Editor: David Ladd, daveladd@microsoft.com

Security, Privacy, and Policy Roundup

Lee Garber

SECURITY

US National Security Agency director Army General Keith Alexander has said the hacking group Anonymous could have the capabilities necessary to attack the nation's electricity grid, thus causing limited power outages, in the next two years. Alexander's warning reflects increasing concern about Anonymous's capabilities. Although Anonymous hasn't claimed it wants to cause a blackout, some US officials say the group appears to be heading toward more disruptive attacks. Power suppliers say that their systems are attacked regularly and have invested in defense mechanisms and backup systems to use in case of a disruption. However, US officials express concern that even a power-grid attack with limited success could cause alarm.

Sony, which incurred several high-profile security breaches last year, has announced that it was hit again, this time by hackers who stole more than 50,000 music tracks, including unreleased music from the company's Michael Jackson catalog. Sony Music paid the late Jackson's estate US$250 million in 2010 for a seven-year deal for the rights to his songs. The theft occurred shortly after Sony's PlayStation Network was compromised last year. The company says it only recently discovered the problem via routine social network monitoring and is unclear how much, if any, of the stolen music has made its way online.

Apple plans to introduce its new Gatekeeper security model when the company releases OS X Mountain Lion this summer. The OS will permit users to install only those programs accessed from the Mac App Store or those digitally signed by registered developers. Apple will link each of its digital certificates to a specific developer. If a developer eventually releases a malicious application, Apple will know who is responsible and can revoke the applicable certificate. According to Apple, Gatekeeper will block Trojan horses executed after users have been tricked into downloading and installing malicious software.

According to former employees, hackers had access to much of Nortel Networks' system for perhaps a decade, reportedly breaking into its network from China-based Internet addresses as early as 2000. They used seven passwords stolen from Nortel executives, hid spying software, and downloaded many documents including technical papers, R&D reports, and business plans. According to the internal report, Nortel took no security steps after discovering the breach other than resetting the passwords. Nortel—which is selling its assets to companies such as Avaya and Ciena as part of its bankruptcy—didn't comment on reports of the security breach. Former employees said the company didn't try to find out whether its products were compromised by hackers before selling its assets and didn't disclose the problem to potential buyers.

The number of attacks on and the amount of malware targeting devices running Google's Android OS appear to be increasing. Android is the world's most popular smartphone OS with 52.5 percent of the global market, according to market research firm Gartner Inc. Mobile-security company Lookout said 4 percent of Android users encountered malware during 2011, up from

1 percent in 2010. Researchers have found several new and more sophisticated types of Android malware in the wild recently. For example, Opfake—a bogus browser that automatically calls premium phone lines, running up user costs—regularly mutates to stymie antivirus detection, an approach previously seen only on PC malware. In response, Google released the Bouncer application-prescreening tool, which executes server-based simulations to check whether programs exhibit malicious behavior and stops those that do from getting onto the Android Market app store.

Google has added the Chromium OS to the list of products for which it offers bounties to people who find security problems. Since November 2010, Google has paid $410,000 to approximately 200 researchers who found 730 qualifying vulnerabilities in its Web applications and services, and $300,000 for problems found in its Chromium open source browser. Google says the bounties it pays make its products safer and amount to a fraction of the cost the company would need to find all the vulnerabilities itself.

VeriSign, an important provider of critical Internet-related services, recently admitted that it was hacked several times in 2010. It confirmed that the attackers successfully stole data and, in response, the company implemented new defensive measures. VeriSign acknowledged the incidents in a filing with the US Securities and Exchange Commission last year, but they didn't come to light until recently. The firm operates a large part of the Internet's infrastructure along with security services such as cyberthreat reporting. The company has said that the attacks probably didn't affect the servers that support its Domain Name System network but has provided little additional information. In 2010, VeriSign sold its authentication business unit—which provided Secure Sockets Layer, public-key-infrastructure, and other services—to security vendor Symantec. Security experts say that if the hackers acquired VeriSign digital certificates—something Symantec claims didn't occur—they could use them to exploit Internet communications for malicious purposes.

Hackers have been using search results as a way to identify targets in the latest in a series of mass SQL injection attacks. Researchers monitoring the attacks say the latest version might have infected a million webpages using automated tools and search-engine based reconnaissance. The most recent iteration redirects victims who land on an infected page to Lilupophilupop.com, which displays either a fake antivirus-software site or a page that asks them to download an Adobe Flash update. The goal is to convince victims to download software—in some cases for a fee—that can cause problems once installed. Hackers, sometimes employing bots, can use search engines to identify which websites are vulnerable to SQL injection attacks on the basis of, for example, their use of software packages with known bugs.

PRIVACY

Netflix recently paid $9 million as part of a settlement associated with a privacy-related lawsuit. Documents related to the matter say the settlement involved the Video Protection Privacy Act (VPPA), a 1988 US law that forbids the release of video rental histories and requires the deletion of rental records within a year after an account closes. The Associated Press reported that two Virginia residents sued Netflix, alleging it kept records for up to two years after individuals canceled their subscriptions. Netflix, which didn't comment on the settlement, has opposed parts of the VPPA in the past.

The Electronic Privacy Information Center (EPIC)—a public-interest research and advocacy center—has sued the US Federal Trade Commission to make the FTC stop Google from implementing controversial privacy-policy changes. In court papers, EPIC said the planned changes violate a consent order that Google entered into in October 2011. Google plans to start tracking users on, and sharing information among, its various services, including its search engine, the Google+ social networking site, and Gmail. EPIC is asking the FTC to seek a temporary restraining order and preliminary injunction to try to halt implementation of the plans. EPIC is basing its actions on a complaint it made to the FTC about the Google Buzz social networking site, which operated in 2010 and 2011. The complaint alleged that Gmail users couldn't opt out of Google Buzz and that the site publicly exposed user data without consent. As part of a settlement, Google paid $8.5 million to a fund to support privacy organizations.

The US Federal Bureau of Investigation has issued a warning about a phishing scam that could let hackers steal consumers' banking-related user names and passwords. The FBI says the Gameover phishing scam encourages users to open email attachments by attributing them to US government financial institutions, such as the Federal Reserve Bank or the Federal Deposit Insurance Corporation.

The email tells victims there's a problem with their bank account or a financial transaction and that they should click an included link to help resolve the issue. The link takes victims to a phony website from which they download the Gameover malware, which infects their computers and steals their banking information. Gameover is a variant of the notorious Zeus malware, which was designed to steal financial data.

Hackers are using a variant of an older worm, Ramnit, to steal Facebook login credentials, send malicious links to victims' contacts, and gain remote access to corporate networks. In the past, hackers used Ramnit to bypass financial institutions' online security systems, compromise online banking transactions, and intrude into corporate networks, explained threat-management-services company Seculert. Recently, Seculert set up a sinkhole and, after examining diverted traffic, found that Ramnit had infected 800,000 machines between September and December 2011. The company also discovered that a new variant of the worm stole 45,000 Facebook login credentials, primarily in France and the UK.

POLICY

US President Barack Obama has proposed an online-privacy bill of rights that would make it easy for users to opt out of or into Internet tracking. The US Commerce Department now plans to work with businesses and privacy advocates to develop enforceable policies based on the White House proposal. The bill of rights would let consumers communicate with one click whether they want Internet companies to track their online activity. It also calls for reasonable limits on the amount of personal data online businesses can collect and retain, and would require them to store the information securely. In addition, the proposal would let consumers access their data and ensure its accuracy. The privacy bill of rights doesn't impose any requirements on companies. Instead, it is primarily designed to provide a road map of policies that businesses will have to determine how best to implement and that the US Congress could use in designing future legislation. The Digital Advertising Alliance—which includes 90 percent of advertisers associated with Google's, Microsoft's, and Yahoo's advertising networks—recently agreed to implement a Do Not Track button for major Web browsers.

The European Union is proposing that websites in its 27 countries be required to remove personal images and information shortly after users request that they be deleted, or face fines up to 2 percent of their global revenue. Proponents say it's important that Internet users have control over their personal information and how it's utilized. Opponents claim that this proposal is imprecise, is a radical expansion of privacy rights, and could violate freedom-of-expression rights. They say it would be difficult to enforce, given that the Web distributes data globally. They also contend it would conflict with US policies and make the Internet much less open.

The US Senate has proposed a law that would require companies running networks important to US national and economic security to better defend their systems from hackers. If the bill—which combines parts of several measures introduced in the past three years—becomes law, the US Department of Homeland Security would identify critical systems that would cause catastrophic physical or economic damage if attacked. DHS would then set regulations requiring the networks' operators to improve security or face penalties. Proponents say such a law is necessary to cope with increasingly sophisticated attacks that could disrupt power grids, financial systems, and important communication networks. Industry groups, including the US Chamber of Commerce, have said the bill is too broad and could unnecessarily raise costs for companies. A study by the Bloomberg Government news-analysis service found that US banks, utilities, and other organizations that run critical networks would have to raise computer-security spending from $5.3 billion to $46.6 billion per year to stop 95 percent of attacks. The momentum for comprehensive cybersecurity legislation has increased with the number of recent attacks against major defense contractors and financial institutions.

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*