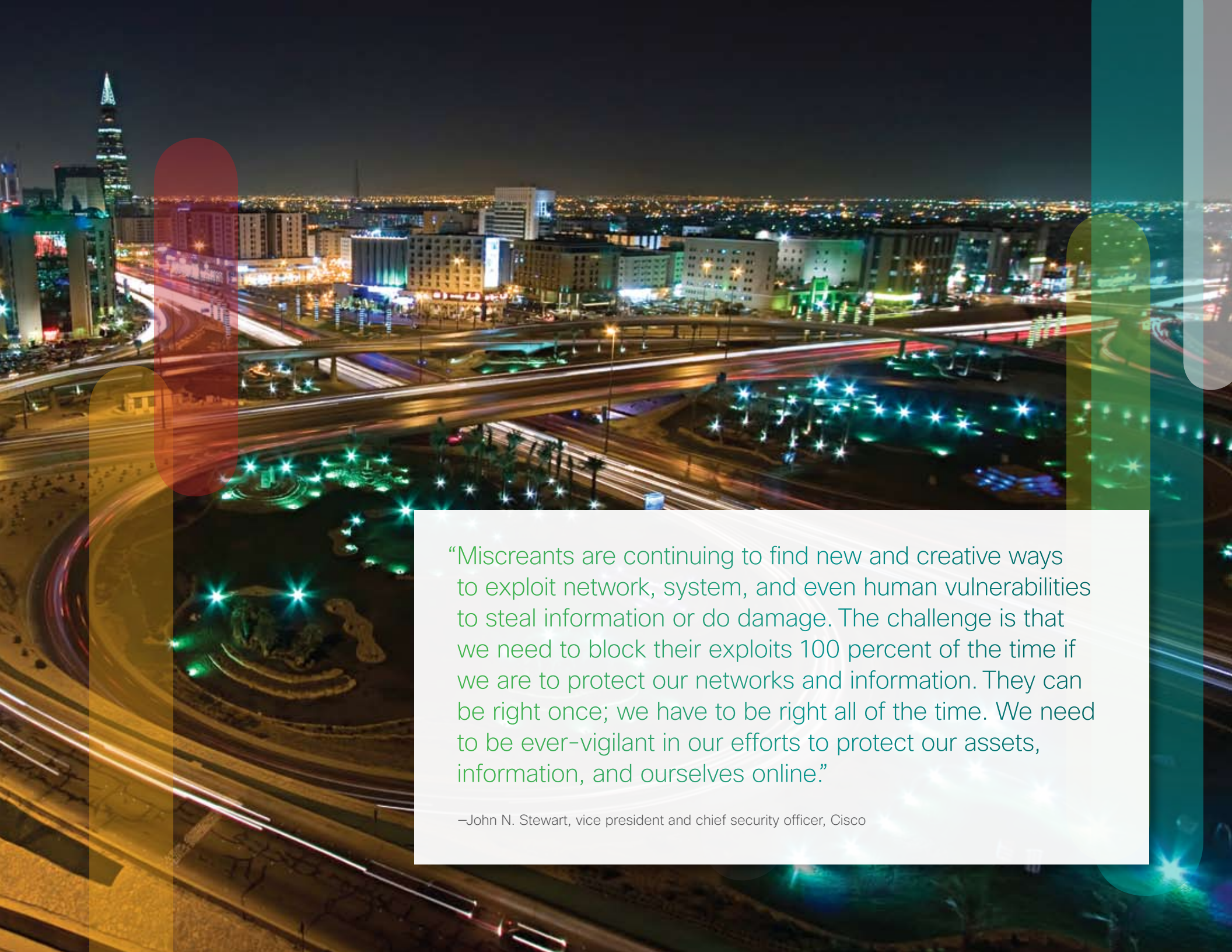
Cisco 2010 Annual Security Report

Highlighting global security threats and trends

The *Cisco® Annual Security Report* provides an overview of the combined security intelligence of the entire Cisco organization. The report encompasses threat information and trends collected between January and December 2010. It also provides a snapshot of the state of security for that period, with special attention paid to key security trends expected for 2011.

Contents



"Miscreants are continuing to find new and creative ways to exploit network, system, and even human vulnerabilities to steal information or do damage. The challenge is that we need to block their exploits 100 percent of the time if we are to protect our networks and information. They can be right once; we have to be right all of the time. We need to be ever-vigilant in our efforts to protect our assets, information, and ourselves online."

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

The Exploitation of Trust: Cybercriminals' Most Powerful Weapon

Whether they're creating malware that can subvert industrial processes or tricking Facebook users into handing over login and password information, today's cybercriminals have a powerful weapon at their disposal: the exploitation of trust. They have become skilled at convincing users that their infected links and URLs are safe to click on, and that they are someone the user knows and trusts. And with stolen security credentials, they can freely interact with legitimate software and systems.

When trust is exploited, more damage can be done with fewer intrusions—the criminal essentially has been given permission to wreak havoc on compromised systems and software. "Miscreants are continuing to find new and creative ways to exploit network, system, and even human vulnerabilities to steal information or do damage," says John N. Stewart, vice president and chief security officer for Cisco. "The challenge is that we need to block their exploits 100 percent of the time if we are to protect our networks and information. They can be right once; we have to be right all of the time. We need to be ever-vigilant in our efforts to protect our assets, information, and ourselves online."

People by nature are inclined to trust others, and criminals use this to their advantage again and again. Take the case of the fake social networking profiles established earlier this year for "Robin Sage," supposedly a young, attractive woman working in the national security arena. A security expert created the fake profiles as a test to see how many security professionals might be fooled by Sage's persona and share information with her. About 300 people within the United States military and government, as well as security companies, connected with "Robin." If even sophisticated security experts fail to think twice before exposing personal and corporate information to strangers, imagine what the average employee might do with your proprietary data. (Read more about the Robin Sage fake profiles on page 17.)

Hackers are also taking advantage of new opportunities to make money. In response to vulnerability exploits in various Windows PC operating systems, Microsoft has improved security in Windows 7 and taken a more aggressive approach to patching vulnerabilities. This makes it tougher for scammers to infiltrate Windows 7 effectively; having reached the Windows vulnerability "tipping point" (see page 30), they have moved on to other operating systems, applications, software services, and devices such as smartphones, iPads, and iPods. Apple and its products, including iPhones, iPads, and the iTunes media service, have all experienced upticks in exploits. Just as important in driving this trend is the embrace of mobile devices and applications by consumers and enterprises.

The worldwide adoption of mobile devices presents even more opportunities for intrusions and theft. While security researchers have identified many focused scams that target mobile devices, a widespread incident is almost certainly on its way. To date, scams have targeted select groups of mobile users, such as customers of a specific bank. The massive and relatively new market for mobile applications also offers new markets for criminals. Researchers have detected exploits in which wallpaper apps for Android Market, the app store for the Android mobile operating system, have been collecting mobile subscriber information and sending it to a website owned by a scammer.

Another type of exploitation involves "money mules"—individuals who help launder money by accepting and transferring funds earned in online scams. Money mules are sometimes criminals; more often, however, they are people in need of money who are tempted into this activity by "work at home" spam. Regardless of whether they are willing participants or unsuspecting victims, money mules are integral to enabling criminals to profit from their campaigns. Users can limit these operations by not becoming unwitting accomplices.

The subject of trust is also in play in the ongoing struggle of governments to work together to combat cybercrime. Governments recognize the need to develop common standards for security solutions, yet they also want autonomy over how technology is deployed within their borders. Some countries and companies are leading efforts to expand the reach of these common standards, since they present the best opportunity for improved security and continued product innovation.

Announcing the 2010 Winners of the Cisco Cybercrime Showcase

As you read the *Cisco 2010 Annual Security Report*, you'll find many stories about the bad guys whose craftiness and lack of morals have brought them to new heights of criminality this year. At the same time, the security industry is fortunate to have "superheroes" who work ceaselessly to bring down the evildoers and help us understand and combat criminal escapades. This year, Cisco is presenting two awards: one for "Good" and one for "Evil."

"The work of Thorsten Holz and his researchers highlights how vital it is for the academic, corporate, and legal communities to work together to weaken and flatten online criminal enterprises. This type of private-public partnership should be nurtured and supported to gain ground against increasingly sophisticated online criminals."

–Adam Golodner, director of global security and technology policy, Cisco

THE GOOD:
THORSTEN HOLZ
Ruhr-University Bochum/LastLine

If it weren't for researchers like Thorsten Holz, an assistant professor at Ruhr-University Bochum in Germany and senior threat analyst for security firm LastLine, we'd all be receiving a lot more spam. Up until mid-2010, a massive spam botnet known as Pushdo or Cutwail was responsible for sending as much as 10 percent of all spam messages worldwide. Then, Holz and his associates at LastLine—professors and graduate students from the technology departments of several leading universities—identified the 30 Internet servers used to control Pushdo/Cutwail, contacted the hosting providers, and urged them to take down the servers.[1] The result: After providers agreed to shut down 20 of the servers, spam dropped from an average weekday volume of 350 billion a day to 300 billion a day.

Just as dramatic was the takedown of the Waledac botnet, which at its peak in 2009 was delivering 1.5 million spam messages daily. In February 2010, Holz and several colleagues from academic and corporate institutions identified the almost 300 web domains controlled by the Waledac perpetrators and convinced a federal judge to grant an order against service providers to shut down these domains and transfer their ownership to Microsoft, thereby crippling the botnet.

THE EVIL:
STUXNET

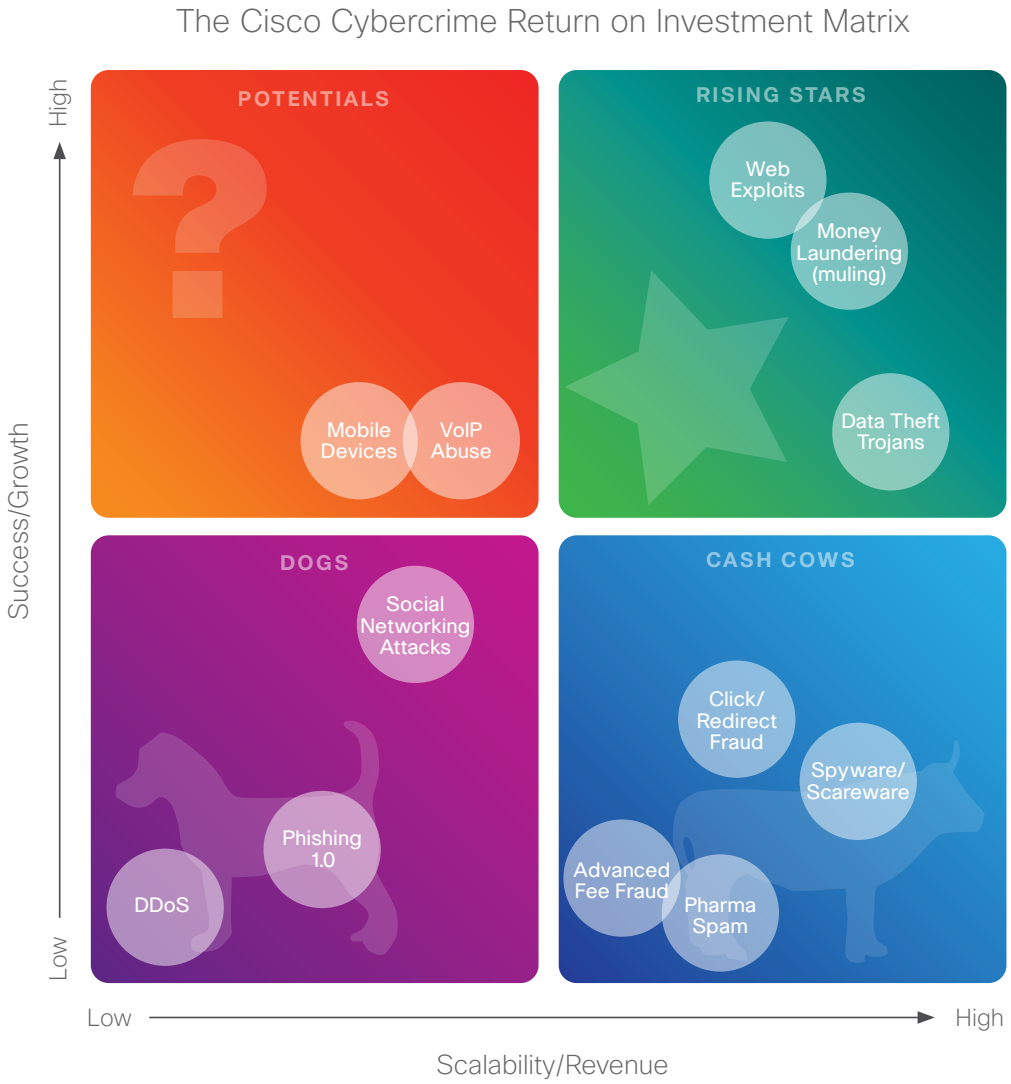
The Stuxnet worm, whose earliest versions appear to date to 2009, differs from its malware "cousins" in that it has a specific, damaging goal: to traverse to industrial control systems so it can reprogram the programmable logic controllers (PLCs), possibly disrupting industrial operations. It's not gathering credit card numbers to sell off to the highest bidder, and it's not selling fake pharmaceuticals—it appears to have been created solely to invade public or private infrastructure. (For more on Stuxnet, see page 21.) Stuxnet's cleverness lies in its ability to traverse non-networked systems, which means that even systems unconnected to networks or the Internet are at risk. Federal News Radio's website called Stuxnet "the smartest malware ever."

"Stuxnet bears watching in 2011 because it breaks the malware mold," advises Kurt Grutzmacher, network consulting engineer at Cisco. "Malware that is designed to disrupt industrial control systems in critical infrastructure should be a concern for every government." Fortunately, fixes are already available for the vulnerabilities exploited by Stuxnet—but Stuxnet is likely just the first in an expected long line of "hypertargeted" malware creations.

[1] "Researchers Kneecap 'Pushdo' Spam Botnet," Krebs on Security blog, August 27, 2010, http://krebsonsecurity.com/2010/08/researchers-kneecap-pushdo-spam-botnet/.

The Cisco Cybercrime Return on Investment (CROI) Matrix

Where will most cybercriminals channel their resources in 2011? Cisco security experts offer their predictions based on recent and emerging trends in the shadow economy.



The Cisco CROI Matrix predicts cybercrime techniques that will be "winners" and "losers" in 2011.

The Cisco CROI Matrix made its debut in the *Cisco 2009 Annual Security Report* and is used to track the performance of cybercrime operations, which increasingly are managed and organized in ways similar to sophisticated, legitimate businesses. Specifically, this matrix highlights the types of aggressive actions Cisco security experts predict cybercriminals are likely to focus most of their resources toward developing, refining, and deploying in the year ahead.

Cash Cows: As predicted in 2009, many cybercriminals were content to sit back and relax during 2010 and let road-tested techniques, such as scareware and spyware, click fraud, advanced-fee fraud, and pharma spam, help them make a profit. Expect to see these "cash cows" maintain their role as workhorses for cybercriminals during 2011—although spammers, particularly those responsible for high volumes of spam traffic, may need to be more cautious. Law enforcement agencies are taking action to address the global spam epidemic by targeting some of the most egregious offenders.

Dogs: As expected, instant messaging scams have dropped off the matrix, but now there's a newcomer among the Dogs: social networking scams, which ranked in 2010 as a wait-and-see moneymaker in the Potentials category. Cisco security experts predict that social networking scams will not be a significant area for cybercriminals to invest their resources in the year ahead. It's not that social networking scams are declining, but they are just a small part of a bigger plan—launching web exploits, such as last year's campaign to lure users of LinkedIn into downloading the Zeus Trojan (see page15). Thus, less up-front research and development are required for social networking scams. Criminals know they work.

Appearing again in the "Dogs" category are phishing 1.0 scams (unsophisticated attempts to steal user credentials and other sensitive information). So, too, are distributed denial of service (DDoS) attacks, despite some notable incidents this year. For instance, in late September 2010, a DDoS attack was launched by hacker website 4Chan against the Motion Picture Association of America's (MPAA) webpage. Dubbed "Operation Payback," the attack was retribution for the MPAA trying to halt the activity of websites that distribute copyrighted content and users who download illegal copies of movies. Film studios had reportedly paid Indian firm Aiplex Software to attack torrent websites in a similar manner.[2] And even in light of the recent spate of DDoS attacks against a number of companies that had cut off services to WikiLeaks.org following the nonprofit media organization's release of confidential U.S. government documents on its website, it is unlikely these types of attacks, which tend to be highly targeted and retaliatory, will be a major investment category for the general cybercrime community looking to make a profit in 2011.

Potentials: According to research firm IDC, the number of mobile devices—from smartphones to tablet PCs—accessing the Internet by 2013 will surpass 1 billion,[3] creating more opportunities for cybercrime (see The Tipping Point, page 30). The massively successful banking Trojan, Zeus—which, according to the U.S. Federal Bureau of Investigation (FBI), has played a key role in the theft of more than US$70 million from 400 U.S. organizations over the past several years—is already being adapted for the mobile platform.[4] In late 2009, SymbOS/Zitmo.Altr appeared; researchers believe it was designed to intercept confirmation SMS messages sent by banks to their customers. (Note: "Zitmo" stands for "Zeus in the Mobile.")[5] It appears the mobile malware, which users download after falling prey to a social engineering ploy, is designed to defeat the SMS-based two-factor authentication most banks use to confirm online funds transfers by customers.

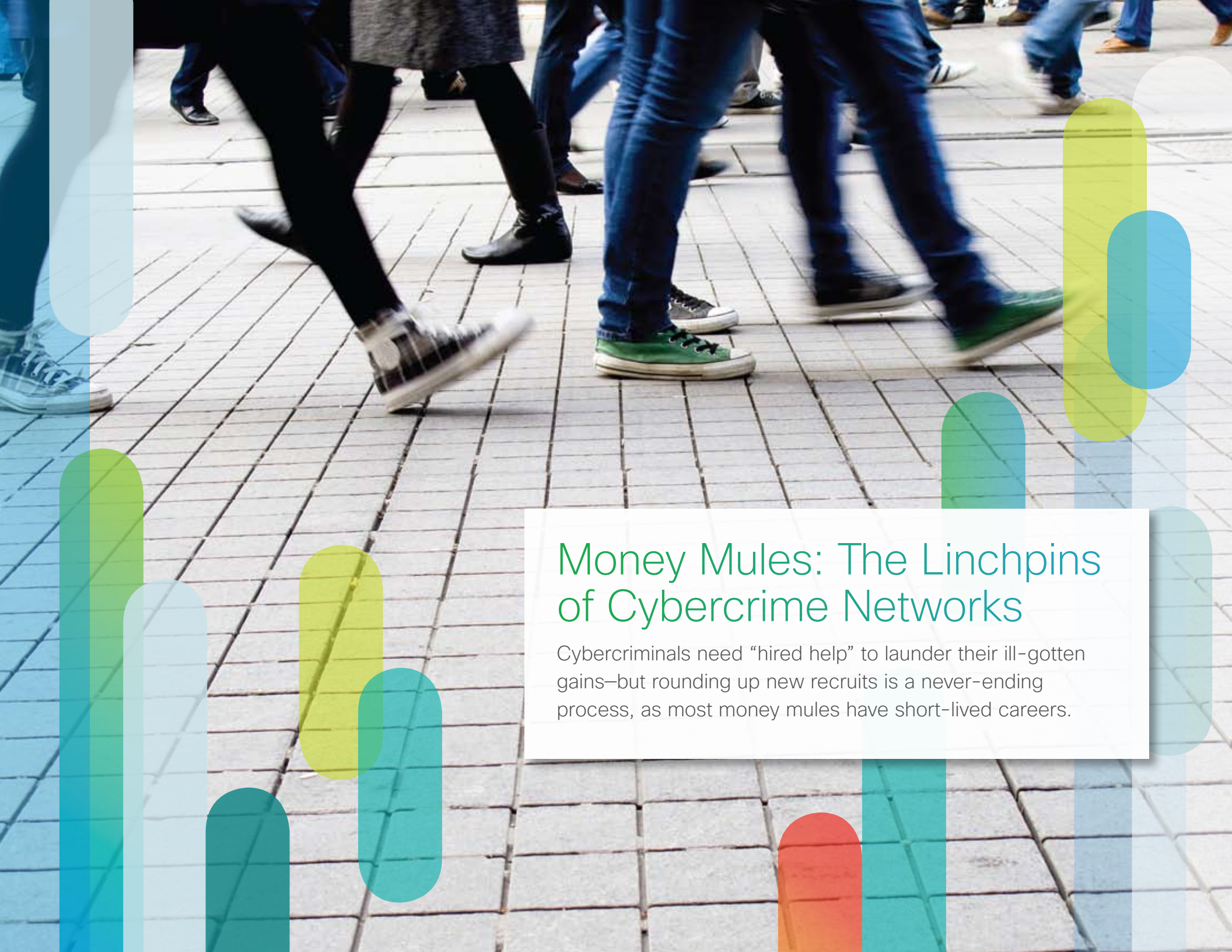
Meanwhile, VoIP abuse has been on the upswing and appears poised for further growth. Criminals use brute-force techniques to hack private branch exchange (PBX) systems to place fraudulent, long-distance calls—usually international. These incidents, often targeting small or midsize businesses, have resulted in significant financial losses for some companies. VoIP systems are being used to support vishing (telephone-based phishing) schemes, which are growing in popularity. In one recent vishing scam targeting the Federal Deposit Insurance Corporation (FDIC), vishers called U.S. consumers via mobile and land-line phones to inform them they were delinquent in loan payments that had been applied for over the Internet or made through a payday lender.[6] Criminals were able to collect personal information, such as Social Security numbers (SSNs), from victims.

Rising stars: The Zeus Trojan, and the entire field of lucrative, easy-to-deploy web exploits, like those seen in 2009 and 2010, will continue to receive significant investment from cybercriminals in 2011. The aptly named Zeus, which is powerful, pervasive, and targeting everything from bank accounts to government networks, has become extremely sophisticated and is much more customizable; as of October 2010, there were hundreds of different Zeus botnets known to security researchers. (See page 15 to learn about the recent Zeus exploit involving fake LinkedIn spam alerts, and page 23 for details on the Zeus-related fake Apple iTunes spam event.) However, the attention Zeus commands is making it easier for other highly sophisticated but less widespread Trojans such as Bugat, Carberp, and SpyEye to avoid detection. Also of note: In October 2010, Brian Krebs, who was spotlighted as a "Cybercrime Hero" in the Cisco 2009 Cybercrime Showcase, reported in his Krebs on Security blog that malware developers were merging the Zeus codebase with that of the SpyEye Trojan to create an especially potent threat for "a more exclusive and well-heeled breed of cyber crook."[7]

Cisco security experts anticipate that the real focus of cybercriminal investment for 2011, however, will be on improving the success and expanding the number of cash-out services ("money muling" operations). These operations, which have been discussed in previous Cisco security reports, are a vital component of the cybercrime lifecycle and are becoming more elaborate and international in scope. Zeus is often in the mix here, as well: See page 11 to read about its central role in a complex international money muling scheme operated by Eastern European gangs that was recently exposed by United Kingdom and U.S. law enforcement.

---

[2] "Film studios 'launch cyberattacks on torrent sites,'" by Emma Woollacott, TG Daily, September 9, 2010, www.tgdaily.com/games-and-entertainment-features/51458-film-studios-launch-cyber-attacks-on-torrent-sites.
[3] "IDC: 1 Billion Mobile Devices Will Go Online by 2013," by Agam Shah, CIO.com, December 9, 2009, www.cio.com/article/510440/IDC_1_Billion_Mobile_Devices_Will_Go_Online_By_2013.
[4] Graphic depicting global reach of Zeus: http://krebsonsecurity.com/wp-content/uploads/2010/10/globalreach.jpg.
[5] "Zeus Goes Mobile – Targets Online Banking Two-Factor Authentication," by Mike Lennon, SecurityWeek, September 27, 2010, www.securityweek.com/zeus-goes-mobile-targets-online-banking-two-factor-authentication.
[6] "Vishing Scam Hits FDIC," ConsumerAffairs.com, September 15, 2010, www.consumeraffairs.com/news04/2010/09/fdic_vishing_scam.html.
[7] "SpyEye vs. Zeus Rivalry Ends in Quiet Merger," by Brian Krebs, Krebs on Security blog, October 24, 2010, http://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/.



Money Mules: The Linchpins of Cybercrime Networks

Cybercriminals need “hired help” to launder their ill-gotten gains—but rounding up new recruits is a never-ending process, as most money mules have short-lived careers.

While online scammers have no difficulty stealing enough information to use their victims' credit cards and access their online bank accounts, they still need a way to get paid in the physical world, and thus, turn to money mules who facilitate money laundering. Money mules are individuals recruited by handlers or "wranglers" to set up bank accounts, or even use their own bank accounts, to assist in the transfer of money from a fraud victim's account to another location—usually overseas—via a wire transfer or automated clearing house (ACH) transaction.

One major hitch with any type of cash-out operation involving money mules is that there simply aren't enough mules in service. Mules typically work only one day before they are either abandoned by their handler or are taken into custody by law enforcement. As the cybercriminal economy continues to expand, it will be increasingly challenging for scammers to maintain an adequate supply of these temporary "employees" to profit fully from their exploits: One money mule expert estimates that the ratio of stolen account credentials to available mule capacity already could be as high as 10,000 to 1.

So, what type of people serve as money mules? They can be lower-level criminals willing to engage in a shady financial transaction to make some quick cash. Someone who is aware of his or her role as a money mule often believes that he or she is somehow "smarter than the average mule"—and therefore, will never be caught by authorities. Or, they do not believe what they are doing is that serious, and think, perhaps, "Well, what's the worst thing that could happen?" Not surprisingly, many money mules are caught quickly. Often, they face substantial fines—even jail time.

However, mules are quite often individuals seeking legitimate employment who end up being lured by too-good-to-be true job offers such as "Earn Thousands Working at Home!" Some ads, designed to appeal to people struggling with consumer debt, lure in victims with calls to action like, "Get Out of Debt Now!" These offers are often sent via spam, but some operations still advertise in the physical world with posters, flyers, and newspaper ads. People scouring employment ads on legitimate, well-known job search sites also have been duped by these scams. And given the challenging economic environment of the past few years, recruiters for money mules are likely finding their inboxes brimming with job application materials from potential candidates for hire.

Currently, the ratio of stolen account credentials to available mule capacity could be as high as 10,000 to 1.

Students are often targets for money mule recruiters, as are those simply looking for an "easy" way to make extra cash. A mule may be promised a monthly base salary, as well as a small commission (for example, US$50) per successful transaction. Some mules are told they can keep 5 percent per transaction, minus any wire transfer fees. As most mule handlers aim for mules to withdraw up to US$10,000 per transaction (amounts over that figure trigger a financial institution's anti-money laundering controls), the potential "earnings" are attractive. But even if they do make money in the short term, mules often pay a high price for their involvement in facilitating a crime: When a bank detects fraud, the mule, once identified by authorities, is often held responsible for repaying the money that was illegally transferred.

The more sophisticated cash-out organizations act as legitimate financial services firms. Individuals who come in contact with these operations usually have no idea they are being recruited as money mules, and believe they are dealing with a recruiter for a legitimate company. Quite often, they have responded to an ad on an online employment site for a position with a title such as "regional assistant," "company representative," or "payment processor." The contact the applicant interacts with online or by phone plays the role of human resources specialist, and when the victim inquires about vacation time, the availability of a 401(k) plan, or whether the "company" honors the U.S. Family and Medical Leave Act, they are provided a satisfying answer. As part of the "hiring process," mules are asked to provide sensitive information to the handlers, such as images of their government-issued identification.

Once hired, money mules are expected to work in a short time window—usually from around 9 to 11 a.m.—so that cash can be wired out of their account before a financial institution's security staff are able to respond to an incident of suspected fraud. (Mules also must own a cell phone; in fact, not having one is a deal-breaker. They won't get the job.) Mule operatives instruct mules to open two bank accounts: one for their "salary" and another for "funds." They also tell the mules to provide them with the online banking passwords for those accounts so they are able to check the balances. Mules are then asked to locate their local Western Union and Moneygram branches so that the cash-out process can commence; wire transfers, even though they require a fee to be paid up front by the sender, are typically very fast transactions, and don't require a bank account-to-bank account transfer.

It is not unusual for criminals to recruit dozens of money mules to stage just one large operation, or keep several on hand for repeat check-cashing and wire-transfer assignments. For example, one money mule recruitment and management website managed more than 4100 mules working in the United States during the course of a single year. Experts have noted that criminals, for reasons not entirely clear, prefer to hire East Coast residents when setting up money muling operations in the United States.

The following are examples of common cash-out systems that involve money mules:

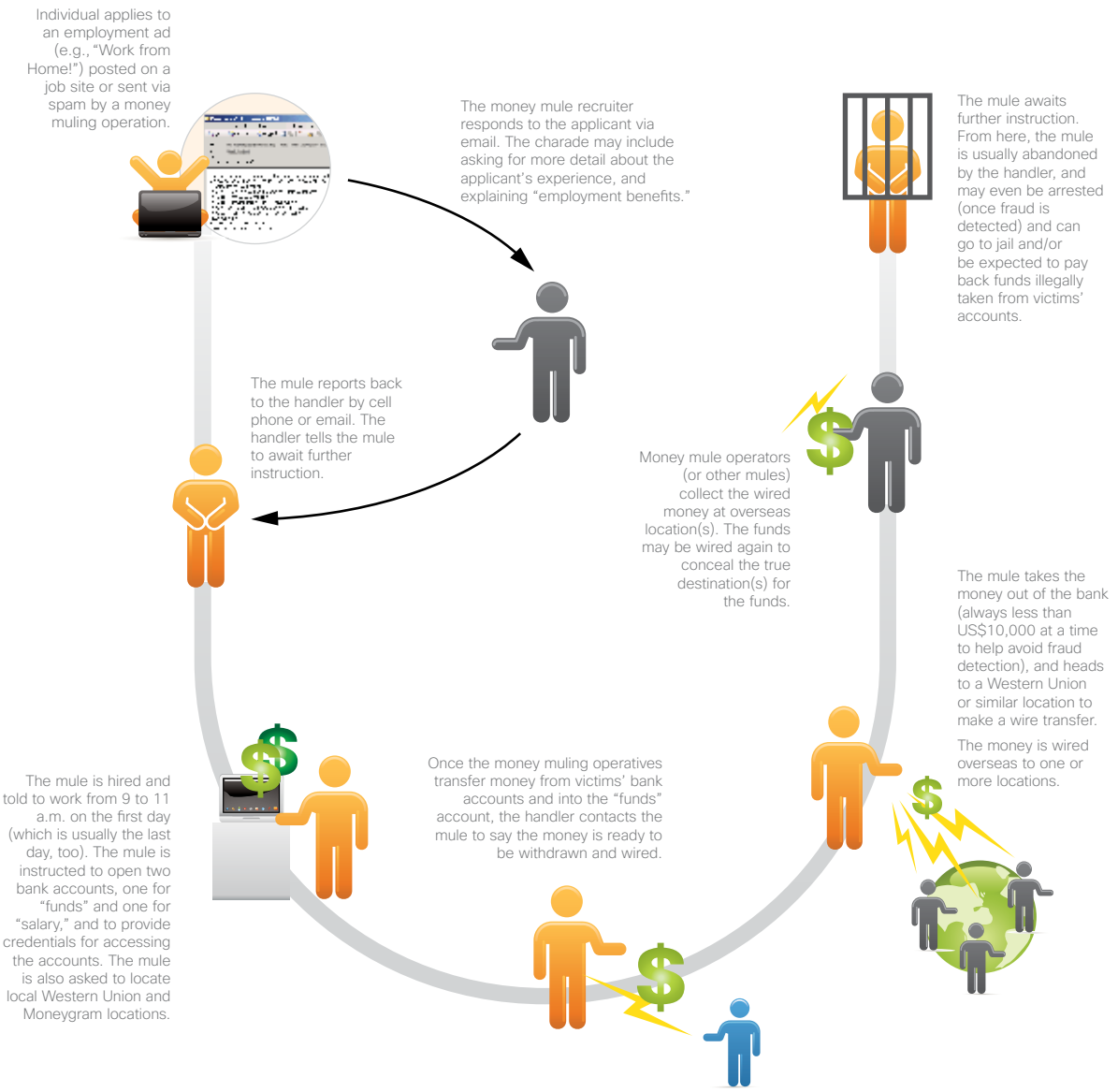
Operation 1:

Standard money is placed into legitimate in-country accounts via wire transfers (for example, Western Union) or ACH transactions. Mules are recruited to use their own accounts. Criminals move stolen money into these accounts. As an example, a mule conducts transactions at three or four Western Union locations, each time sending approximately US$3,000 by wire transfer to an overseas location. These wire transfers are often redirected after they are posted–using information the mule provided when he or she entered the mule organization, such as bank account information–so the mule doesn't know the true final destination for the funds.

Operation 2:

J-1 visa holders who obtain permission to work in the United States for short periods, such as for seasonal work, are recruited by money mule operatives in their country. While in the United States, the J-1 visa holders/money mules set up bank accounts in major metropolitan areas using bogus names and passports provided by their contacts. Information about money

A Day in the Life of a Money Mule



muling assignments is spread by word of mouth or through social networking, which is becoming an increasingly important tool for cybercriminals looking to spread their cash-out operations around the globe. An example of a money muling operation that targets J-1 visa holders is the Russian site "Work & Travel USA," which has a Facebook-like page with more than 50,000 "friends."

In September 2010, the U.S. Attorney's Office in Manhattan announced that it had charged 37 individuals from Russia and Eastern European countries—most of them in the United States on J-1 nonimmigrant visas—for their participation in a sophisticated scheme involving the Zeus banking Trojan and a team of money mules who stole funds from dozens of U.S. business accounts. The operation, which primarily targeted the bank accounts of small businesses and small municipalities, was code-named ACHing Mules because it involved unauthorized ACH transactions (see sidebar, "The Appeal of Automated Clearing House Transactions for Money Mule Operations" on page 12).

Earlier that same month, U.K. authorities charged 11 Eastern European citizens in connection with the same scam.[8] According to authorities, at least US$3 million was stolen from U.S. accounts from May to September 2010 through this specific money muling operation. In the United Kingdom, as much as US$9.5 million was siphoned from U.K. bank accounts. Money mules used units of Bank of America Corp. and TD Bank Financial Group to open accounts for laundering the money.[9]

Operation 3:

Because banks and credit card companies are becoming more adept at deterring fraud, some cybercriminals are turning to reshipping scams as a way to cash out. A scammer uses stolen or fake credit card or bank account information to purchase merchandise—usually, popular consumer electronics such as MP3 players, laptops, or flat-screen TVs—from e-commerce or auction sites. Since criminals obviously cannot send the goods to their own address, they rely on "shipping mules" to receive and forward the deliveries to foreign locations.

Social networking is an increasingly important tool for cybercriminals looking to spread their cash-out operations around the globe.

Mules participating in reshipping fraud may or may not be willing conspirators. But criminals have been known to prey on those who are looking for personal relationships online. They lure victims with overtures of friendship or romance communicated via email or instant messages—perhaps even sending nominal gifts as the "relationship" progresses. Over time, as the victim becomes convinced he or she has found a new best friend or a potential soul mate, the criminal begins to ask for favors.

Typically, scammers tell their victims that they cannot ship items they have purchased online directly to their home or business address in a foreign country due to some type of "legal" restriction. They ask the victim's permission to send the goods to his or her home, and offer to handle all of the shipping expenses.

Once the victim agrees to help, he or she quickly receives a flood of parcels containing the illegally purchased goods and is asked to repackage and send them to one or more locations outside the country. This may go on until the scammer's specific mission is complete, or until the victim grows suspicious (or weary of the reshipping process) or is visited by law enforcement and informed that the products being shipped outside the country were paid for with stolen or fraudulent credit cards.

---

[8] "Zeus Trojan bust reveals sophisticated 'money mules' operation in U.S.," by Jaikumar Vijayan, Computerworld, September 30, 2010, www.networkworld.com/news/2010/100110-zeus-trojan-bust-reveals-sophisticated.html.

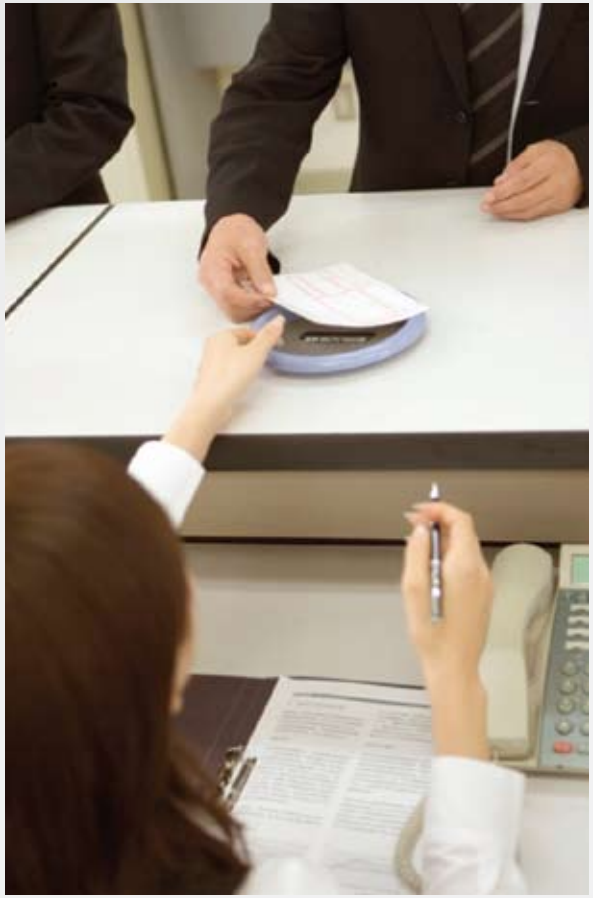
[9] "Accounts Raided in Global Bank Hack," by Chad Bray, Cassell Bryan-Low, and Siobhan Gorman, The Wall Street Journal, October 1, 2010, http://online.wsj.com/article/SB10001424052748704483004575523811617488380.html.

The Appeal of Automated Clearing House Transactions for Money Mule Operations

An automated clearing house (ACH) transfer takes more time to complete than a wire transfer (a day or more, versus minutes), but because the process is automated, ACH transactions are less expensive. In addition, larger amounts of cash can be transferred. And unlike a wire transfer, the identities of the sender and recipient are not verified, which makes them an even more attractive tool for criminals.

When an automated clearing house (ACH) transfer is initiated, all the information is sent in a "batch" to a clearing house, which then handles the transaction. When a financial institution attempts to reverse a transfer–which is not a quick and easy process to initiate–it is "all or nothing."

For example, if a fraudulent US$100,000 transfer is sent via an ACH transaction to a money mule's account, when the bank tries to reverse the US$100,000, if there is less than that amount in the account (maybe a mule has already started wiring some of the money overseas), the reversal fails.



The appropriate thing for the bank to do is to keep retrying with progressively smaller amounts until it succeeds in recouping at least a portion of the stolen money. However, many banks are not sophisticated enough to do this, and the money is lost.

That's not always the end of the story, though. More financial institutions are pursuing money mules after illegal ACH and wire transfers have been detected and holding them liable for funds lost. Mules often use their own bank accounts to help carry out the fraud, which makes them easy for authorities to trace. In addition, in the United States, the federal government is becoming more aggressive about tracking down and prosecuting mules–as well as their handlers.

An Offer You *Should* Refuse

If a money mule recruitment email arrived in your inbox, would you immediately know it was a scam? Maybe—especially if the email is poorly written and tells an outlandish tale. But if you are someone who is eager to make extra (and supposedly easy) income, and you have difficulty saying no—particularly when the person writing to you for help seems so friendly—then you might be more likely to believe an offer that sounds too good to be true is on the level. And you would not be alone.

In an October 2010 blog post for *The Huffington Post*, Cisco senior security advisor Christopher Burgess shared an example of a money mule solicitation he recently received in his own email inbox.[10] The "work online from home" offer seeking a U.S.-based representative/online bookkeeper for a U.K. fabric company indicates that the supposed employer, Owen Geven, is willing to pay 10 percent for every payment from a client that is processed through the representative (who apparently needs no bookkeeping experience whatsoever to handle this important job).

Emails like the one below that are used to attract money mule candidates feature telltale signs that can help targets recognize a scam is likely afoot. Burgess outlined several of these warning signs in his recent blog post[11]:

- You are told to "keep this offer secret"
- You are asked to "respond to this offer right now"
- You are informed the company needs protection from taxes associated with international sales remittance
- You are asked to spend your money
- You are requested to open or provide any information associated with your bank account(s)

From: Owen Geven ([redacted])
To: Christopher Burgess ([redacted])
Subject: Work Online From Home!

My name is Owen Geven, a designer and also the Manager of Owen Geven Fabric and Consultant and I live and work here in United Kingdom, Would you like to work online from home and get paid without affecting your present job? Actually I need a representative who can be working for the company as online book-keeper. We make lots of supplies to some of our clients in the EUROPE/USA/CANADA, for which I do come to USA/CANADA to receive payment and have it cashed after I supply them raw materials. It's always too expensive and stressful for me to come down and receive such payment twice in a month so I therefore decided to contact you. I am willing to pay you 10% for every payment receives by you from our clients who make payment through you. Please note you don't have to be a book keeper to apply for the job. Kindly get back to me as soon as possible if you are interested in this job offer with you're:

1. FULL NAMES..... 2. ADDRESS (not P.O.box).....
..... 3. STATE..... 4. ZIPCODE.....
5. COUNTRY..... 6. PHONE NUMBER(S).....7. GENDER.....
8. AGE..... 9. OCCUPATION.....

PLEASE SEND YOUR REPLY ASAP TO: ([redacted])

[10] "Use Horse Sense, Don't Be a Mule," by Christopher Burgess, The Huffington Post, October 27, 2010: www.huffingtonpost.com/christopher-burgess/use-horse-sense-dont-be-a_b_774340.html.
[11] Ibid.

Social Engineering: Taking Advantage of Trust

Criminals continue to take advantage of the high levels of trust that users place in social networking services. They often exploit this trust by masquerading as someone the user knows.

As discussed in the introduction, exploitation of trust is now an essential tool across all sectors of cybercrime. Nowhere is this tactic more widespread than within social networking, where it continues to attract victims who are willing to share information with people they believe are known to them.

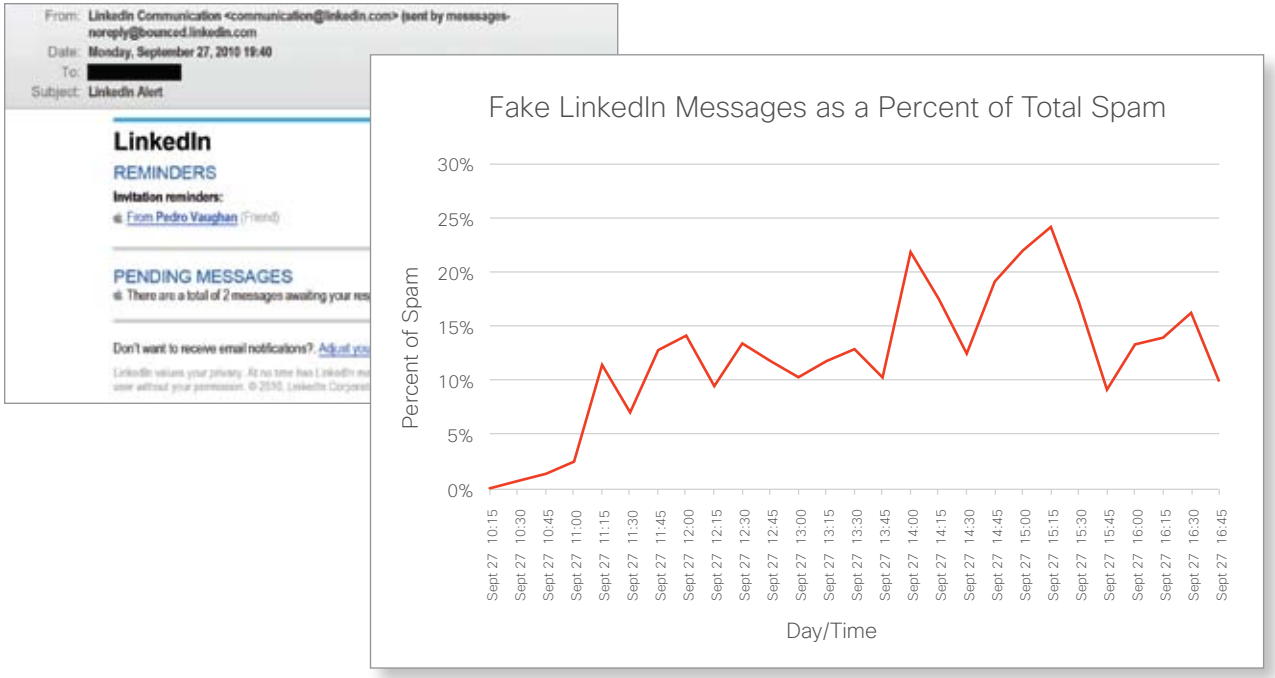
One noticeable shift in social engineering is that criminals are spending more time figuring out how to assume someone's identity, perhaps by generating emails from an individual's computer or social networking account. A malware-laden email or scam sent by a "trusted person" is more likely to elicit a clickthrough response than the same message sent by a stranger. Koobface malware, which first appeared on Facebook in 2008, uses this tactic, sending messages to friends of an infected Facebook user and convincing them to download the malware. (See the sidebar on page 18 for more about the evolution of the Koobface botnet.) And in October 2010, a freelance web developer created Firesheep, an extension for the Firefox browser that allows someone on an unsecured wireless network to hijack another wireless user's Facebook or Twitter account.[12]

As Cisco has discussed in previous security reports, users of social networks continue to place high levels of trust in information they (supposedly) receive from other members of these networks, or what seem to be official messages from these networks. Knowing this weakness, scammers are naturally directing more of their spam messages at social network users, employing social engineering tactics to drive necessary clickthroughs and malware downloads.

In September 2010, spam emails that were purportedly from business social networking service LinkedIn were sent worldwide and contained fake reminders. If the recipient clicked through on any links contained in the message, their computer became infected with Zeus data-theft malware, which captures personal banking information.

The scale of this particular spam operation was daunting: On the day the messages were sent, they numbered in the billions and accounted for 24 percent of spam messages worldwide. While this has been the largest outbreak of social networking-related spam to date, it's not the first: The Cutwail botnet, which was first detected in 2007, routinely sends emails that try to convince recipients that they originate from social networks.

The LinkedIn spam operation is worth noting and watching in the future because of the high volume of messages delivered, as well as the fact that supposedly savvy business users (presumably, higher-value targets) were targeted and that Zeus malware was used to steal personal login data. "The LinkedIn spam campaign strongly suggests that its perpetrators are most interested in employees with access to financial systems and online commercial bank accounts. According to the FBI's Internet Crime Complaints Center, in 2009, more than US$100 million was stolen from commercial bank accounts using methods like this," explains Nilesh Bhandari, product manager at Cisco. "The scammers are targeting the professionals who used LinkedIn, not people who frequent MySpace or Facebook. Organizations should encourage people to be suspicious of any email that purports to be from a legitimate source, but appears slightly different than they might expect."



In September 2010, spam messages lured recipients into clicking on links in fake LinkedIn notifications that infected their computers with Zeus malware.

[12] "Firesheep Firefox extension opens fire on sheep-browsers," Computerworld.com, October 26, 2010, http://blogs.computerworld.com/17228/firesheep_firefox_extension_opens_fire_on_sheep_browsers.

Spammers Get Social

Spammers are not only spoofing social networking messages to persuade targets to click on links in emails—they are taking advantage of users' trust of their social networking connections to attract new victims. As communications shift from traditional email and toward the messaging features used in social networks, such as those provided by Facebook and LinkedIn, criminals follow closely behind.

One tactic is to lure individuals into "liking" a particular Facebook page, claiming that the user will see a shocking photo or read a dramatic news story. Once the user has clicked on Facebook's "Like" button for that page, its creator can now email the user to click on other links (perhaps to malware), and can also see the user's personal information, if they have made it viewable for other friends. Another tactic is to send out fake friend requests, which frequently include a picture of an attractive man or woman. If the recipient decides to view this supposed person's Facebook page, they will usually find only a single post, which links to some type of scam.

How to Educate the "Problem Users"

Since people are the weak point in forming a defense against socially engineered scams, user education must be ongoing and effective. However, in spite of many organizations' best efforts to teach workers to exercise caution when responding to emails or social network messages, social engineering continues to be a highly successful method for cybercriminals.

The problem may be that there is a small but significant group of users for whom safety messages do not resonate. Clickthrough rates for most malware or spam incidents consistently hover at around 3 percent, according to data from Cisco ScanSafe. While 3 percent may not seem high, imagine the impact of repeated waves of spam to which 3 percent of workers consistently respond to and click on. Even this small percentage is the equivalent of having a gaping hole in the network firewall that cannot be closed. Instead of trying to change human behavior, security researchers are exploring the possibility of changing the way we use software to reduce risks.

Scammers trick social network users into "liking" an intriguing Facebook page, allowing the scammers to see user profiles.

For instance, all computer users are conditioned to click on dialog buttons to initiate certain actions. Scammers can simply design their schemes so that malware is delivered, or the user is redirected somewhere else, by encouraging clicks. "Because of this automatic behavior, user awareness campaigns based on the idea of not clicking on suspicious links or downloads don't have a lot of impact," says Gavin Reid, Cisco computer security incident response team manager. "We can't fix this problem with training—we need to fix it with software that the end user can operate with confidence."

A tougher solution may be to establish harsher penalties for workers who consistently ignore directives from IT about social engineering—for instance, isolating or "sandboxing" problem users from network access until they receive remedial training. The hardest-to-reach users may not fully understand the impact of their actions, and they may not have compelling reasons to change their behavior. In addition, organizations need to measure the efficacy of their education programs—there's no point investing time and money in training that consistently misses the mark.

Also on the horizon are tighter controls on how workers use social networks like Facebook. Security solutions that allow businesses to fine-tune how individuals navigate around a social networking site, and what information they can post and share, already are on the market.

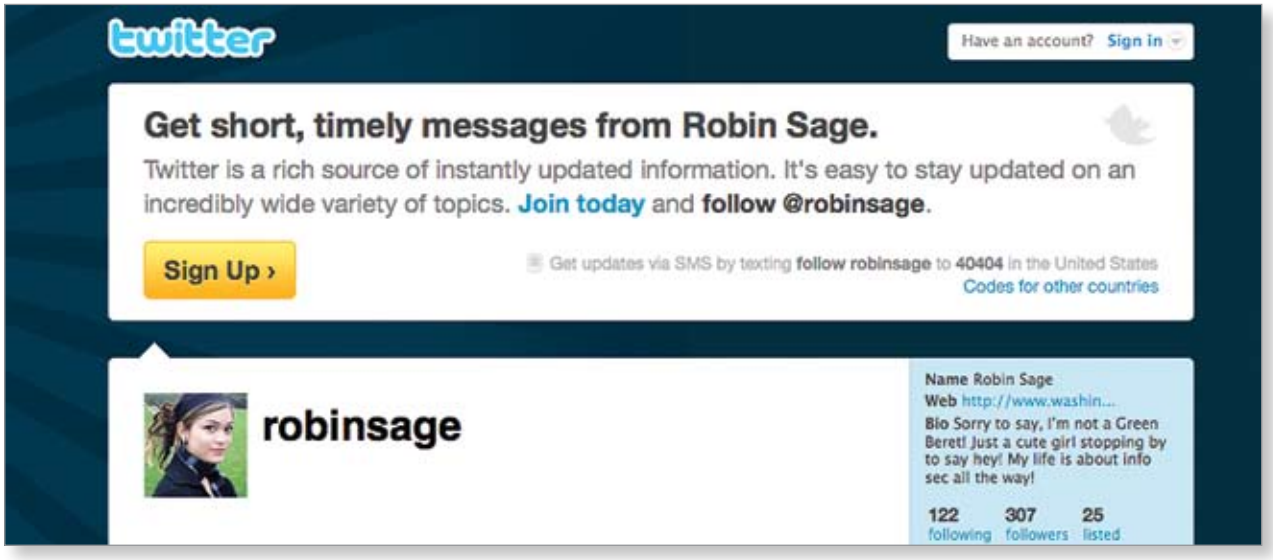
In users' defense, not all of the problems associated with safe navigation of social networking stem from user ignorance. Facebook's frequent changes to its privacy and security settings can confound even the most expert social networker, making it challenging to know when and if one is truly shielding private information.

Fake Profiles: Enabling Access to Personal Information

Instead of hacking into private social networking profiles, why not have your targets willingly show you the personal information you need? The potential success of such a strategy was highlighted at the beginning of 2010, when Thomas Ryan, founder of the firm Provide Security, created fictitious profiles on Facebook, LinkedIn, and Twitter for a woman named Robin Sage.

Sage was described as woman in her 20s with a degree from the Massachusetts Institute of Technology who analyzed cyberthreats for the U.S. Department of the Navy. Her profile included a picture of an attractive young woman as an additional lure. "Robin" quickly made connections with about 300 people in the U.S. military, government agencies, security companies, and government contractors.[13] According to DarkReading.com, the fictitious woman was offered jobs by several firms, including Lockheed. Some of Sage's connections said they determined fairly quickly that the social networking pages were fakes; on the other hand, Sage's profiles continued to rack up high-level connections until Ryan took them down in January 2010, a month after creating them.

The lesson of Ryan's experiment for security experts and all employees is that within social networks, even users who think they are exercising caution by locking up information against people who aren't members of their social networks can be put at risk by the careless acceptance of connection or friend requests.



The fake "Robin Sage" Twitter account was intended to attract highly placed officials within government and security.

The old adage, "If it sounds too good to be true, it probably is," should be put into play when it comes to responding to social networking connection requests. A pretty young woman whose resume sounds a bit too advanced for her age, and who quickly amasses hundreds of friends, should raise suspicion—much the same as a message from a supposed celebrity, or an alert that you've won a prize, should be viewed with skepticism. In many ways, social network exploits borrow the same tried-and-true tactics used by scammers for decades.

The old adage, "If it sounds too good to be true, it probably is," should be put into play when it comes to responding to social networking connection requests.

[13] "'Robin Sage' Profile Duped Military Intelligence, IT Security Pros," DarkReading.com, July 6, 2010, www.darkreading.com/insiderthreat/security/privacy/showArticle.jhtml?articleID=225702468&cid=RSSfeed_DR_News.

The Evolution of Koobface: Adapting to the Changing Security Landscape

The Koobface botnet, which first hit Facebook and MySpace in July 2008 and convinces victims to download malware that can steal credit card data, is a textbook example of the creativity and ingenuity of cybercriminals. As methods of detecting and blocking the Koobface malware were developed, and as new ways to monetize the botnet were needed, Koobface's creators became adept at adapting their invention to new scenarios. We can expect similar levels of innovation from today's cybercriminals.

"The Koobface operator has been forced to creatively adapt his botnet in order to circumvent efforts by the security community to eliminate it. By watching Koobface's evolution, we can gain insights into the protective mechanisms that may be the baseline of future botnet families."

—Henry Stern, senior security researcher, Cisco

Below is a chronology of Koobface's most significant milestones from the paper *Koobface: The Evolution of the Social Botnet*, co-authored by Cisco security researchers and researchers from the University of Alabama at Birmingham.[14]

August 2008, spoofs URLs: In the first week after Koobface launched, the URLs in the messages delivered to potential victims were modified to appear innocuous. For instance, the prefix of the URL might have been changed to begin with www.google.com to make users think the link led to Google. In addition, the domains were part of a "Fast Flux" network, in which domain name system (DNS) settings are rotated so that the IP address resolving to the hostname is changed, which complicates investigations.

September 2008, reroutes traffic: Koobface adds a new executable, tinyproxy.exe, which allows Koobface operators to route traffic through their own nodes instead of another Fast Flux infrastructure. This meant they removed their dependence on a third-party infrastructure, saving them money and giving them more control over their "product."

December 2008, expands to other sites: Koobface expands the sites on which it could operate to other social networks, including Bebo and Friendster. The list expanded again in March 2009 to include such sites as LiveJournal, NetLog, and Tagged.com.

March 2009, adds spam as delivery vehicle: Koobface begins to be delivered via spam campaigns instead of just social networks.

July 2009, shows up on Twitter: Koobface surfaces on Twitter, no doubt because the shortened URLs commonly posted by Twitter users would mask the offending Koobface URLs.

July 2009, changes DNS servers: Koobface adds a DNS changer, which changes the victim's DNS server to one controlled by the criminal, allowing them to hijack any hostname they want. For example, if a victim tried to log in to their online bank account, they could be redirected to the scammer's own server.

August 2009, redirects search engine results: Koobface adds a new way to monetize itself by adding search engine result redirection on infected computers. Victims were redirected to various ad affiliate sites before finally landing on the sought-after page.

August 2009, adds reputation hijacking: Koobface avoids "bad reputation" filters by using sites with a good reputation, such as blogspot.com, as its advertised destination so that users felt comfortable clicking on the link. However, these pages were created by the malware itself.

December 2009, creates fake malware warnings: Koobface creates a warning about downloading malware that appeared to originate from Facebook itself—but the link for the so-called "Facebook Security Update" executed the Koobface malware.

December 2009, hacks CAPTCHA protections: Social networking sites add CAPTCHA tests for users who post URLs. Koobface dodges this protection by sending the CAPTCHA to other computers that are part of the botnet, and directing an unsuspecting user to enter the CAPTCHA information to prevent their Microsoft Windows operating system from shutting down.

[14] *Koobface: The Evolution of the Social Botnet*, by Brian Tanner and Gary Warner, The University of Alabama at Birmingham; and Henry Stern and Scott Olechowski, Cisco Systems, October 2010.

Social Engineering: The "Seven Deadly Weaknesses" That Criminals Exploit

Like athletes and chess players, cybercriminals are skilled at identifying their targets' weak points. Social engineering offers a host of techniques for preying on potential victims and their weaknesses, fooling them into downloading malware or paying for sham pharmaceuticals or anti-virus programs. Following are seven weaknesses that workers need to watch if they want to avoid falling prey to social engineering scams—whether they take the form of emails, social networking chats, or phone calls.

"Compassion and urgency are common social engineering hooks for criminals. The individual seeking information will attempt to trigger the target's basic human need to be helpful. The individual will also infuse a sense of urgency in their quest for information or specific action, with the expectation that you won't have sufficient time to verify their credentials."

—Christopher Burgess, senior security advisor, Cisco

1 Sex Appeal

Scammers will try to tempt users into action by masquerading as an attractive man or woman, particularly on social networks. People should assume that a flirtatious advance from someone they don't know has a less-romantic purpose behind it.

2 Greed

As stated in the section on fake Facebook profiles (page 17), if something is too good to be true, it probably is. People considering free iPod offers, or a percentage of a Nigerian wire transfer, need to resist the urge to make a deal.

3 Vanity

Scammers will try to convince potential victims that they have been chosen, that they're winners, or that they are somehow part of a select group to be on the receiving end of an exclusive offer. Users should assume they're not that special.

4 Trust (implied or transient)

In scams involving implied trust, cybercriminals attempt to convince individuals that they represent a high-profile brand and therefore can be trusted. The recent spam campaign involving fake Apple iTunes purchase receipts (see page 23) is an example. With transient trust, scammers pretend to be a trusted companion of someone who the user trusts—therefore, the trust relationship extends to the unknown person. Users should be taught to question any message or phone call that plays on a trust relationship.

5 Sloth

Criminals rely on user laziness to ensure that poorly written messages and shortened URLs don't rouse suspicion. For instance, users will often click on a link in an email that is supposedly from their bank, instead of calling the bank or visiting the bank's website to determine if the email is legitimate. Or users who receive messages from business contacts on Facebook or LinkedIn will click on a link that supposedly offers a video of a Hollywood starlet—instead of questioning why a colleague would send such a link.

6 Compassion

In 2009, one of the most successful scams on Facebook involved criminals hijacking users' accounts, then posting status updates claiming that the account holder was stranded somewhere and needed money. Many kindhearted people fell for this ploy. Other similar scams involve requesting donations to nonexistent nonprofits when a major disaster occurs, such as the earthquake in Haiti. Users should maintain a high level of skepticism toward these types of messages.

7 Urgency

Hand-in-hand with compassionate pleas are scams that insist on a fast response and tell the potential victim to "act now" or that "time is running out." These requests don't come only via email or the web: Workers may receive phone calls from individuals who claim they need login information or company files sent to them right away. Users should double-check any such request with a colleague, and not feel pressured to respond immediately.

For more information about creating a Security Education Program at your organization, visit www.cisco.com/web/about/security/cspo/awareness/index.html.

Risks and Vulnerabilities: The Most Lucrative Targets

Creative cybercriminals are fine-tuning their exploits to achieve specific goals or steal from particular targets. They're also combining several scam tactics to boost their chances of success.

The earliest cybercriminals specialized in casting a wide net to find targets for their schemes. Poorly written spam messages, sent out by the millions, were aimed at any and all possible email addresses. Most of these messages are now caught by spam filters, but a small fraction of recipients will still click through to download malware unwittingly or decide to order nonexistent pharmaceuticals.

While broadly aimed spam still appears to be an effective tool, cybercriminals are seeing value in fine-tuning their efforts so that their malware reaches a single high-profile target or performs a specific function. The newest twist in "hypertargeting" is malware that is meant to disrupt industrial systems—such as the Stuxnet network worm, which exploits zero-day vulnerabilities in Microsoft Windows to infect and attempt to tamper with very specific industrial systems, such as supervisory control and data acquisition (SCADA) systems.

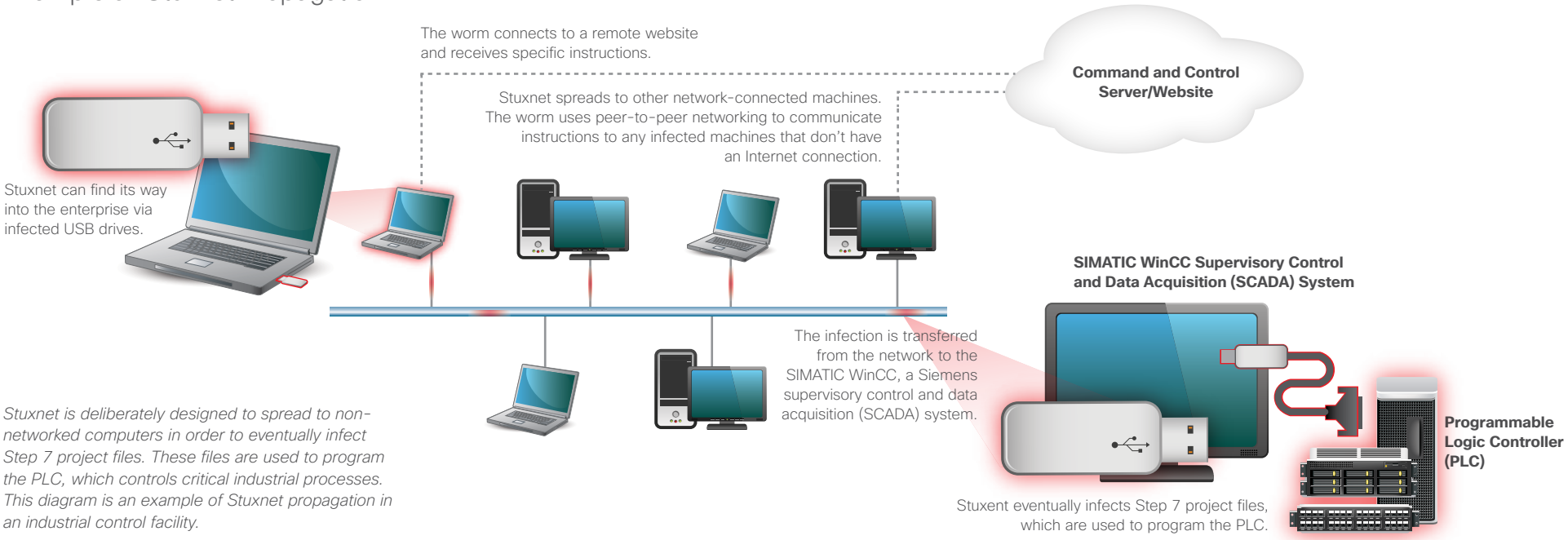
While components of Stuxnet date back to 2009, the worm in its complete form was initially detected in June 2010. The first known copy of the worm was discovered in a plant in Germany. A subsequent variant led to a widespread global outbreak.

The appearance of Stuxnet is sobering for several reasons, not the least of which is the worm's potential to severely disrupt critical infrastructure. Stuxnet seems to have been designed to deflect remediation and response actions from security professionals. Operators believed that a default Siemens password (which had been made public on the web some years earlier) could not be corrected by vendors without causing significant difficulty for customers. The SCADA system operators may have been laboring under a false sense of security that since their systems were not connected to the Internet, they would not be prone to infection.

Stuxnet's built-in features exploit both technical and operational trusted relationships—for instance, the malware used stolen security certificates, fooling other systems into believing it was a legitimate piece of programming. Stuxnet has already been studied extensively, and much has been revealed about its inner workings—providing a blueprint of sorts for future such campaigns, and educating criminals on how exactly to create these exploits themselves.

"Stuxnet showcases the determination, resources, and dangerous intent of today's cybercriminals," reports Mary Landesman, senior security researcher at Cisco. "Stuxnet raises the already alarmingly high bar of data and intellectual property theft to an entirely new level—sabotage of our critical infrastructure."

Example of Stuxnet Propagation



Stuxnet is deliberately designed to spread to non-networked computers in order to eventually infect Step 7 project files. These files are used to program the PLC, which controls critical industrial processes. This diagram is an example of Stuxnet propagation in an industrial control facility.

Advanced Persistent Threats Take Targeted Approach

Advanced persistent threats (APTs) have also adopted the hypertargeting approach. Over the past several months, the definition of an APT has shifted, particularly since the term has become a catchall definition for any kind of serious cybercriminal threat.

In the *Cisco 2010 Midyear Security Report*, APTs were defined as attempts to infiltrate networks via a "low-and-slow" approach—that is, threats that lurk within a network and remain undetected so that they could steal information over an extended period of time. This year, "APTs are more accurately defined as a threat that is highly targeted toward specific individuals or with a dedicated mission in mind," clarifies Rod Bachelor, senior product manager at Cisco. "Those who create APTs are going after people based on their access to information, such as intellectual property, that can be monetized. These targeted attacks often use the same software used in conventional attacks, which can make them harder to distinguish."

APTs are using social engineering to get a foot in the door of networks—like all other areas of cybercrime, APT creators are exploiting trust to lure users into downloading malware payloads. For instance, an APT operator might leverage LinkedIn to locate names of relevant staff at a targeted organization—likely people who have access to administrative passwords. The APT operator then crafts a message to these targets, designed to persuade them to follow a link to malware. This socially engineered approach can offer an easier entry path than exploiting network vulnerabilities.

The methods for detecting and thwarting APTs remain the same as those discussed in the *Cisco 2010 Midyear Security Report*: multilevel defenses that involve reputation scoring, consistent patching against vulnerabilities, and ongoing examination of outbound traffic. These defenses also include educating users on the specific threats or malware being aimed at the organization or industry, educating users on how to navigate the Internet safely, protecting critical and confidential data, only providing "need to know" access to information and data, and, in general, preventing and fending off social engineering campaigns (see "Seven Deadly Weaknesses," page 19).

Organizations that are familiar with APTs often baseline legitimate business traffic to more easily identify traffic that is malicious—or at least different from legitimate traffic. Correlating alerts and log messages from network and security devices may help as well.

Java and PDFs: Widely in Use, Heavily Exploited

Cybercriminals aim their campaigns at software programs, devices, and operating systems where they can reach the widest net of potential victims, as demonstrated by the noticeable increase in exploits involving the Java programming language—and the ongoing use of PDF documents to launch exploits. At this point, Java appears to be the greater threat.

The flaws in Java have made it a promising target for criminals—for instance, the Blackhole, Crimepack, and Eleonore exploit software packages, which are created by and sold to other criminals, make heavy use of Java.[15] The latest exploits based on Java have certain characteristics that make them worrisome from a security standpoint. These exploits are:

- **Evasive:** The most reliable detection for Java exploits is to run the exploits on a virtual machine, and then monitor the systems for security violations—however, this approach is prohibitively resource-intensive for most organizations. Enterprises need security solutions that can intercept and detect exploits on any device, regardless of whether they are on the network (such as mobile devices using Java).
- **Pervasive:** Java works in the background; for the most part, users are not aware that it is running or whether they've updated it recently. Therefore, it's not difficult for scammers to configure malware to check for older versions of Java during exploits.
- **Invasive:** Multiplatform interoperability is a hallmark of Java. While this is largely a benefit, it also makes it easy to distribute malware across several platforms, as well as any devices that run Java.

When it comes to PDFs, organizations rely heavily on these documents to conduct business, so the idea of limiting their use within corporate networks is seen as impossible. Yet Adobe Reader and Acrobat continue to be strong threat vectors online, even though such exploits are on the decline. It's the rare business or personal computer that doesn't have the Adobe Reader software for viewing PDFs, and computer users continue to place an undue amount of trust in these documents.

In September 2010, security researchers detected a zero-day exploit in which PDF documents were used to deliver a malicious file with a valid (but stolen) VeriSign signature for a credit union. The valid signature allowed the exploit to bypass two important defenses in the Microsoft Windows operating system.[16] The infected PDFs were delivered in emails touting advice from prominent golfing coach David Leadbetter, and they prompted the recipient to open the PDF for more golf tips.

[15] "Java: A Gift to Exploit Pack Makers," Krebs on Security blog, October 11, 2010, http://krebsonsecurity.com/2010/10/java-a-gift-to-exploit-pack-makers.
[16] "Do the Recent Viruses Have Specific Targets?" PCWorld.com, September 11, 2010, www.pcworld.com/article/205292/do_the_recent_viruses_have_specific_targets.html.

Once again, trust exploitation was at work, with a message aimed at golf-friendly executives who would presumably be eager to improve their game. The use of a stolen digital certificate was also designed to fool networks into trusting that the file was safe. In addition, it appeared that the Leadbetter emails were aimed at major corporations, so the infected PDF's creators may have been targeting high-profile individuals.

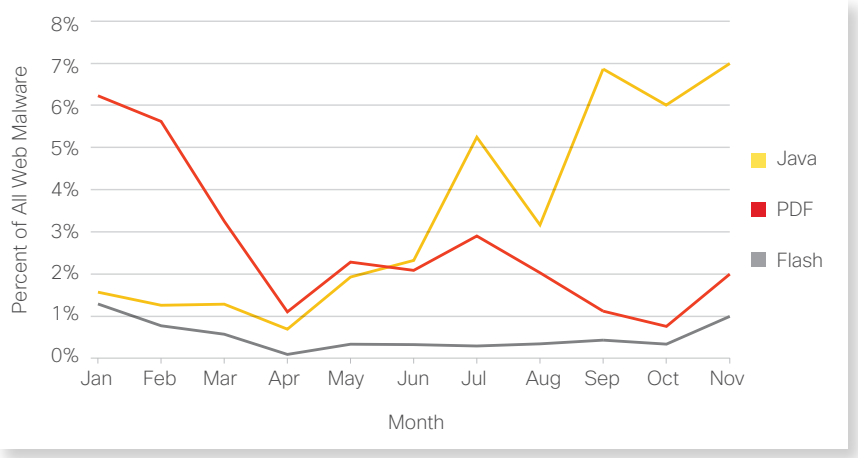
Until Adobe Acrobat and Reader become less vulnerable to such exploits, IT departments can either raise awareness among users about downloading PDFs from unknown senders, or take steps to block PDF downloads completely within their networks. If a blanket block of PDFs is not possible, network administrators can choose to disable JavaScript in Adobe Reader and Acrobat, and not allow PDFs to be launched automatically via the web. Security researchers are reacting in many ways to the prolific rise in PDF threats, even going as far as suggesting an alternative to PDFs.

In mid-2010, in response to the growing use of PDFs as launching pads for threats, Adobe announced that it would include a security improvement in the next major release of Adobe Reader. When the Adobe Reader Protected Mode is enabled, all operations required to display a PDF document will take place inside of a confined or restricted environment, known as a "sandbox." If Adobe Reader needs to perform an action that is not allowed by the sandboxed environment—for instance, launching an attachment using another application—these requests are put through a "broker process," which sets policies for what is allowed and what is blocked.[17]

Criminals Favoring Java Over PDFs

Online criminals pay close attention to the success and failure rates of their exploits. As of late 2010, it became clear that they feel Java is a gold mine. In January 2010, Java exploits made up 1.5 percent of web malware blocked by Cisco ScanSafe. By November 2010, such exploits skyrocketed to 7 percent. Conversely, PDF exploits are on the decline: In January, PDF exploits totaled slightly more than 6 percent of web malware blocked by Cisco ScanSafe; by November, that number had dropped to just 2 percent.

Why is Java favored over PDFs as an exploit launching pad? Possible reasons are the increased availability of public Java exploit code and the decreased availability of public Adobe Reader and Adobe Acrobat exploits. In addition, users have begun shifting toward alternative PDF readers, and users who still favor Adobe PDF solutions are more likely to disable JavaScript and Flash. For these reasons, PDF exploits have not succeeded as often. Furthering the rush to Java was the fact that in April 2010, public exploit code for Java was released and quickly adopted.



In 2010, Java exploits rose while PDF exploits fell.

Spammers Adopt Multivector Strategy

Combining several tactics can yield greater results than simply deploying a single scam. An October 2010 spam outbreak, featuring fake iTunes purchase receipts and custom-crafted links, was a notable example of this strategy.

In this outbreak, individuals received emails with a fictitious receipt for a purchase on the iTunes music and media service. The supposed invoice was blank, and contained the text, "Click here if you not see image" (sic). Recipients who clicked on the link were asked to download a fake PDF reader, and then redirected to an infected webpage that contained the Zeus malware, which steals banking data.

The creators of this scam used several tactics:

- They used familiar consumer brands—in this case, Apple iTunes—to lure victims into clicking on links.
- They compromised thousands of legitimate websites so that users would think they had reached a legitimate site, not one that would deliver malware.
- They redirected people to fake pharmaceutical websites and fake anti-virus sites.

New on the horizon are exploits delivered via social networking that can infiltrate multiple platforms. In early November, researchers detected malware called Java/Boonana, which is sent to Facebook users and is downloaded by unsuspecting users via a link to a supposed video. The malware is written in Java, and can infect computers using Microsoft Windows, Apple, or Linux operating systems.[18]

[17] "Introducing Adobe Reader Protected Mode," Adobe Secure Software Engineering Team blog, July 20, 2010, http://blogs.adobe.com/asset/2010/07/introducing-adobe-reader-protected-mode.html.
[18] "It's NOT Koobface! New multi-platform infector," Microsoft Malware Protection Center, November 3, 2010, http://blogs.technet.com/b/mmpc/archive/2010/11/03/its-not-koobface-new-multi-platform-infector.aspx.

Building Better Security Into Passwords

In spite of pleading from IT professionals to choose tough-to-guess security passwords, workers are still disconcertingly likely to come up with something like “password1!”—or simply attach a few numbers, like “123,” to the end of a word. The problem of weak, guessable passwords is not a new one, but it isn’t going away—in fact, it’s getting worse, as users are forced to create several passwords for different systems and change them every 60 or 90 days.

No wonder users default to using the least complicated password that their systems allow, and make only minor variations when forced to change them. Unfortunately, such passwords are easy to guess. At the other end of the scale are passwords that are randomly generated by the software solutions themselves, which are difficult for users to remember.

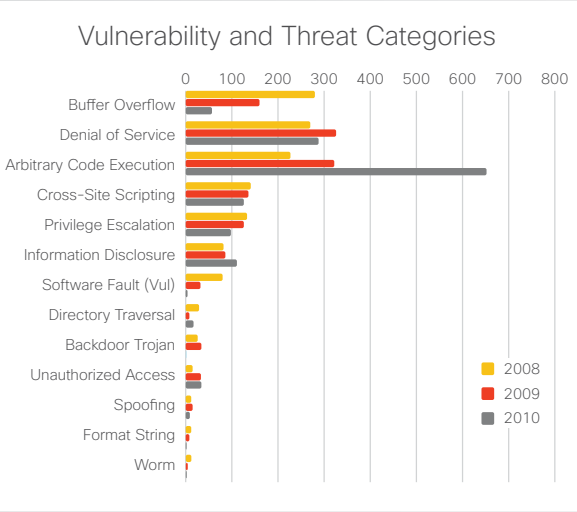
In a recent paper coauthored by Cisco, Florida State University, and Redjack LLC, researchers examined how different password requirements affected password strength—such as requiring the use of a minimal password length or the addition of a special character such as an exclamation point. As the researchers discovered, such policies usually don’t provide greater security, since hackers are well-versed in these tactics and can use them to guess passwords and access accounts. For instance, hackers know that when users are required to use a special character in a password, they will usually simply append that character to the end of the password.

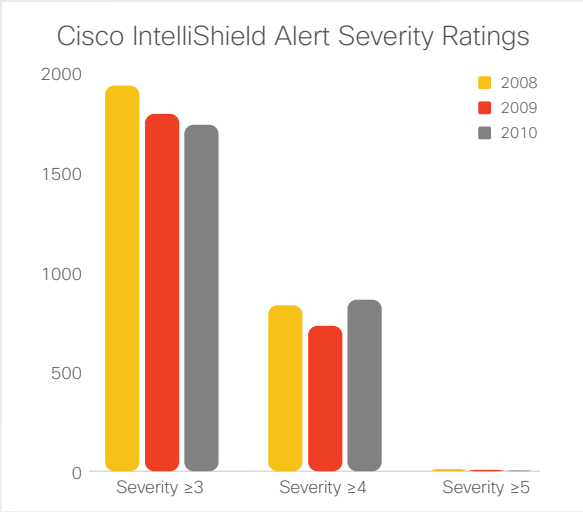
A better practice, say the researchers, is an external password creation policy that changes a password after it is created to add a guaranteed amount of randomness—for example, adding two random digits to the end of a password. This allows users to choose a password that they are likely to remember, while making it difficult to guess. Another tactic is an implicit password policy, which will reject a password instantly based on its estimated strength, and suggest a stronger one. In addition, administrators should implement available password protection software, which means users only need to remember one strong master password, since the application stores encrypted passwords that the user saves.

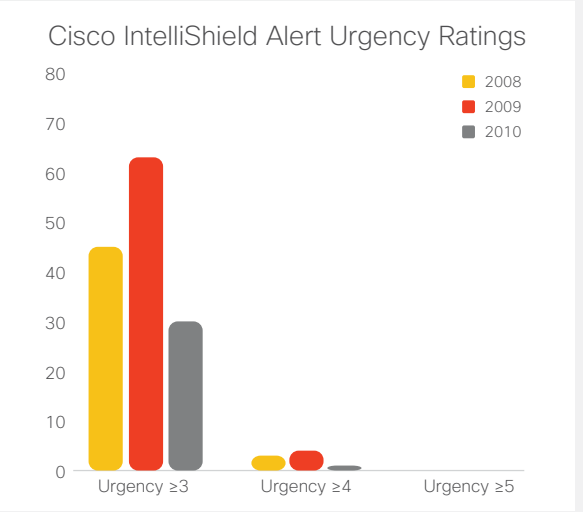
The problem of weak, guessable passwords is not a new one, but it isn’t going away—in fact, it’s getting worse.

2010 Vulnerability and Threat Analysis

The *Cisco Annual Security Report* provides a comparison of the rise and fall of vulnerabilities and threats by category, as well as the estimated impact of these exploits.







The **Vulnerability and Threat Categories** chart above demonstrates a sizable shift from buffer overflows to arbitrary code executions between 2009 and 2010. Buffer overflow vulnerabilities have likely declined due to the identification of such vulnerabilities in previous years, as well as improvements in coding practices. However, the rise of arbitrary code execution vulnerabilities and threats indicates an increase in criminals' exploit capabilities—that is, the use of automated tools to find the vulnerabilities as well as the tools criminals use to exploit these vulnerabilities.

In 2010, there was also a notable increase in information disclosure vulnerabilities and threats. Most other categories showed decreases in 2010, including denial of service, cross-site scripting, software faults, and format strings. Trojans and worms continue to show low numbers, reflecting the lack of new exploits in this category.

The **Cisco IntelliShield Alert Severity Ratings** reflect the impact level of successful vulnerability exploits. For 2010, severity levels remained relatively consistent with those in 2009 and 2008, although the shift to arbitrary code execution vulnerabilities is reflected in the increase in Severity 4 (moderate damage) ratings. The decrease in Severity 3 (mild damage) ratings reflects the decrease in buffer overflows and denial of service vulnerabilities.

It is notable that the shift in vulnerability and severity ratings reflects an increased level of criminal control on targeted systems. While the buffer overflow and denial of service vulnerabilities of previous years primarily reflected a system availability concern, the arbitrary code execution and information disclosure vulnerabilities of 2010 have a higher-risk impact to both system confidentiality and integrity.

Cisco IntelliShield Alert Urgency Ratings reflect the level of threat activity related to specific vulnerabilities. After increases in 2008 and 2009, urgency levels in 2010 decreased. This trend reflects both the repetitive widespread exploitation of individual vulnerabilities across a large user base (such as Adobe and Java vulnerabilities), and the continued shift toward social engineering methods that rely on exploitation of the user—not exploitation of a software vulnerability.*

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

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

Worldwide Government Trends

As governments become more focused on improving cybersecurity and developing global standards, private industry is stepping up to help ensure legislation does not stifle innovation.

United States Government Update

2010 saw a continued focus on cybersecurity legislation, with increasing momentum toward creating a comprehensive bill that would cover law enforcement, critical infrastructure protection, research and development, and global norms for cybersecurity. Growing concerns about foreign entities hacking into networks to gather intelligence, the safety of national infrastructure in light of the Stuxnet threat (see page 21), the effects on the competitive edge of the United States due to theft by domestic and international cybercriminals of intellectual property from businesses, and a focus on ensuring supply chain integrity for software and hardware are just some of the key factors behind the recent push by U.S. lawmakers for more substantial cybersecurity legislation.

However, while obviously well-intended, several new legislative proposals now being considered by the U.S. Congress could be potentially intrusive on private industry. For example, there is some concern in the private sector that the U.S. government, with its substantial procurement power, may become more involved in the development of IT products. Many companies worry this may stifle their innovation—and perhaps, could undermine efforts to develop more secure technology products.

There also is concern within private industry that new regulatory demands that may evolve from proposed cybersecurity legislation could prevent enterprises from responding effectively to emerging and changing threats. Leading companies—including Cisco—have been engaged in ongoing dialogue with the federal government, and are advising lawmakers on how to avoid the creation of legislation that might adversely affect the security of networks and private industry's innovation.

Getting the Word Out on Cybersecurity: Private-Public Partnership

Stop. Think. Connect.™ was the tagline for the National Cyber Security Alliance's public awareness campaign launched in October 2010 in partnership with the U.S. Department of Homeland Security, the Federal Trade Commission, and others.[19] The campaign was designed to "guide the nation to a higher level of Internet safety" by challenging the American public to be more vigilant about practicing good "cyber hygiene" and to view Internet safety as a "shared responsibility."

The effort included a music video—created by EMC Corp. and RSA—used to inform young people about the potential dangers of the Internet. Posted on YouTube, the video features Jay Wise and Friends (Wise is an eighth grade social studies teacher and director of performing arts in Roxbury, Massachusetts). The song lyrics included "stay safe" messages such as, "Don't talk to strangers, even on the web."

The "Stop. Think. Connect" public awareness campaign is the result of a yearlong, collaborative effort by the Online Consumer Security and Safety Messaging Convention, organized by the National Cyber Security Alliance (NCSA), the Anti-Phishing Working Group (APWG), several government agencies, nonprofits, and members of private industry. This was the seventh annual National Cyber Security Awareness Month initiative.

Young Internet users are encouraged to "Stop. Think. Connect." in an online music video featuring Jay Wise and Friends. The effort was part of a recent U.S. public service campaign about cybersecurity.

[19] www.staysafeonline.org: Founded in 2001, NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals' use, the networks they connect to, and our shared digital assets.

Another notable cybersecurity development for the U.S. government in 2010: The Obama administration, which has made strengthening national cybersecurity one of its top priorities, reached a significant milestone on November 3 when the new U.S. Cyber Command (also known as "CYBERCOM") finally reached full operating status after several delays. Led by four-star Army General Keith B. Alexander, CYBERCOM works side-by-side with the National Security Agency (NSA) and has the authority to defend the nation's military networks.

European Union Update

ENISA, the European Network and Information Security Agency, has been actively working with European Commission ministers and departments and European Union (EU) Member States on policy and operational issues around cybersecurity. Through these discussions, private-public partnerships have emerged as the most promising approach for tackling such issues as information sharing, cross-country collaboration, cloud computing, and identity management.

ENISA is also heading EP3R, the European Public Private Partnership for Resilience. EP3R is the flexible Europe-wide governance framework for resilience of information and communication technology infrastructure, which works to foster cooperation between the public and private sectors on security and resilience objectives, baseline requirements, policy practices, and measures.

Geopolitical Trends: Cooperate or Separate?

The ongoing process of developing and refining global standards for security and information technology has come up against the desire of some governments to create domestic standards around IT solutions that can be deployed within their borders. In fact, this struggle to maintain global standards versus instances of non-standard domestic requirements surpasses hardware and software, and can affect network architecture and business processes as well.

Information technology networks are based on global standards that help ensure interoperability and security. In security, these goals are achieved by international standards bodies such as the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE); for product assurance, these goals are achieved by the Common Criteria, an International Organization for Standardization standard and the subject of a multilateral agreement among 26 nations, known as the Common Criteria Recognition Arrangement.

In the EU, private-public partnerships have emerged as the most promising approach to tackling many policy and operational issues around cybersecurity.

2010 saw a number of countries attempt to use nonstandard domestic requirements for product assurance, along with a corresponding reaction by a majority of countries to return to the primacy of international standards such as the Common Criteria. Cisco and other companies are leading an effort to embrace, reform, and extend the Common Criteria in order to drive the benefits of increased security, and extend the benefits of global innovation in products and systems.

An example of the complexities of these collaborative security efforts is the ongoing debate, led primarily within the EU but taking place in many countries, on protecting personal data in cross-border computing systems. Countries recognize that the interests and concerns of their own citizens must be raised if they are to be recognized in regulations that affect cross-border transactions—although these differing standards can affect the development of technologies that are meant to be in use globally.

EU privacy laws limit the transfer of personal data outside the EU's borders and arguably has restricted the growth of cloud computing in Europe. In response, organizations with a major stake in the cloud computing market are working on ways to adjust to different laws and values as data moves beyond borders.[20]

[20] "Cloud Computing Hits Snag in Europe," The New York Times, September 19, 2010, www.nytimes.com/2010/09/20/technology/20cloud.html.

Global Spam Update: Spam Down Globally, but on the Rise in Europe

In the global spam update in the *Cisco 2009 Annual Security Report*, emerging economies showed the sharpest increases in spam production. In 2010, the problem spots were developed nations, with France, Germany, and the United Kingdom displaying markedly higher rates of spam volume. In the United Kingdom, for example, spam volume rose almost 99 percent from 2009 to 2010, according to Cisco research. One likely reason for this spam growth is the spread of broadband Internet in these countries. As in other developed nations, the faster the Internet pipeline, the easier it is to launch botnet-driven spam campaigns.

In spite of these increases, it's important to note that global annual spam volumes actually dropped—the first time this has happened in the history of the Internet. The reason is that some key players in the spam world were halted by security researchers, resulting in a marked decline in spam.

The good news is that Brazil, China, and Turkey—all of which figured high on last year's list of spam nations—showed significantly lower volumes of spam in 2010. In particular, Turkey's spam volume dropped 87 percent from 2009 to 2010. Service providers in China and Turkey have made concentrated efforts to eradicate the botnets that produce spam by working closely with their customers. Brazil's spam volume has been in decline since Internet service providers began restricting access to port 25, which is used by spammers for relaying email.

Governments seem to place greater importance on taking a leadership role in fighting spam, and are setting aside resources for anti-spam efforts.

In Germany, for example, where spam volume increased 10 percent in 2010, a new Anti-Botnet Initiative has been funded by the country's Ministry of the Interior, with funds intended to help consumers clean up computers that have been infected by botnets.

Five German Internet service providers are participating in the program, and will identify infected computers on their networks and notify owners, who are then eligible for free malware-removal assistance.[21]

Global annual spam volumes actually dropped in 2010–the first time this has happened in the history of the Internet.

Spam Growing in Some Developed Nations

Country	2010 Volume	2009 Volume	Volume Change
United States	11.1	11.3	-1.6%
India	9.1	6.4	40.7%
Brazil	7.0	13.3	-47.5%
Russian Federation	6.4	5.0	27.7%
Vietnam	4.3	5.6	-22.4%
Poland	3.6	3.8	-5.9%
China	3.6	4.2	-13.5%
United Kingdom	3.6	1.8	98.9%
Ukraine	3.4	2.4	45.4%
France	3.0	1.4	115.3%
Germany	2.8	2.6	10%
Turkey	.45	3.7	-87%

Volume in trillions per year

Source: Cisco Security Intelligence Operations

[21] "Germany to launch antibotnet program for consumers," IDG News, September 3, 2010, www.networkworld.com/news/2010/090310-germany-to-launch-antibotnet-program.html?source=nww_rss.

The Tipping Point: Cybercriminals Targeting Mobile Platforms

PC vendors are building better security in their products, making them much harder to exploit. Cybercriminals are responding by shifting their focus to the ever-expanding legion of mobile users.

While it's only beginning to percolate, a trend is clearly emerging: Cybercriminals, looking for new opportunities outside of the PC environment, are investing more resources toward developing exploits that specifically target users of mobile devices. Most notably, perhaps, was the emergence of SymbOS/Zitmo.Altr in late 2009 (see page 7), which represented the first known appearance of mobile malware featuring the powerful and pervasive banking Trojan, Zeus.

Taking advantage of the rapidly multiplying number of mobile users worldwide makes business sense. Less-developed nations are particularly ripe for opportunity: According to the United Nation's telecommunications agency, the International Telecommunications Union (ITU), even though high-speed Internet is still out of reach for many citizens of poorer nations, mobile telephony is filling the void because it is available and affordable. The ITU estimates that by the end of 2010, of the more than 5 billion mobile subscriptions worldwide, 3.8 billion will be in the developing world. And by late 2010, ITU predicted mobile penetration in developing countries would reach 68 percent.[22]

This shift in focus toward mobile users is being spurred for another reason: A significant "tipping point" in vulnerabilities has been reached. PC vendors are building better security into their products, and they are moving faster than ever to provide updates, alert users to potential flaws, and make patches available to users.

This means it is becoming increasingly time-consuming and resource-intensive to find ways to exploit platforms that once were so lucrative—in particular, the Microsoft Windows platform. "For a long time, cybercriminals have found many opportunities to take advantage of users through the Windows PC," notes Patrick Peterson, senior security researcher and Cisco Fellow. "It was easy, so why go anywhere else? But now, the Windows operating system is in much better shape—and criminals are getting hungry."

Cybercriminals' shift in focus toward mobile users and away from the PC environment is being spurred partly by a significant "tipping point" in vulnerabilities.

[22] "ITU estimates two billion people online by end [of] 2010," International Telecommunications Union, media release, October 19, 2010, www.itu.int/net/pressoffice/press_releases/2010/39.aspx#url.

Peterson likens cybercriminals to bears who have been "feasting on Windows boxes for a long time." He adds, "The Windows platform was the 'slowest hiker' in the woods. But now, it's getting harder for the bears to catch, so other platforms are in more danger. Apple's iOS and Mac OS and the Google Android OS are hikers that the bears have largely ignored, but now, these platforms are looking much tastier." Peterson concludes, "Just keep in mind, if you are a vendor facing the threat of bears, to survive you don't have to be faster than the bears—just faster than the slowest hiker."

For a long time, the Microsoft Windows platform was easy game as the "slowest hiker." But now that it is more secure and harder to exploit, other platforms, like Apple's Mac operating system and the Google Android operating system, are in greater danger of being targeted by cybercriminals (the "bears").

Android and Apple Operating Systems Likely Key Targets in 2011

The "bears" may be changing their hunting patterns, but cybercriminals are still very much in the research and development phase with their methods of snaring victims using mobile devices. Over the past two years, there have been a number of phishing scams, mostly regional in focus, targeting individuals or select groups—such as customers of local banks or credit unions. And Apple's products, including iPhones, iPads, and the iTunes media service, have all been recent targets (for more on Apple vulnerabilities, see sidebar "Recent Spike in Exploits Targeting Apple Users" on page 33).

As for the Apple iPhone, users of the newly released iOS 4 have benefitted from more than 60 patches designed to fix security vulnerabilities, including an exploit that allowed third-party applications ("apps") to access information on an iPhone user's location without permission. However, many users are undermining the security of their smartphones and other devices, including iPads and iTouch devices, by "jailbreaking" them. Discussed in previous Cisco security reports, jailbreaking is a process that allows users to unlock the iOS, thereby removing Apple-imposed limitations on what apps they can download and from where.

In July 2010, the U.S. Library of Congress added jailbreaking to its list of actions that do not violate copyright protections—leaving iPhone users free to unlock their devices and download applications not authorized by Apple. Only a week after the ruling, JailbreakMe 2.0, the one-click, mobile, Safari-based iPhone jailbreak utility, was unveiled. The new tool makes it easier than ever for users to jailbreak their phones; in the past, some advanced technical skill was required. The advent of this tool also revealed a significant security flaw in the iOS 4 (which Apple has since patched) that could leave iPhone users with jailbroken phones more susceptible to hackers who could gain access to root privileges and essentially take control of the devices.

Since the Library of Congress lifted the threat of legal liability from Apple customers looking to unlock their devices, more than a million users have jailbroken their iPhones, according to the Electronic Frontier Foundation, a San Francisco-based privacy rights organization that petitioned the library. And users are finding ample opportunity to download unofficial iPhone apps, including those from a market called Cydia, which provides access to "Installous" from Hackulous, an app that offers free, pirated versions of thousands of apps available through the iTunes store.

Meanwhile, many users are avoiding the hassle of jailbreaking their iPhones and instead are fully embracing the open architecture of the Google Android smartphone operating system. In fact, market share for the Android OS expanded significantly during 2010, and the open-source operating system is proving to be a significant, competitive threat to the Apple iPhone (both operating systems are still trailing Research in Motion's BlackBerry OS, however, in terms of popularity by numbers).[23]

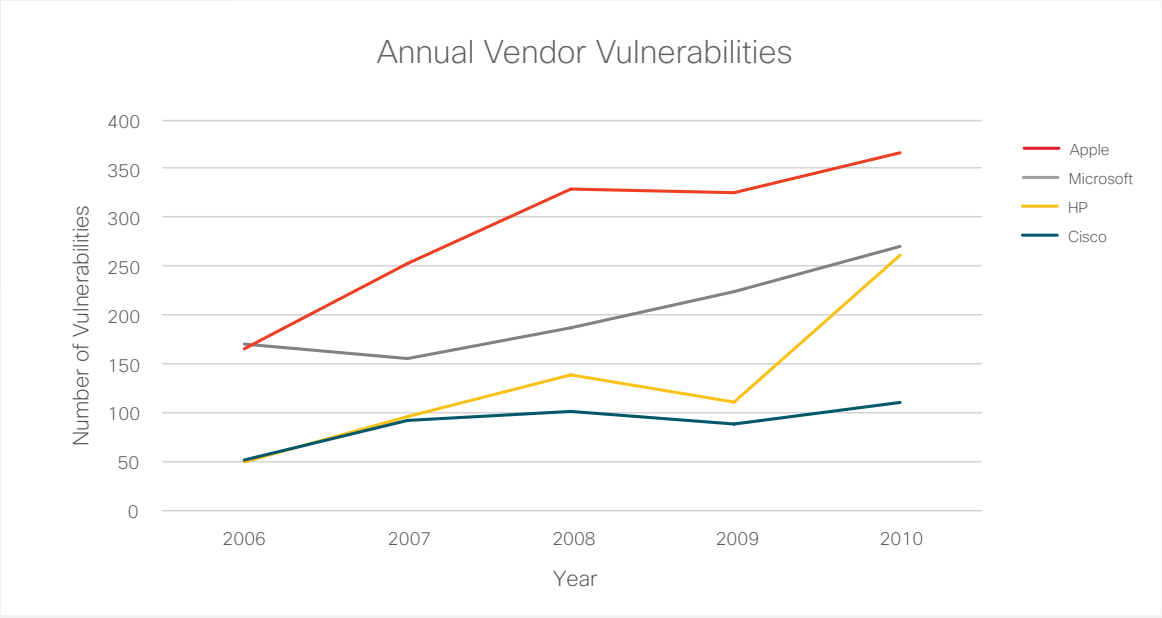
"Three years ago, there was no Android. Now, there are only a few major handset manufacturers that aren't developing devices based on Android," says Cisco threat research manager Scott Olechowski. "The growth of this platform will be exponential. From smartphones and tablet PCs to cars and refrigerators, we will see billions of devices, including a massive number in the enterprise, relying on this platform within the next few years. The relative youth of the Android OS, including its apps and ecosystem, combined with the sheer number of users will make this a very attractive platform for exploitation."

[23] "iPhone vs. Android: By the Nielsen numbers," by Jolie O'Dell, Mashable.com, November 3, 2010, http://edition.cnn.com/2010/TECH/mobile/11/03/iphone.android.mashable/.

Recent Spike in Exploits Targeting Apple Users

A few years ago, Apple and its operating system and products were viewed as somewhat impervious to criminal hacks—at least, less vulnerable than Microsoft Windows and other PC systems. That picture is changing: Over the past five years, Apple has released a growing number of security updates in response to the vulnerabilities detected in its products. According to data from Cisco IntelliShield, while reported vulnerabilities and updates are on the rise from most major vendors, Apple is showing the greatest increase. "As with most large vendors with a broad product base and many new product and software releases, you'd expect to see a related increase in vulnerabilities," explains Jeff Shipley, Security Research and Operations manager at Cisco. "In Apple's case, the difference is that its products are being rapidly adopted by a growing user base, providing an attractive pool of potential targets." In other words, Apple has reached the "tipping point" at which scammers see potential in shifting their exploits to a new venue.

To its credit, Apple has taken substantial steps (beyond those of many other vendors) to protect its technologies against exploits—for instance, creating a tightly controlled application store that limits malicious application postings, developing proprietary controls to limit user environments, and making Java installations more secure. At the same time, users have done their best to bypass these safeguards, "jailbreaking" their products so they can be used with non-Apple applications and unapproved service providers.



According to Cisco IntelliShield, reported vulnerabilities from Apple are on the rise.

Adapting to an Open-Source World

The Android OS is based on a modified version of the Linux Kernel, which is at the core of a growing range of products and platforms that includes mobile devices, readers and tablets, PCs, and many other products, platforms, and systems. When the Linux Kernel and other open-source software are modified or ported for a specific platform or system, dependency for patches and updates shifts to the new development structure, which may include inputs from the public. Management of open-source software is a challenge for many organizations and users, requiring them to understand new bug-tracking processes, release cycles, and open-source licensing.

This added complexity can result in unknown and unpatched vulnerabilities that are hidden in assets, disconnected support channels, and extended vulnerability windows. Users potentially could be left exposed while waiting for patches and updates from their vendors, especially if there is an excessive delay in their release. However, the good news is that most open-source development managers are quite responsive to inputs, which are provided more frequently and from many more sources than commercial update processes.

"Open-source software and its security challenges are here to stay," affirms Russell Smoak, senior director and general manager of Cisco Security Research and Operations. "To scale effectively, an increased understanding of secure development, greater situational awareness and coordination, and granular management are required. Developers choosing to incorporate open-source software must institute the same security controls as they would for their own software. More critically, we must extend the same sense of ownership over the entire product, not just the code we have written."

"The Apps" of Criminals' Eyes

The mobile applications marketplace is a way for cybercriminals to reach millions of users worldwide quickly. According to recent data from market research firm comScore, smartphones–while representing only about 25 percent of the total U.S. wireless subscriber market–accounted for 60 percent of app downloads and nearly 56 percent of mobile browser access for a three-month period ending August 2010, up from 43.6 percent and 41.4 percent, respectively, over the same period in 2009.[24] And according to a recent Pew Internet study, the average U.S. adult has 18 apps on his or her smartphone–and 20 percent of cell phone users under the age of 30 download apps frequently.

Weather, mapping, social networking, search, and news apps are among the types of mobile apps most frequently downloaded by adults. But game apps, according to the *Nielsen App Playbook*, are most popular: 60 percent of adult users (those over the age of 18) have used a game app in the past 60 days.

Unfortunately, cybercriminals channeling more energy into the mobile market have already honed in on taking advantage of younger users. This is not surprising, though, considering the statistics: Mediamark Research and Intelligence reports that the number of children using cell phones has doubled since 2005. Today, one in five children in the United States between the ages of 6 and 11 carries a cell phone. And what do they like to do with Internet-enabled mobile devices? Browse the web and download games.

One notable example of an exploit aimed at compromising younger mobile device users came to light in mid-2010. It was discovered that free wallpaper apps uploaded to the Android Market, featuring themes popular with children such as *Star Wars* and *My Little Pony*, were collecting unnecessary information from subscribers such as

mobile device phone numbers and subscriber identifier and currently programmed voicemail numbers (but not voicemail passwords or SIM card numbers). The information was sent to a site–www.imnet.us–owned by someone in Shenzen, China. The app was downloaded millions of times before the surreptitious data-collecting activity was discovered.

"Third-party mobile apps are emerging as a serious threat vector. And right now, that market is like the Wild West," warns Horacio Zambrano, product line manager for Cisco. "No one is looking at these apps and determining what is a 'good app' or a 'bad app.'"

Slow Emergence: Cybersecurity Strategy for the Mobile Enterprise

Businesses are becoming more receptive–partly by choice, partly by necessity–to mobile working and less resistant to the consumerization of IT. In fact, the recent financial crisis has motivated cash-strapped organizations to allow employees to purchase the mobile devices they prefer, simply because it is more cost-effective for the organization. Other leading companies have taken the position that mobile devices are part of modern employees' basic "uniform" for work, and therefore expect them to purchase their own devices.

IT security professionals are hopeful that, as they allow more types of mobile devices into the organization, more mobile device manufacturers will prioritize many of the same business-friendly security features that have made Research in Motion's BlackBerry devices popular with enterprises, such as PIN locking, data deletion, and camera control enabled through remote enforcement.

Some organizations are also beginning to recognize that they should assign the responsibility of mobile management and security to a dedicated specialist or team. But many businesses currently lack the resources to establish a fully fledged function, and the IT personnel already responsible for mobility issues–such as managing policies for the BlackBerry Enterprise Server (BES) or enabling iPhones for a select group of executives–do not have the time to take on full ownership of the mobility issue.

"In the classic enterprise organization today, no one truly owns–or wants to own–the mobility issue," says Tom Gillis, vice president and general manager of the Security Technology Business Unit at Cisco. "This is actually part of the reason that the adoption of consumer-driven smartphones in the enterprise has been slow. When it comes to enabling these devices and making sure they are secure, no one is stepping up."

[24] "Smartphone Subscribers Now Comprise Majority of Mobile Browser and Application Users in U.S.," comScore, Inc., media release, October 1, 2010, www.comscore.com/Press_Events/Press_Releases/2010/10/Smartphone_Subscribers_Now_Comprise_Majority_of_Mobile_Browser_and_Application_Users_in_U.S.

Mobility and Virtualization Trends Contributing to Renewed Focus on Data Loss Prevention

Rigorous compliance demands, high-profile incidents of data loss, and the potential security risks due to an expanding mobile workforce and growing number of mobile devices in use in the enterprise have brought about a renewed focus on data loss prevention (DLP) at many businesses in 2010.

More enterprises are placing greater emphasis on protecting their data assets as part of a proactive, overall cybersecurity strategy. They recognize that today's malware is designed to steal information–and their information assets must be protected, as they are critical to business.

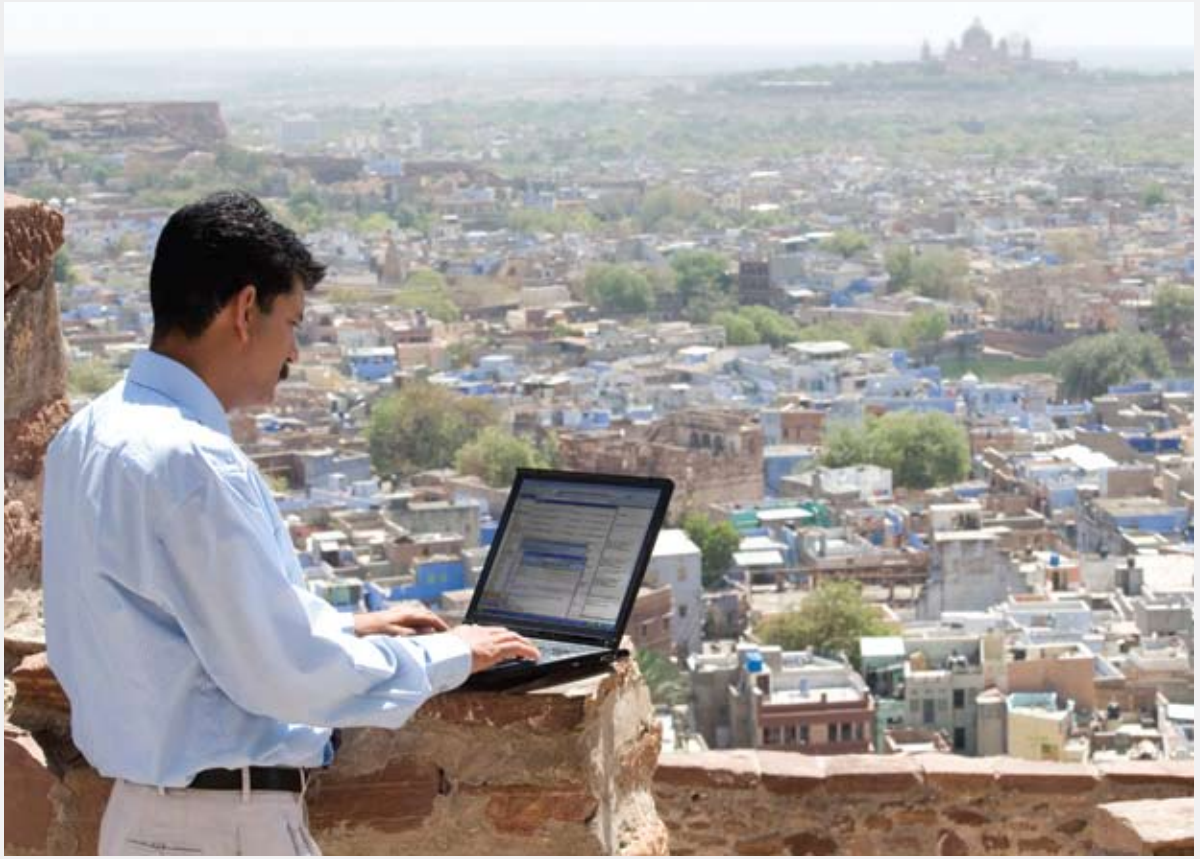
As the economy improves, more organizations are assessing the state of their enterprise security and investing in improvements such as DLP systems. Vendors are making it easier for them too; today, there are more solutions that are easier and more cost-efficient to deploy than ever before. One trend to watch, particularly in the healthcare and financial sectors, is the "containerization" of corporate data. More enterprises likely will explore the option of using digital certificates in an effort to "containerize" mobile users and prevent data loss in the event a mobile device is lost or stolen.

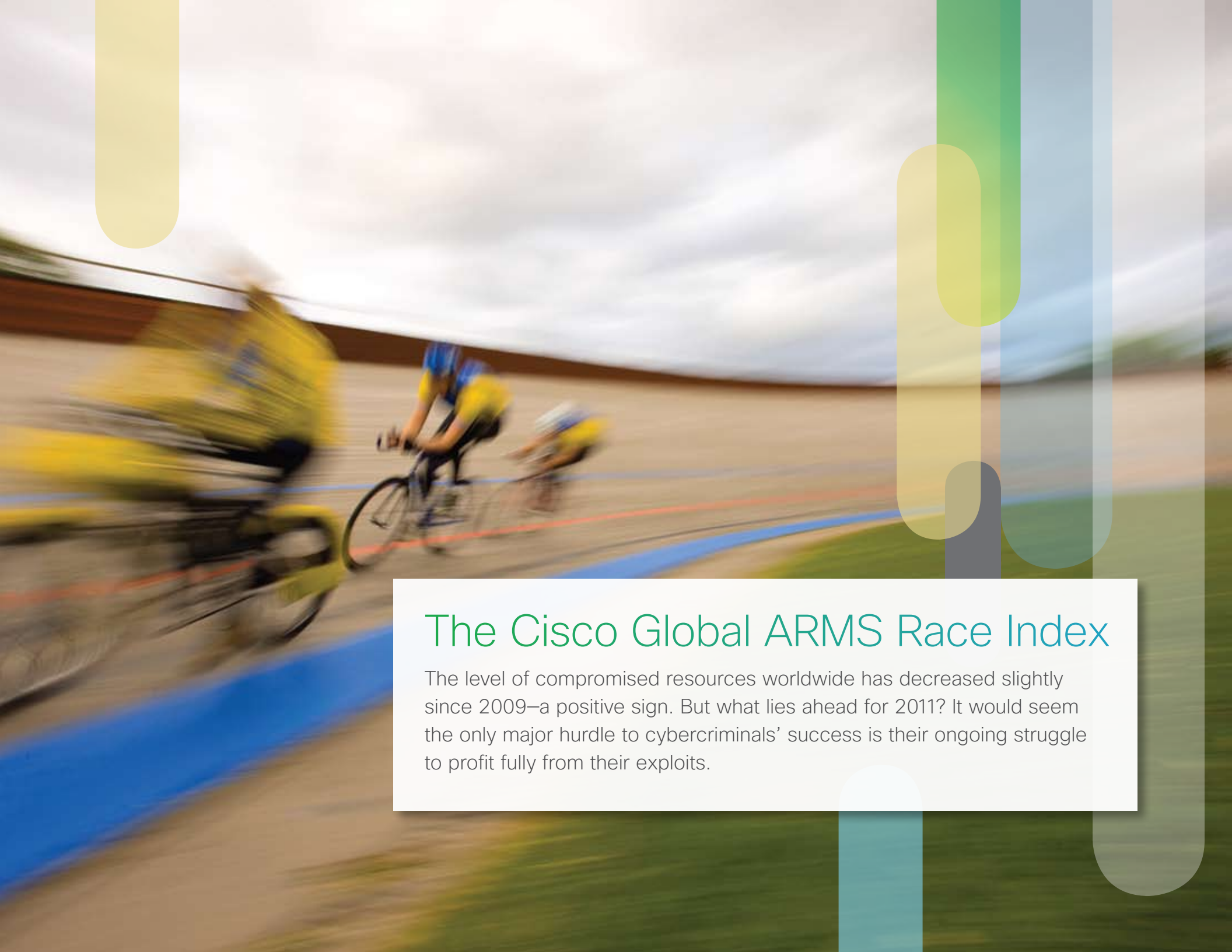
Enterprises are also focusing more attention on DLP because of the virtualization trend. More organizations are accessing hosted services through the cloud that otherwise might be too expensive to purchase or difficult to implement. But virtualization presents both risks and benefits from a cybersecurity perspective. When data is moving from the network, to hosted services providers, to devices such as employees' smartphones and laptops, and then back to the network, how is it being protected?

As for the security benefits: If data is not resident on end devices, it is not as easy for criminals who steal employees' equipment to access sensitive enterprise data, such as financial information and intellectual property. Cloud-based data also offers availability in case of a business disruption.

The bottom line is that virtualization and mobility, while presenting some obvious cybersecurity concerns for the enterprise, also represent a tremendous boon to forward-thinking organizations who embrace them and adapt their security policies appropriately to support these new ways of working.

The *Cisco 2010 Midyear Security Report* outlines recommendations from Cisco security experts for creating a formal corporate policy for mobility and an action plan for adopting cloud computing that can help enterprises to protect their employees and information.





The Cisco Global ARMS Race Index

The level of compromised resources worldwide has decreased slightly since 2009–a positive sign. But what lies ahead for 2011? It would seem the only major hurdle to cybercriminals' success is their ongoing struggle to profit fully from their exploits.

The annual Cisco Global ARMS Race Index, inspired by the Richter Scale used to measure earthquake magnitude, tracks "Adversary Resource Market Share" (ARMS). The index provides a way to measure the overall level of compromised resources worldwide—the networks and machines currently under "adversarial control." Cisco security experts created the index as a way to gain a better understanding of overall trends based on the global online criminal community's activities and their rates of success at compromising both enterprise and individual users.

According to data collected for this year's index, the aggregate number that represents the level of compromised resources at the end of 2010 is 6.8, down from the December 2009 level of 7.2, which was reported in the *Cisco 2009 Annual Report*. This means enterprise networks are still experiencing persistent infections, while consumer systems continue to be infected at levels capable of producing consistent and alarming rates of service abuse; however, the trend shows that infections of enterprise networks and consumer systems are less frequent compared to 12 months ago.

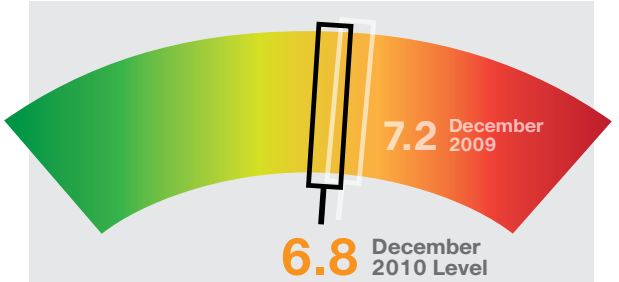
To arrive at this year's measurement on the 10-point index, Cisco relied on leading botnet-tracking estimates of total bots and other data points derived through internal research and other expert sources, such as The Shadowserver Foundation, which tracks cybercriminal activity and is comprised of volunteer security professionals from around the world. The methodology for the Global ARMS Race Index is based on:

- Current aggregate botnet size
- Statistics used to estimate the total number of Internet-connected systems in the world
- Estimates on home and work infection rates, which measure factors like resource availability (such as bandwidth and computing power)
- The high-profile takedowns of botnets such as Waledac, Mariposa (reportedly, the largest botnet ever), and Cutwail have had an impact on the reduced Cisco Global ARMS Race Index number for 2010. (To read more about recent botnet disruption, see the Cisco 2010 Cybercrime Showcase, page 4.) According to data collected for the index, the average botnet size is one-third smaller compared to 12 months ago. However, this doesn't mean that botnets are weakening threats; in fact, they may be strengthening. "For cybercriminals, how many botnets you have in operation, and their size, are no longer important," emphasizes Seth Hanford, Intelligence Operations team lead at Cisco. "It's what you can do with them."

In addition, global spam levels have declined overall, even though there has been an uptick in spam in developed economies where broadband Internet is spreading (see Global Spam Update: Spam Down Globally, but on the Rise in Europe, page 29). Authorities worldwide are taking the spam problem more seriously, as well, and have been successful at taking down some egregious offenders.

One example: In October 2010, Russian authorities launched their first criminal investigation against a man they believe is responsible for spreading 20 percent of the world's spam—primarily spam featuring offers for extremely low-priced prescription drugs (mostly for male enhancement) from unlicensed distributor, Canadian Pharmacy.[25] The alleged spammer, Igor Gusev, operated Spamlt.com, which provided website design and order fulfillment services for spammers. When the site stopped operating in late September 2010, global spam volume was reduced by more than 60 billion messages per day, according to Cisco research. As of January 2011, Gusev was still on the run and believed to be outside Russia, but Russian authorities are working with Interpol to locate him.

The Cisco Global ARMS Race Index



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

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

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

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

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

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

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

According to the Cisco Global ARMS Race Index, the level of resources under adversarial control worldwide was 6.8 at the end of 2010. This is a decline from the 2009 level of 7.2, showing that infections of enterprise networks and consumer systems are less frequent compared to 12 months ago.

[25] "Russia Files Criminal Case Against Major Spammer," by Jeremy Kirk, IDG News, October 27, 2010, www.pcworld.com/article/208902/russia_files_criminal_case_against_major_spammer.html.

Also contributing to the lower level of compromised resources worldwide is the "tipping point" in vulnerabilities, discussed in detail earlier in this report (see The Tipping Point: Cybercriminals Targeting Mobile Platforms, page 30). PC vendors are building better security into their products and are issuing alerts and patches at unprecedented speed. Wanting to use their time and resources wisely, many criminals are abandoning their efforts to take advantage of weaknesses in the Microsoft Windows platform and are focusing more attention on mobile platforms such as the Apple iOS and Android OS. Other miscreants, meanwhile, are simply adapting their techniques to seize opportunities in an increasingly mobile world. The emergence of the SymbOS/Zitmo.Altr—the first known version of the Zeus Trojan designed as mobile malware—underscores the shift in focus by more cybercriminals toward mobile users (for more on SymbOS/Zitmo.Altr, see page 7).

Bank fraud enabled by credential-stealing Trojans like Zeus that target both traditional and mobile Internet users is poised to remain a favorite moneymaker for cybercriminals in the year ahead. "Now that malware developers reportedly have merged the Zeus codebase with that of the SpyEye Trojan, expect the banking Trojan threat to only increase in potency in the coming months," cautions Andy Norton, threat response manager at Cisco.

However, one recent, positive development has been international law enforcement's increased vigilance toward tracking and taking down cybercrime networks that execute bank fraud with help from banking Trojans. In October 2010, for example, authorities, after a lengthy investigation, exposed a well-established, multinational group of scammers delivering malware via Zeus. (Their takedown was so significant, it helped to move down the needle on this year's Cisco Global ARMS Race Index.) It was reported that the U.S. FBI, working in partnership with international law enforcement in the Netherlands, Ukraine, and the United Kingdom, disrupted an elaborate cybercrime network that had been targeting small to midsize companies, municipalities, churches, and individuals by infecting their computers with malware delivered by Zeus.[26]

> "For cybercriminals, how many botnets you have in operation, and their size, are no longer important. It's what you can do with them."
>
> —Seth Hanford, Intelligence Operations team lead, Cisco

According to FBI reports, the group was able to steal US$70 million from victims' bank accounts—although they had been aiming to collect as much as US$220 million before they were caught. Operation "Trident Breach" was launched in May 2009 after FBI agents in Omaha, Nebraska, learned of automated clearing house (ACH) batch payments, initiated by money mules, that were sent to 46 separate bank accounts in the United States.[27] (For more about money mules, see page 8.)

While there has been good news to report in 2010, there is still a big question mark on the cybercrime horizon that must be monitored in the months ahead: Stuxnet—the "Evil" award winner in this year's Cybercrime Showcase (see page 4). As discussed earlier in this report, the worm has the potential to severely disrupt industrial computing systems, such as those used for facilities like power stations—and can deflect remediation and response actions from security professionals. Cisco cybersecurity experts predict that Stuxnet is the debut offering in a new area for extensive research and development by some cybercriminals: hypertargeted malware.

Stuxnet is considered a question mark by cybersecurity experts because its potential is difficult to assess: It can be programmed with enough intelligence to carry out a very specific action against a particular target, and essentially, defend itself against the efforts of security personnel. Experts warn that variants of Stuxnet could be developed to target a wide range of critical infrastructure, from water supplies to transportation systems—or even industrial or business targets, such as chemical or automotive plants.[28]

What this type of threat is capable of in the future will be largely determined by what the cybercriminals designing and deploying it intend to achieve, and what their own technological capabilities are. In a November 2010 hearing of the U.S. Senate Committee on Homeland Security and Governmental Affairs, Michael Assante, president of the National Board of Information Security Examiners (NBISE), a not-for-profit certification body focused on information security practices and policies, said, "Stuxnet is, at the very least, an important wake-up call for digitally enhanced and reliant countries—at its worst, a blueprint for future attackers." He added that the malware's sophistication "should disturb security professionals, engineers, businessmen, and government leaders alike."[29]

---

[26] "Global Law Enforcement Cooperation Key in Disruption of Cybercrime Ring," by SecurityWeek News, SecurityWeek.com, October 4, 2010, www.securityweek.com/global-law-enforcement-cooperation-key-disruption-cybercrime-ring.

[27] Ibid.

[28] "Son of Stuxnet? Variants of the cyberweapon likely, senators told," by Mark Clayton, The Christian Science Monitor, November 17, 2010, www.csmonitor.com/USA/2010/1117/Son-of-Stuxnet-Variants-of-the-cyberweapon-likely-senators-told.

[29] Ibid.

Cybercriminals in 2011: Compromising Trust, Cashing In, and Carrying Out More Complex Missions

In 2011, as enterprises continue to grapple with how best to address security issues around mobile devices, mobile working, and trends such as virtualization, and develop a cybersecurity plan that both protects and enhances the productivity of their employees, cybercriminals will continue to try to more effectively manage and fully profit from their own success.

Not having enough "personnel" to serve as money mules, or "wranglers" to recruit and manage them reliably, is a serious bottleneck to cybercriminals' profitability. Therefore, in the months ahead, expect cybercriminals worldwide to focus more resources toward developing money muling operations that are more sophisticated, creative, complex, and multinational, and structured and managed in a way that enables perpetrators to attract more "candidates" for hire, achieve quick profits, conceal their ultimate whereabouts, and stay ahead of law enforcement.

And while this year's Cisco Global ARMS Race Index shows a modest reduction in the number of compromised resources worldwide compared to 2009, what has not abated is criminals' reliance on trust exploitation. Expect to see more creativity in campaigns against select individuals, either taking advantage of someone's trust, or compromising others to reach an intended target.

There is also the potential for more Stuxnet-style targeting of corporations and infrastructure, carried out by ambitious or vengeful cybercriminals who may either work alone or are enlisted by others to carry out misdeeds and create disruption—or, at least, incite fear around the prospect of "What if?"

The headline-grabbing DDoS attacks launched in late 2010 by supporters of WikiLeaks.org do not mark a shift in how profit-oriented cybercriminals will be investing their resources in the year ahead (see The Cisco Cybercrime Return on Investment Matrix, page 6). But these events should motivate organizations to review the strength of current cybersecurity measures, including existing threat response and disruption reduction plans, while also protecting their data, employees, customers, and partners.

"We predicted that we would see more politically motivated online attacks in 2010," notes Patrick Peterson, senior security researcher and Cisco Fellow. "So, the 'hacktivism' following WikiLeaks was not a surprise—it's a trend that's been on the rise since 2007. If people want to make a statement, and be heard, it's only logical they would do so through the Internet. What's more interesting, perhaps, is how easy it was for hackers to create disruption for some major businesses. That's really the wake-up call. Enterprises must take seriously the need to maintain effective cybersecurity because they could be targeted at anytime, for any reason, by anybody."

For many operators in the shadow economy, the interest is no longer in how many victims they can touch. They know they can collect what they need from more than enough faceless victims, and thanks to the proliferation of mobile devices, have the opportunity to target even more individuals worldwide. Moving forward, the real challenge for some of the more sophisticated players in the cybercrime community will be whether they can bend technology enough to their advantage so they can target with precision exactly the person, business, organization, or government they want to somehow influence or cause harm to, and carry out a highly specific mission successfully, or even repeatedly, before detection.

Cisco Security Intelligence Operations

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

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

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

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

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

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

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

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

For More Information

Cisco Security Intelligence Operations
www.cisco.com/security

Cisco Security Blog
blogs.cisco.com/security

Cisco Security Services
www.cisco.com/go/ros

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

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.