INFORMATION SECURITY

FEBRUARY 2014
VOL. 16 | NO. 01

# CYBERTHREATS: KNOW THY ENEMY

New threats and tried-and-true hacking techniques test security teams.



TechTarget

# New Ways to Navigate Security Threats

*It's a new year and a new look for information security.*

BY KATHLEEN RICHARDS



**ONE MONTH INTO 2014** and we have already faced landmark data breaches of major U.S. retailer Target Corp. and online search turned media company, Yahoo. The extent of both attacks is further reaching than first (publicly) thought in December. Target admits that it faced a malware attack that exposed the credit and debit card data of 40 million, make that 70 million, no wait, it's 110 million customers. The fallout continues as the public at large gives a collective shrug and considers returning to cash when they shop at the once-beloved retailer.

These advanced threats will keep on coming in 2014. "Defending a network has never been harder," says Johannes B. Ullrich, dean of research at the SANS Technology Institute and the Internet Storm Center. Ullrich examines the advanced threat techniques to watch out for this year. High on his list, more watering hole attacks and sophisticated spear phishing, driven by social engineering and automation to produce mass customization of emails as malware lures.

> **"Defending a network has never been harder."**
>
> *—Johannes B. Ullrich, dean of research, SANS Technology Institute*

Meanwhile, global scanning services and reputation management techniques are evolving to help security organizations head off advanced threats and heed earlier

warning signs. "Because these systems are collecting data from actual Internet traffic, they can serve as better early warning systems when new infections start moving across the globe," writes technology journalist David Strom, who reports on advanced malware detection techniques this month.

Some consumers are going back to cash, others are using Bitcoin. Security veteran Adam Rice dives beneath the surface and explores the underbelly of the deep Web. Facilitated by Tor Networks and Bitcoin (coming soon to an ATM near you), "employee participation in unapproved activities on the deep Web can take many forms," warns Rice.

We also welcome a new column on mobile security authored by Kevin Johnson, founder and CEO of Secure Ideas, to help you evaluate all those gadgets that showed up at work after the holidays. ■

**KATHLEEN RICHARDS** *is the features editor of* Information Security *magazine. Follow her on Twitter @RichardsKath. Send comments on this column to feedback@infosecuritymag.com.*

# KNOW THY ENEMY IN 2014

## There's no place to hide as new cyberthreats and tried-and-true hacking techniques test security teams. Here's what to watch out for.

By Johannes B. Ullrich

**YOU'RE ON YOUR WAY** to give a presentation at a conference when your phone vibrates, indicating a new email just arrived. Having some time, you check the message. An irate customer sent it, informing you that the email he received advertising the event directed him to the wrong hotel. As proof, he attached a PDF of a screenshot of the email. You open it, and it indeed lists a venue across town that the same hotel chain happens to own. It's almost time to get started, so you flag the message to deal with it later and forward it to the marketing person responsible for the event flyer.

This isn't just an angry email; it's a targeted attack. The recipient in this case was lucky, however. This was a test his organization's network security team conducted. Targeted attacks like this one are still infrequent; the vast majority use less-sophisticated methods. But like many attacks, customized email phishing is becoming easier and faster to execute thanks to automation.

Defending a large network has never been harder. Expensive perimeter protection systems, complex host-based malware detection and even whitelisting systems

have crumbled as attackers perfect an almost unbeatable pair of attacks: spear phishing and watering holes. Both attacks apply an age-old strategy: If a defense is too complex to beat head-on, bypass it.

At the same time, social engineering, the Internet of Things and the combination of traditional Web applications, embedded applications and networked devices often with "versions" of Microsoft or Linux operating systems, present untold security challenges.

To have a chance of defeating these attacks, security organizations need to move away from an overreliance on large, static defenses. Your strategy, instead, should focus on a flexible, nimble approach that, combined with continuous network monitoring, can detect attacks early and allow timely defenses.

## MASS CUSTOMIZATION MOBILIZES

Increasingly, Facebook and LinkedIn profiles are actively being harvested to identify trust relationships and craft more accurate phishing email automatically. In a widespread malware attack in December, a malicious website used geolocation techniques to craft a "voicemail" message with area code and city name matching the recipient. The email claimed to include a link to a WhatsApp voicemail. WhatsApp Messenger is a popular, cross-platform Voice over IP application for mobile devices. The victim clicked on the link and was presented with a program to run to listen to the voicemail.

This attack was made more plausible by using a phone number as the executable file name, which matched the area code of the IP address from which the email was downloaded: *VoiceMail_Jacksonville_(904)4582213.exe* appeared when the file was downloaded in Jacksonville, Fla., and *VoiceMail_Wayne_(610)4582235.exe* when the same executable file was downloaded from a server whose IP address (geolocation) is commonly associated with Wayne, PA.

Smarter bots crafting customized email to large pools of recipients is a trend that is expected to continue to evolve. The individual email will differ to evade spam and malware detection systems. Many of these emails will likely reach their targets and a sufficient number of recipients will click on the links or execute the attachments.

Mass customized email attacks inevitably will become an everyday occurrence, inexpensive to deploy and as effective as targeted spear phishing attacks are today. This technique will likely be adopted soon by organized crime syndicates, who in turn will then use it in massive attacks on populations and organizations.

"Wait a minute—I don't click on links *ever*!" While that's hard to believe—even among security professionals—attackers will get you eventually because you do use Web browsers and visit websites.

It's not unusual for Web applications to rely on a dozen or more external websites to provide images, scripts and other content, such as news feeds. Efforts to

reduce this reliance on external content are not always 100% successful. A compromise of any of these external resources implies a compromise of the site. An attacker may not have direct access to any of the content stored at the website, but they would have access to the people who visit it. Those individuals have (often unwittingly) extended their trust and security to other content delivered through the site.

## MORE WATERING HOLES

Security researchers have reported an increase in watering hole attacks, and this trend is going to continue. A watering hole attack typically targets a group of individuals with common interests by compromising a website that's a shared trusted resource. Often, this is in a geographical area. The RSA Advanced Threat Intelligence Team coined the term "watering hole" after they identified a hacking attack that used these techniques.

In December 2013, the website of the Council on Foreign Relations (CFR), an independent, non-partisan think tank—along with some Washington, D.C., media sites—was compromised, allegedly to target individuals interested in U.S. foreign policy and international affairs. According to reports, a Trojan infected the CFR website and exploited a zero-day flaw in Internet Explorer, which enabled drive-by downloads for its victims.

The appeal of a watering hole attack is that it provides the attackers with a large attack surface. To target a group or an individual, the attacker has to find only one weakness in a large number of resources that the group uses. Using a combination of social and technical trust relationships, the attacker can abuse the trusted resource to access otherwise well-guarded applications and systems.

The appeal of a watering hole attack is that it provides the attackers with a large attack surface.

In late December and early January, people who visited Yahoo websites were met with malicious advertisements, or "malvertising," that, when clicked on, directed users to websites that tried to install malicious software. According to several reports, the Yahoo attack may be part of a much larger malware scheme (based on Web iFrames) that focuses on larger online communities. A security breach affecting a large network of sites like Yahoo is sometimes detected quickly. Smaller, more targeted compromises can go unnoticed for days, weeks and, in some cases, months.

## REVERSE ENGINEERING THE INTERNET OF THINGS

Large traditional Web applications, smaller embedded applications and networked devices combined also present an increasing threat to network security. Sometimes these devices (firewalls, security cameras, air

conditioning controllers) are included in what is referred to as the "Internet of Things." Currently, it is estimated that 9 billion of these devices are connected to the Internet, and the number is growing at an alarming rate.

Recently, the tools and techniques to reverse engineer the embedded applications controlling these devices have substantially improved and become easier to access. Stringfighter, created by IOActive Inc., automates the search for embedded hard-coded passwords. The result is a long list of newly discovered vulnerabilities—from simple hardcoded administrative passwords and support backdoors to more subtle application vulnerabilities.

Of late, many embedded system vendors' bulletins read more like the Open Web Application Security Projects "Top 10" list of Web application vulnerabilities. Even if a vendor releases a patch, these devices usually do not have an automatic update function, and applying patches can be tricky. At the same time, these devices are critical to network and business operations.

Along with device-specific vulnerabilities, we commonly see operating system vulnerabilities. Many of these devices use slightly modified and tuned versions of operating systems like Linux and Windows. As the landmark data breach at Target Corp. painfully illustrates, one favorite target for attackers has been point of sale (POS) systems or cash registers. With many transactions involving credit and debit card payments, POS systems can be a source of lucrative information for attackers, and their distributed nature makes it challenging to monitor and manage them centrally. In December 2012, Visa issued a security alert for merchants on "Dexter" malware that was targeting POS systems running Microsoft Windows. The malware stole the track data or strip from memory and sent it to command-and-control domains and IP addresses.

Attackers can breach the POS system directly if it is reachable from the outside. If it is behind a firewall, but used for tasks like Web browsing and reading email, attackers may employ desktop techniques, such as spear phishing. They may also be able to infect these systems through vulnerabilities in devices used to manage the network.

## STOPPING INVISIBLE TARGETS

As a defender, one of the most burning questions is how to protect your network against constantly changing attacks. Defenses have to be nimble, and they need to be informed by network monitoring and threat intelligence. Too few security people watch system and network traffic logs regularly. (See sidebar, "Continuous Network Monitoring to Fight Next-Generation Attacks" on page 8). Monitoring is often reactive and recognized as valuable only after an attack happens.

To detect data exfiltration and the covert channels used in the process, it is important to not only know what is normal in your network, but to also assess weaknesses and

*(Continued on page 9)*

# Continuous Network Monitoring to Fight Next-Generation Attacks

**CONTINUOUS REAL-TIME** network monitoring is less reliant on attack signatures. It focuses on outbound traffic to detect network abnormalities and traffic that may indicate compromise.

The following controls are the most useful—and overlooked—sources of information to detect compromise.

- **Outbound firewall logs.** Firewalls are one of the most fundamental and widespread security controls. In addition to enforcing network separation, fire wall logs provide important data to detect compromised systems. Traditionally, firewall logs focused on inbound traffic. However, inbound firewall logs are hardly ever linked to actual breached systems. Instead, logs recording blocked outbound connection attempts tend to provide much more valuable data. Why is your Web server trying to connect to an IRC server? Why is a workstation trying to send email directly, instead of using the corporate mail server? These are the kind of indicators you are looking for.

- **DNS logs.** Firewall logs are useful because firewalls are installed to control network choke points. In many modern networks with their mobile clients, VPN connections and geographically diverse IT deployments, firewalls can be too dispersed to provide useful data, and the fidelity of the data is limited. In these cases, central DNS servers can present a great opportunity to monitor clients. One of the most useful reports to detect compromise is a daily list of the top 10 domains and host names requested that were not requested at all the preceding day. Attackers need DNS too and frequently employ fast DNS updates to support a distributed attack infrastructure, which leads to large numbers of DNS requests.

- **Web server logs.** Web servers tend to be the most vulnerable publicly accessible service in an organization. In particular, if custom code is deployed, Web servers need to be monitored closely. But to do so successfully, staff reviewing the logs has to understand Web applications and the attacks that may be

(CONTINUED ON PAGE 9)

(CONTINUED FROM PAGE 8)

used against them. It can be very helpful to request help from Web developers, or have Web developers regularly monitor Web server logs to better understand how applications are attacked.

- **Web proxy logs.** All traffic from an internal network to external websites should pass a proxy. The proxy inspects and filters requests as well as responses, and it provides a rich source of data to identify not only attacks but also vulnerable clients.

  Instead of just focusing on attack signatures, a proxy also inspects the user agent that the host sent and identifies out-of-spec responses, such as a system that wasn't updated or malware using its own user agent string instead of the standard user agent.

- **IPv6 traffic.** Just because nobody is talking about it doesn't mean you are not using it. IPv6 is enabled in all modern operating systems. Microsoft, for example, specifically recommends against disabling it. You need to monitor and control IPv6, or you may end up with native IPv6 traffic internally or IPv6 tunnels externally that evade your monitoring systems. At the very minimum, you need to be able to detect tunneled IPv6 traffic traversing your network perimeter.

— JOHANNES B. ULLRICH

*(Continued from page 7)*

vulnerabilities passively. This alleviates having to rely solely on periodic scans of the network alone.

Network monitoring can also be used to simplify network traffic by eliminating "chatty" and unused services, making it easier to spot threats, reducing the attack surface and, likely, increasing network performance. Current network monitoring is often incomplete and misses newer technologies, like IPv6, which are present in most networks but not configured and managed appropriately. In the end, it will not be the machines and automated systems that are able to adapt to new threats; it will be a sufficiently staffed network and security group with skills to find these gaps, adapt defenses and close them. ■

**JOHANNES B. ULLRICH**, *Ph.D., GIAC, GCIA and GWEB, is the dean of research at the SANS Technology Institute and head researcher at its Internet Storm Center. Follow him on twitter @johullrich.*

# New Devices, New Threats

*How to evaluate the devices we love.* BY KEVIN JOHNSON

**WE'VE ALL SURVIVED** the holiday rush and celebrations, and now the real fun begins: evaluating the security implications of the new mobile "toys" that people want to use to access corporate data, applications and networks. Niche items such as Google Glass and the Samsung Galaxy Gear smartwatch make for great stories around the water cooler, but in most organizations these devices currently have little impact. However, the influx of iPad and Android tablets and wide range of smartphones can really challenge network security, especially in organizations that support the bring your own device (BYOD) trend.

BYOD is one of those topics that has adamant supporters and detractors. Honestly, I think BYOD is something that each organization has to evaluate based on its needs (and wants). But whatever the choice, mobile devices have to be evaluated at some level before you allow them to run on internal networks.

How can you determine which devices to allow or what level of access these products should have? Of special concern are those that are increasingly popular among staff (the new phablets) and company executives (tablet/laptop transformer devices). Analysts expected consumers to opt for smaller-sized tablets over older smartphone replacements during the holiday season, and so should you in the coming year.

## DEVICE-SPECIFIC EVALUATIONS

Security organizations have to ask a number of device-specific questions, and those answers will drive support and security decisions.

**What is the device?** Is it an Android tablet, a Windows phone or some other odd gadget, such as a 3D printer for mobile devices, or coming soon, mini drone? This basic question helps you determine the category of devices to consider, and drives the rest of the questions. It also provides a starting place based existing policies and procedures. (You do have policies right?)

**Are similar or related devices already supported?** Is the new device an upgrade to a Samsung Galaxy Android tablet or Apple iPhone smartphone that you already deal with within your existing security controls? If it is, does the latest version change something fundamental (for instance, the cellular connection on the cellular model of the iPad Air or an operating system upgrade, such as the Google Nexus 5 running Android KitKat?) If it is similar enough, then the device likely has the required security controls; it's already supported in key areas (access control, authentication, mobile device management, data encryption), so you can move on and evaluate the next device.

**What is the need for the device?** This question is a bit more complicated. You have to evaluate the business reasons behind why people want to use specific devices, and dig into their underlying thought processes. Is it just a new fad or is there a business driver? This evaluation is often more difficult if the device has little practical business application. Who wants to admit to their boss that the primary purpose for the device is the cool factor? (If I had told my management team I wanted them to sign off on Google Glass because it made me popular, there's no way I would own one.)

Look for business efficiencies as well as technology advances that can make jobs easier or provide benefit to the company. I recently signed off on a Nexus 5 purchase for one of our consultants. Yes, I know he wanted a new gadget, but he was able to show a potential value to the company. Long story short, Jason now has a Nexus 5, and it's already shown benefits to the business by providing us with information on attacks possible against the device.

> Mobile devices have to be evaluated at some level before you allow them to run on internal networks.

**What connection types does the mobile device support?** The connections are often where the real risks of adding a device comes into play. A Wi-Fi-only device limits the number of connections the attacker can use against the organization, but this may also cause some employees to connect to an untrusted wireless network to get their jobs done.

Security organizations also need to think about how different connection types can affect the security of their internal wireless network systems. A device that has a cellular connection active while it's connected to the corporate wireless network could allow an attacker to pivot from that cellular connection on to the network, bypassing the typical Internet controls a company has in place.

To sum up, think about why your employees want these new devices, and despite the onslaught, try to keep an open mind. As security people, we have to accept that sometimes new things aren't so scary (wait for more wearables and the Internet of Things). Many devices actually benefit the organization. ■

**KEVIN JOHNSON** *is the founder and CEO of Secure Ideas, an IT security consulting firm specializing in identifying comp anies' cybersecurity vulnerabilities. In a career spanning over 20 years, Kevin has worn almost every imaginable IT security hat, including instructor, consultant, public speaker, administrator and architect. You can find him on Twitter at @secureideas.*

# Data on Devices

*A new survey shows the battle between corporate-issued devices versus personally owned smartphones and tablets is too close to call.*

BY KATHLEEN RICHARDS

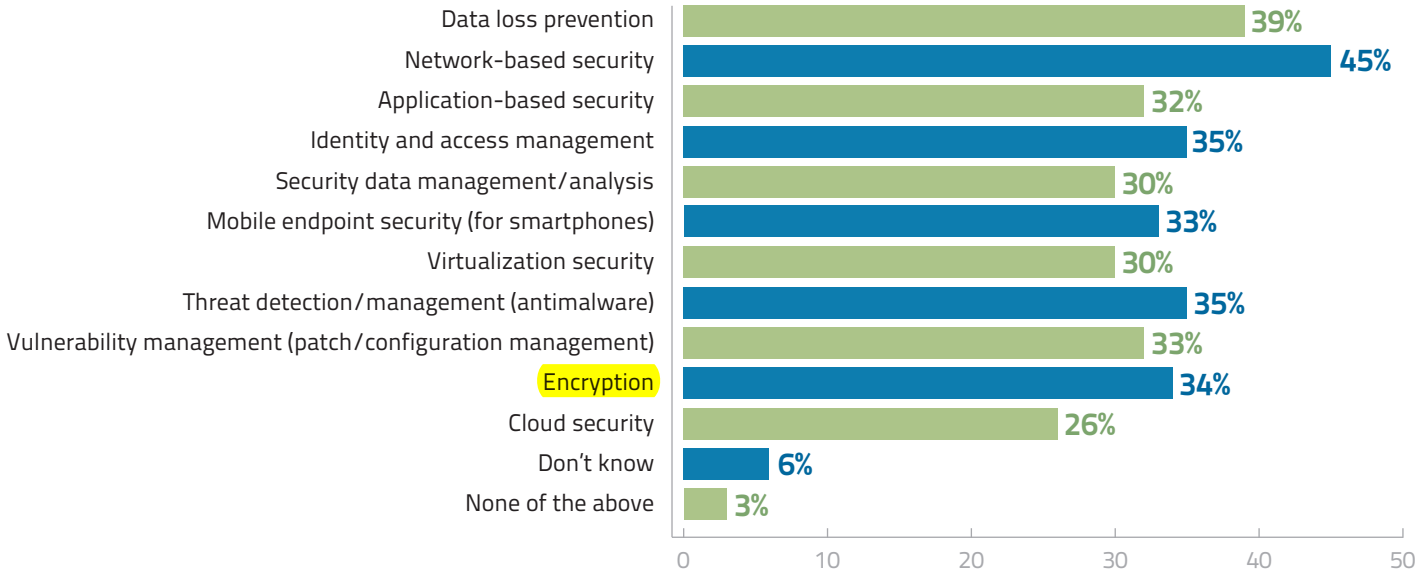
**WE ASKED THE READERS** of *Information Security* and its sister sites (of which there are many) about their IT security initiatives in 2014. Not surprisingly, one-third of respondents to our Global IT Priorities Survey, conducted in Q4 2013, indicated that mobile endpoint security is part of a crowded to-do list. It ranked in the 30% range in our mobile security report data, alongside fundamental security controls including: threat detection/management, application-based security, vulnerability management, encryption, security data management/analysis and virtualization security. Only network-based security and data loss prevention ranked notably higher.

For this survey, TechTarget electronically polled 4,151 IT managers and security professionals about their technology implementation strategies in 2014.

While mobile security is stuck in the middle of an ambitious list of initiatives in 2014, IT managers and corporate executives have struggled in recent years to secure their corporate data and internal networks, which must accommodate a mix of corporate-issued and personally owned devices. In an April 2013 TechTarget networking purchasing intentions survey of 2,700 IT managers, respondents ranked network security (31%) as the top priority for the next 12 months, followed by Wi-Fi/WLAN (27%) and data center network upgrades (25%). Bring your own device (consumer devices) outpaced all other categories as the top blind spot in existing implementations for network management (58%). Security (40%) ranked a distant second, followed by WLAN (31%) and cloud computing (31%), according to those surveyed.

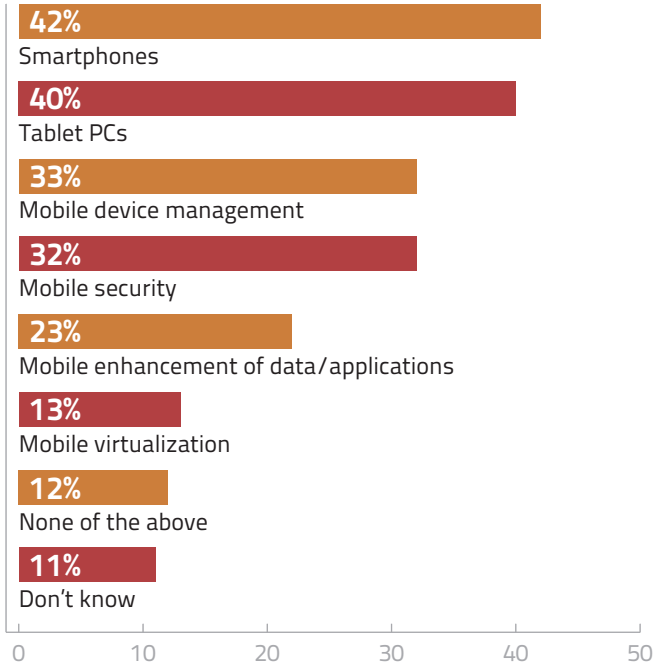
Data from the latest TechTarget Global IT Priorities survey shows that mobile device security is still a hot spot for IT executives as tablets continue to gain ground on smartphones, and some organizations are exploring mobile virtualization and other security initiatives. Despite the clamor around BYOD, fewer than one-fourth (24%) of those surveyed are basing their mobile device strategies on plans that allow employees to choose and purchase their own devices. Most of those surveyed said their organizations will either use corporate-purchased devices (37%) or a combination of corporate-purchased and individually chosen (39%) smartphones and tablets PCs.

## Which of these security initiatives will your company implement in 2014?



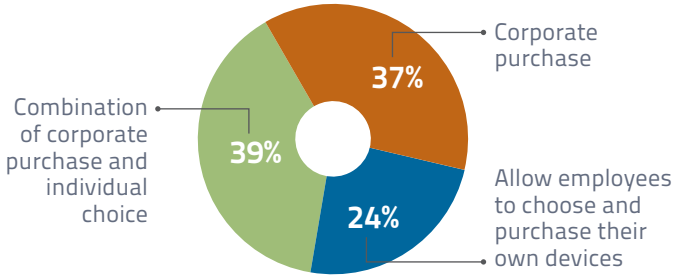

*N=2,072; Respondents were asked to select all that apply; Source: TechTarget Global IT Priorities 2014*

## Which of these mobility initiatives will your company implement in 2014?



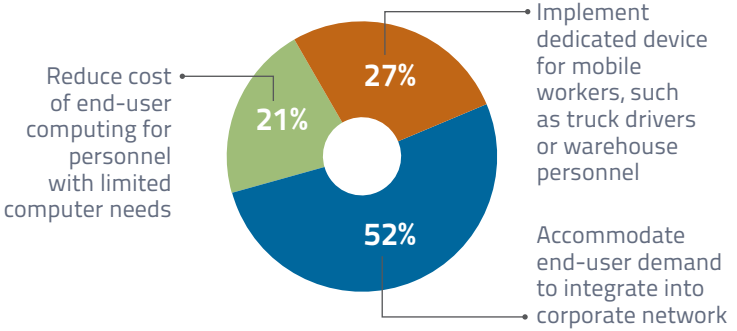

*N=3,360; Respondents were asked to select all that apply; Source: TechTarget Global IT Priorities 2014*

## How will your company implement smartphones?




*N=1,407; Source: TechTarget Global IT Priorities 2014*

## What is your main goal with tablets?




*N=1,339; Source: TechTarget Global IT Priorities 2014*

# THE CHANGING FACE OF ADVANCED MALWARE DETECTION

It's a new year of advanced threats, malicious code and holes to plug. Security organizations are fighting back with help from global services.

By David Strom

**IN THE ESCALATING ARMS RACE** against advanced malware, many organizations require defenses to protect enterprise networks in real time that go beyond desktop endpoint virus scanners and network-based intrusion prevention products.

Unfortunately for security organizations, advanced malware is getting harder to detect, thanks to the proliferation (more than 100) of automated online tools called "crypters" and "packers." Add to these exploits a range of new techniques that use social networks to establish trust, more use of in-memory attacks and ransomware. All of this means it is an increasingly nasty online world.

Crypters and packers make it easier for criminals to create (within seconds) custom code destined for a particular desktop. The effect of this "individualized" approach is that signature scanners are ineffective, making zero-day attacks, such as the November Windows XP privilege escalation attack, increasingly difficult to stop.

Ransomware is also becoming more popular, according to IT security firm Sophos. Note the latest attack

targeting SAP installations in November and a variation called CryptoLocker that is plaguing networks. In these types of attacks, infected code is inadvertently downloaded through phishing in the guise of protective software, such as a fake antivirus or antimalware program. But rather than protecting you, this code ends up demanding payment (sometimes in Bitcoins) before it will release your data.

## IMPROVING THE ODDS

It doesn't take much for bad events to slip through your defenses. "An organization of between 9,000 and 12,000 users can expect to have an average of 1,000 to 1,200 virus events per month, and while traditional antivirus products catch many of these [events], these desktops still need to be properly maintained," says Andy Hubbard, a senior security consultant for Neohapsis and former IT manager for a California hospital chain.

According to Hubbard, "Various versions of FakeAV programs are still really common. This means that even a small percentage of malicious email traffic getting past spam filters can be significant." Gulp.

Having those sorts of odds means managing updates becomes critical. Dougan McMurray, IT manager at Australia-based Brennan IT, advises: "While spam and Web content filters and network threat protection appliances may not be new, having them 100% up to date is mandatory."

Even a small percentage of malicious email traffic getting past spam filters can be significant.

Sometimes, it is a knowledge gap that lets the bad stuff in. Tim Crawford, a former CIO and now a strategic advisor at AVOA, says, "Companies can't always justify the expense of the additional protective features beyond those of a traditional firewall. As the threat vectors increasingly change from relatively simplistic signature-based [threats] to more complex behavior-based [threats], the awareness of many IT managers has not evolved as quickly."

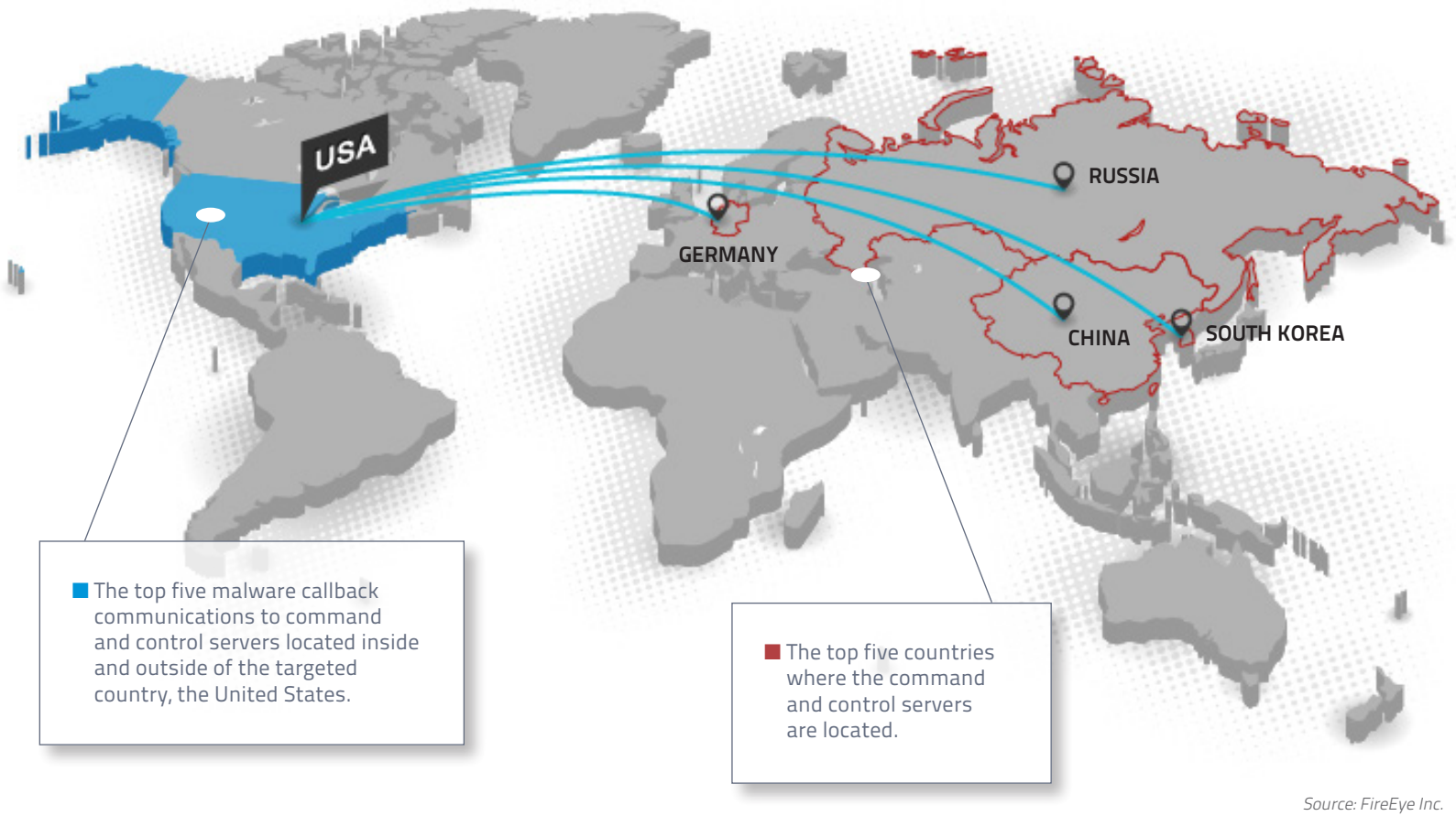
## MORE WAYS TO FIGHT BACK

But the good guys are fighting back, using two general technologies. First, many organizations are improving their real-time global scanning efforts. (The National Security Agency isn't the only entity watching Internet traffic.) These systems include products and services from McAfee Inc., Norse Corp., FireEye Inc., Palo Alto Networks Inc. and Network Box Corp. Security vendors have placed sensors around the world at key customer or Internet connection points to detect zero-day exploits in near real time.

*(Continued on page 20)*

# Malware Callbacks to Command and Control Servers Worldwide

Security vendors such as FireEye have placed sensors around the world at key customer or Internet connection points to detect zero-day exploits on infected enterprise hosts in near real-time.




*Source: FireEye Inc.*

*(Continued from page 18)*

Palo Alto Networks uses its WildFire service to trap and investigate threats and communicate this information to its customers (See sidebar, "Advanced Malware: Five Prevention Tactics from the Trenches" page 21). McAfee has paired its Advanced Threat Defense appliance with its Real Time software for endpoints and servers to try to do a better job of catching zero-day attacks.

**These systems place sensors around the world, but they are looking for particular network domains that are broadcasting malware.**

Norse Corp. has software that credit card companies can use during the few seconds that a card reader is checking to see if a card has been compromised. Network Box's Z-Scan Anti-Malware service also uses hundreds of thousands of probes spread around the world on key network segments to detect advanced malware and other anomalies. The company also added more than a dozen antimalware scanners and three IPS engines to examine packets.

Other companies, such as Verdasys and FireEye, are combining forces and announcing integrated security systems. Introduced in September, the Verdasys Digital Guardian Connector for FireEye combines FireEye's detection network with Verdasys' endpoint protection. Expect more of these partnerships in the future.

## EARLY WARNING SYSTEMS

More sophisticated and integrated reputation management techniques are also becoming available from companies such as Cisco Systems Inc., Blue Coat Systems Inc., Bit9 and Symantec Corp. Again, these systems place sensors around the world, but they are looking for particular network domains that are broadcasting malware. While reputation services have been around for several years, the difference is now these services are being integrated into the ordinary network firewall and IPS devices so they can do a better job of targeting malicious software and anomalous network events. Because these systems are collecting data from actual Internet traffic, they can serve as better early warning systems when new infections start moving across the globe.

Cisco's Security Intelligence Operations, which had its origins in the SenderBase product line, can be used in a wide variety of Cisco gear, including its IPS, Web Security Appliance and ASA CX firewall line. Because of Cisco's reach and market share, this can be a great first line of defense and identify a lot of potential exploits.

Some of the firewall vendors have taken things a step further. These companies have integrated geofencing

*(Continued on page 22)*

# Advanced Malware: Five Prevention Tactics from the Trenches

**SO WHAT ARE SOME STRATEGIES** that IT managers have used to stem the advanced malware tide? First is a combined approach of network and desktop protection. Susan May is a technical support specialist in the IT department at Amherst College. The campus uses a combination of ESET's antimalware scanner and Palo Alto Networks' WildFire sandboxing analysis service to protect its network. "We have seen a lot of spear phishing and fraudulent email messages that use *Amherst* subjects in them," says May. "The threat detection console feature of ESET is very helpful as it notifies [us] about infections and lets us track ones that are symptomless. This way we don't have to rely on users reporting alerts they received from ESET."

Some traditional endpoint products have already included this integration, such as Symantec's Endpoint Protection. "I know of a single government employee managing 40,000 endpoints from one central console. That is impressive," says Tony Stirk, president of Iron Horse, a West Virginia security reseller and consultant.

Second, extreme measures such as eliminating or restricting USB ports or introducing air gaps might be necessary for creating the most secure networks. The gaps refer to networks that don't have any live Internet connections. Stirk works with a variety of government clients that employ these measures. While "these networks can be infected by some pretty heavy-duty malware, this malware can't 'phone home' because of the air gap," says Stirk. "And this also means that cloud-based software delivery and online security updates don't work either."

Third is a focus on social networks and social engineering techniques. While not new, in the age of 'everyone is connected to everyone else,' advanced malware can gain entry through false trusted relationships. "Social engineering training and assessments should be added to most organization's security awareness training initiatives," says Andy Hubbard, senior security consultant at Neohapsis. "This is especially important for executives." He also recommends keeping a cool head after you get infected: "Post-infection, it is important to not just blindly rebuild an infected machine but understand that the user data may still have an active infection."

Fourth, keep track of advanced malware by moni-

(CONTINUED ON PAGE 22)

(CONTINUED FROM PAGE 21)

toring your outbound traffic. "We can detect problem machines by the traffic they attempt to send out to the Internet," says Dougan McMurray, IT manager for Brennan IT, an Australian reseller. "This traffic is then blocked, and we track down the machine by IP address and remediate as needed."

Finally, don't depend on tiger teams to fix things post-breach. "Incident response teams are similar to homeowners trying to put out the fire themselves before calling the fire department," says Stirk.

"It isn't always successful. Instead, IT people should be planning for various levels of degradation that could happen for all kinds of reasons—from lost passwords, to death or incapacity of an employee, to a lost communication link," he says.

One example of this lack of planning is the many IT departments that are without formal response plans for distributed denial-of-service attacks. ■

—DAVID STROM

*(Continued from page 20)*

with their own proprietary reputation management systems, so they can tie in their protection and identify particular domains that are known to send advanced malware as well as locate where lots of exploits originate. This means you can deny or allow traffic from particular countries using a simple series of menus.

But with all this technological firepower, it still isn't a fair fight. Tony Stirk is the president of Iron Horse, a consultancy in White Sulphur Springs, West Virginia. He cautions, "Nothing is perfect. Bad people want to hurt you. You will make mistakes. Stuff breaks. Incidents are inevitable. With that in mind, and imagining how things might go wrong, you can start designing in safety procedures that will make things more resilient, and response procedures in case something goes wrong. If you assume that you will eventually get an infection, the only real defense is to have reliable backups and good restore procedures." ■

**DAVID STROM** *is a freelance writer and professional speaker based in St. Louis. He is former editor-in-chief of TomsHardware.com, Network Computing magazine and DigitalLanding.com. Read more from Strom at Strominator.com.*

# TOURING THE DEEP WEB

## Are your employees using Tor to view blocked websites or mining Bitcoins on corporate resources? Sinister or not, it needs to stop.

By Adam Rice

**INTEREST IN THE DEEP WEB** exploded in 2013 as international headlines broadcast the unexpected reach of National Security Agency's mass surveillance programs, and the made-for-Hollywood story unfolded of the Silk Road website and arrest of its alleged proprietor, "Dread Pirate Roberts."

A marketplace for computer hacking and illegal drugs, among other goods and contraband, Silk Road used a Bitcoin-based payment system and "tumbler," which made the identities of the people involved in transactions hard to trace. According to a U.S. criminal complaint, the FBI was not able to defeat the anonymity afforded Silk Road by the onion router (Tor) networks and its decentralized, peer-to-peer Bitcoin payment system, two technologies that underpin much of the deep Web.

Silk Road's alleged proprietor Ross Ulbricht was publicly unmasked because of a simple mistake. In January 2011, a user who identified himself as "altoid" was trying to publicize Silk Road on various websites, including the Bitcoin Talk forum. In October 2011, altoid was looking for an "IT pro in the Bitcoin community" on the Bitcoin

Talk forum and directed interested parties to Ross Ulbricht's Gmail address.

While the deep Web encompasses legitimate activities like scientific research and e-commerce, it poses a major problem for information security professionals, because employee participation in legal pastimes (Bitcoin mining) or illegal pursuits (computer hacking, narcotics and pornography) often goes undetected on corporate networks and devices. These activities, violations of almost any acceptable use policy (AUP), open up organizations to security risks, liability and potential litigation.

## INTERNET PRIVACY WITHOUT ANONYMITY

The deep Web refers to the majority of the World Wide Web that runs over a traditional IP network to fully defined domain names but is not searchable by conventional search engines such as Google or Yahoo. Traditionally, deep websites operated exactly the same as surface websites except they were not linked to other sites, and they opted out of being indexed by search engines. Blocking that traffic was typically done at a Web proxy by allowing access only to approved, categorized websites. Early on, the deep Web was primarily used for storing large data sets (proprietary databases) and hosting restricted or private sites, which were not (necessarily) illegal.

This part of the deep Web does not allow anonymity of the sites or the IP numbers of the people viewing those sites. It rides on the global IP network and is subject to any type of eavesdropping technologies a law enforcement organization or foreign government can deploy.

In 2006, the Tor network was developed with funding from the U.S. Navy and DARPA. It uses multiply relay servers and layers of encryption to create a parallel but truly anonymous Internet that effectively hides the identity of its users. The software to access the Tor networks (.onion) is freely available for download and supports all operating systems. The Tor bundle includes a hardened browser based on Mozilla Firefox and a control panel, which allows users to participate—as relays or proxy endpoints for someone else—and run websites or hidden services such as Silk Road.

The proliferation of the Tor network was not a conduit for a black market on the Internet unto itself. For a black market to thrive, money must change hands anonymously. Otherwise, law enforcement can follow the money trail to the owners of hidden sites and arrest them, which happened before Bitcoin.

## DARKER NET DEVELOPS

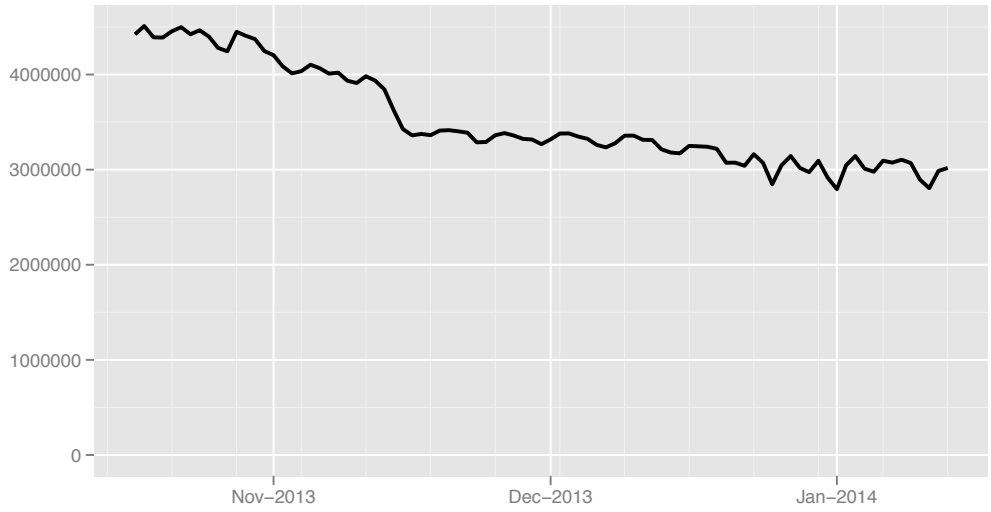
Bitcoin was introduced in 2009 and is now valued against the U.S. dollar for paper currency on global exchanges. (Satoshi Nakamoto, who introduced the Bitcoin concept in a white paper, left the open source project in 2010, according to Bitcoin.org.) Bitcoin is a legal form of currency, and it continues to gain legitimacy as millions of transactions are logged daily and its valuations skyrocket.

Some governments, major retailers (Virgin Atlantic, Overstock.com) and third-party vendors are beginning to explore how to facilitate virtual currency—namely Bitcoin—which appears unstoppable as mobile devices continue to proliferate.

Bitcoins can be traded for goods and services or purchased and redeemed for real money, and all of this can be done anonymously. A cryptocurrency, Bitcoin's shared public ledger is a block chain of chronological transactions. People can buy Bitcoins, or they can "mine" Bitcoins by trading computational power to help manage the Bitcoin encryption. But as Silk Road demonstrates, there's a growing dark side to transactions that are virtually impossible to trace to individuals. Bitcoin, coupled with the Tor suite of technologies, has created a perfect recipe for an underground economy that shields illicit

## Directly Connecting Users

All users directly connecting to the Tor network from multiple countries, Oct. 2013 to Jan. 2014.




*Source: The Tor Project, Inc.*

activities. In March 2013, the U.S. Department of the Treasury's Financial Crimes Enforcement Network issued guidance on the use of virtual currencies, such as Bitcoin.

Today, there is a real underground economy on the Tor networks that deal exclusively in Bitcoin commerce. The top items on the known websites are drugs of all types, computer hacking, forged documents (passports and credentials), guns and, sadly, a lot of child pornography. Some sites claim to provide murder-for-hire services. (Silk Road's Ulbricht allegedly solicited six murders, but there is no evidence that anyone was killed.)

## DOING WHAT THE FBI COULDN'T

Why should any of this matter to enterprise security organizations? While you may not have to worry about murder, employee participation in unapproved activities on the deep Web can take many forms:

- Employees violating the corporate AUP
- Employees using corporate resources to purchase illegal goods and services
- Employees downloading and using the Tor network to bypass edge security controls
- Employees establishing Tor hidden services on corporate networks
- Employees using corporate services to mine Bitcoins
- Tor networks used by intruders to steal data by bypassing security controls

How can you see Tor traffic or Bitcoin mining over a network? Both applications use SSL connections over Web ports but can be adjusted to use any port. This makes discovery of the protocols impossible if you don't use an application-aware firewall or a Web proxy. A typical stateful firewall is going to allow the traffic out along with the rest of the Web traffic, but Tor uses entry, exit and bridge nodes to access the Tor network. Those IPs, while not static, can be found in several places, with some sites claiming to update them every 30 minutes. By developing a blacklist, and then creating an explicit outbound deny rule on your border firewalls based on those IPs, you should be able to stop a lot of the traffic and build a log of all hosts attempting to connect with the Tor nodes. The blacklist must be maintained to remain relevant.

Bitcoin runs on port TCP/8333. Closing that port to all traffic would block Bitcoin effectively, but people can change the default ports. And because it is not dynamic (yet), it is unlikely to run on any other port.

A more graceful solution is to get to the core of the way both Tor networks and Bitcoin communicate. Both technologies use self-generated SSL certificates to encrypt traffic between nodes and servers. Using self-signed digital certificates, or SSL digital certificates not signed by a certificate authority, is a typical communications strategy of botnets and other nefarious actors. As a rule, it's not a good idea to allow outbound SSL traffic across your network at all. Web proxy services are very good at

proxying SSL connections and can stop all traffic using self-signed digital certificates. Because both Tor and Bitcoin run on Web service ports, proxies and application-aware firewalls can inspect traffic deeper in the stack and, regardless of the port, block traffic based on packet content. This stops port hopping and endpoint shifting, which are difficult to manage, and allows for the traffic to be stopped based on its behavior rather than the port, source or destination, which are variable.

## CLEAR POLICY ON TOR USAGE

The proliferation of Tor networks and the coming of age of anonymous digital money mean that companies need to begin to pay attention to the risk of employees using corporate networks and resources to access these sites. Unmonitored activities, criminal or otherwise, can create security risks and liability for organizations.

Prevention should start with awareness, training, and making sure the supporting processes and policies speak directly to the use of the Tor bundle on corporate resources. Once the AUP is updated, it is important to communicate to the entire staff that downloading the Tor bundle on any company computer or use of the Tor network over company networks is a fireable offense. Once the policy is in place and communicated, then the traffic should be stopped, and attempts logged for investigation. ■

**ADAM RICE** *is an information security professional with 17 years of experience. He has served as chief information security officer at a defense and aerospace Fortune 500 company; chief security officer of a global telecommunications company; general manager and vice president of a managed security services business; director in several network consulting companies; and is a retired U.S. Army non-commissioned officer. He is also a regular contributor to several information security publications.*

# Snowden, BSafe and Fixing the Math

*Throwing a curve: Is there a potential weakening of security products and services courtesy of the NSA?* BY ROBERT RICHARDSON

**ONE OF THE RESPONSES** to early salvos of former NSA contractor Edward Snowden's surveillance releases was "trust the math." That's how security veteran Bruce Schneier put it in a posting to his blog site. Snowden himself, when answering reader questions on the *Guardian* website, said, "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

A lot of us heaved a huge sigh of relief upon hearing that. Not because NSA surveillance will reveal our big, dark secrets, but if the security community can't say with confidence that it stores the world's digital data *securely*, it's time to dismantle the industry. And beyond that, privacy is essential. A sense of privacy fosters self-aware, independent identities, which are fundamental to creating modern civilization.

## PROBLEMS IN THEORY

It appears Snowden was wrong—at least, partially—about NSA's access to encrypted data. Or, perhaps, he was putting a lot of weight on the phrase "properly implemented." Because if you had hung your trust on RSA, the security division of EMC Corp.'s BSafe cryptosoftware, and used its default settings (Dual Elliptic Curve Deterministic RBG algorithms), it's pretty clear that the NSA had a backdoor to your plaintext. Snowden should have been aware of this issue. (When his identity was first revealed in the *Guardian*, he said, "I carefully evaluated every single document that I disclosed to ensure that each was legitimately in the public's interest.")

On the other hand, Snowden had a *lot* of documents, and there are plenty of instances where you have to line up the PowerPoint slides side-by-side to make sense of what the NSA is allegedly up to. Whether Snowden was aware of the BSafe alleged backdoor or not, the backdoor was there.

This backdoor was essentially a class break—the NSA could violate the protections of anything encrypted with the default BSafe arrangement. It was a completely different approach than selectively "pwning" equipment or software distributed to specific targets (which the NSA has also done).

In this instance, you couldn't really trust the math. The core precepts of encryption (e.g., products of very large prime numbers are hard to factor) may still hold. But one element at least that's darned nearly as important—the ability to pick pseudorandom numbers that others can't systematically guess—is up for grabs.

## SHUTTING THE DOOR ON SURVEILLANCE?

But it's worse than that. There are perfectly good reasons to suspect even more security problems that the NSA discovered or, perhaps, purposefully injected. As reports surface alleging that various products from Cisco Systems Inc., Dell Corp. and other major hardware vendors have potential security weaknesses, only Apple Inc. has responded with a truly ironclad-sounding denial of any involvement in the NSA's surveillance activities. Other

The core precepts of encryption (e.g., products of very large prime numbers are hard to factor) may still hold.

responses have seemed rather carefully worded. Huawei Technologies Co., for instance, released a statement that said it will "conduct appropriate audits to determine if any compromise has taken place and to implement and communicate any fixes as necessary."

That's just the hardware vendors. I'm no mathematician, but it doesn't appear that we're entirely out of the woods, based on the NSA's capabilities for directly weakening or attacking cryptosystems—namely, elliptical curve-based algorithms, the mechanism used in Dual_EC_DRBG, one of four DRBGs standardized by the National Institute of Standards and Technology (NIST SP 800-90A) in 2007.

Peter Woit, a senior lecturer in the mathematics department at Columbia University, blogged back in September that there was speculation in the math community that "there are other ways in which NIST standard elliptic curve cryptography has been compromised by the NSA (see here for some details of the potential problems)." Woit noted:

*[T]he NSA for years has been pushing this kind of cryptography (see here), and it seems unlikely that either they or the NIST will make public the details of which elliptic curve algorithms have been compromised and how (presumably the NIST people don't know the details but do know who at the NSA does).*

We can't trust the math. Some of it needs to be reexamined publicly, and soon. The industry—and, in particular, vendors that say they'll fix any surveillance-enabling vulnerabilities "as necessary"—need to pour on the funding for research and standards development that returns us to a state where we can store data with confidence that it's secure. ■

**ROBERT RICHARDSON** *is the editorial director of TechTarget's Security Media Group. Follow him on Twitter @cryptorobert.*

# TechTarget Security Media Group



TechTarget
275 Grove Street,
Newton, MA 02466
www.techtarget.com



**About TechTarget:** TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER IMAGE AND PAGE 4: SERGEY NIVENS/FOTOLIA