Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 157
31 Αυγούστου 2009

Hackers Stole IDs for Attacks
Wall Street Journal (08/17/09), S. Gorman

Russian hackers stole US identities and software tools for use in a cyberattack against Georgian government Web sites during the war between Russia and Georgia in 2008, according to a new report by the US Cyber Consequences Unit. The report says that Russian hackers converted Microsoft software into a cyberweapon and collaborated on popular US-based social-networking sites, including Facebook and Twitter, to coordinate attacks against Georgian sites. Although the cyberattacks were closely examined following the war, the connections to the US had remained hidden until this year. Personal and credit card information stolen from US citizens was used to register Web sites that launched the botnet attacks, and once the attacks started, Facebook and Twitter were used to exchange attack code and encourage others to join the attack. Experts say the study shows how cyberwarfare has outpaced military and international agreements, which do not account for the possibility of using US resources and civilian technology as weapons. Identity theft, social networking, and modifying commercial software are all common attack strategies, but combining these strategies raises the attack to a new level, says former US Dept. of Homeland Security cybersecurity chief A. Yoran. White House officials are now studying how laws of war and international obligations need to be adjusted to account for cyberattacks. The US Cyber Consequences Unit says the Georgian attacks were perpetrated by Russian criminal groups, and had no clear link to the Russian government, but the time of attacks, which started only hours after the military invasion started, suggests the Russian government may have at least indirectly coordinated with the cyberattackers.

Internet 'Immune System' Could Block Viruses
New Scientist (08/12/09)

A system that fights highly infectious computer viruses by embedding defense mechanisms in key parts of the Internet has been developed by University of North Carolina at Chapel Hill researcher S. Coull and Rensselaer Polytechnic Institute professor B. Szymanski. The modus operandi of computer worm infection is malware scanning the Internet for vulnerable computers and transferring itself to those systems. Coull and Szymanski say the isolation of worms entails coaxing the Internet's core computers or autonomous systems to collaborate, and each system is managed by an Internet service provider (ISP). In their model, the researchers imbued each system with the ability to spot a compromised computer, which may announce itself by making a series of random requests to link to other computers, the majority of which will fail. Once a threat within the autonomous system's network is detected, the system stops receiving and forwarding messages from the infected computer, and also notifyes its peer autonomous systems about the identity of the threat. Upon the recognition of a genuine threat, all autonomous systems can contain the compromised computer or computers and halt the worm's spread. Coull and Szymanski's model indicates that the viability of this strategy depends on cooperation between about 30-35% of the autonomous systems in the Internet. Collaboration and trust between the ISPs running the systems would be essential, Coull says.

Web Tools Help Protect Human Rights Activists
Reuters (08/19/09), J. Finkle

A new generation of Internet privacy tools is being developed to prevent governments from gathering data, such as where users access the Internet from. One tool, called Tor, scrambles information before sending it over the Web, hiding the user's location. Tor can bypass firewalls, which makes it a popular tool among activists in countries such as China and Iran. Tor connects users to a second PC that links to a third computer, which does not know the location of the first machine, making it impossible to trace the identity of the person accessing the Web. "Tor is a tunnel," says Tor Foundation executive director A. Lewman. "What you send into it comes out the other end, untouched." The US government has contributed $250,000 of the $343,000 in income the foundation reported in 2007. Tor enables surfers to bypass Internet censorship software, whether it is implemented by a government or a company aiming to keep workers off of sites such as Facebook while at work. It also can protect against identity theft and deletes all Web session information after closing a browser. Tor was used to coordinate demonstrations following the disputed presidential election in Iran, and has been used in China and Iran to enable citizens to access Gmail, Twitter, and other communication sites when blocked by their governments. The adoption of Tor has been hurt by its speed, as not all users allow traffic to flow through their computers, which makes the service slower than regular Web browsing. A similar technology is Freegate, which was developed by the banned Fallun Gong movement in China.

NSF Defers to Universities on Ethical Standards
Chronicle of Higher Education (08/20/09), P. Basken

The National Science Foundation (NSF) has published rules in the Federal Register that would make universities responsible for providing ethics training. Under the America Competes Act, which was designed to improve US competitiveness in mathematics and science, all NSF grant recipients must be trained in the "responsible and ethical conduct" of research. The rules would require institutions to certify that they have provided ethics training, but they would not be routinely asked to describe the actual content of the instruction. However, universities would be subject to review upon request. The NSF plans to provide some guidelines for teaching ethics, including workshops and online resources, but they would not involve specific content standards. "Training needs may vary depending on specific circumstances of research or the needs of students," the NSF says.

Online Social Networks Leak Personal Information to Third-Party Tracking Sites
Worcester Polytechnic Institute (08/24/09), M. Dorsey

A Worcester Polytechnic Institute (WPI) study by professor C. Wills found that the practices of many popular social networking sites can make personal information shared by users on their pages available to companies that track Web user browsing habits. The study, presented at the Workshop on Online Social Networks, part of ACM's recent SIGCOMM 2009 conference, described the method that tracking sites could use to directly link browsing habits to specific individuals. Wills says users are given a unique identifier when they sign up with a social networking site, and when social networking sites pass information to tracking sites about user activities, they often include the identifier, giving the tracking site a profile of Web browsing activities and the ability to link that profile to a user's personal information. Wills says this is a particularly troubling practice for two reasons. "First, users put a lot of in-

formation about themselves on social networking sites. Second, a lot of that information can be seen by other users, by default." A unique identifier could give a tracking site access to a user's name, physical address, email address, gender, birth date, education, and employment information. Wills says he does not know what, if anything, tracking sites do with unique identifiers given to them by social networking sites, and while the Web sites provide users with tools to protect themselves, the best way to prevent privacy leaks would be for social networking sites to stop making unique identifiers visible.

Defying Experts, Rogue Computer Code Still Lurks
New York Times (08/26/09), J. Markoff

Conficker, a rogue software program that was discovered spreading across the Internet last November, continues to baffle top security experts working to eradicate the program and discover its origin and purpose. Conficker uses a flaw in Windows software to co-opt machines and connect them to a virtual computer that can be remotely controlled by the software's creators. More than 5 million computers, including government, business, and home computers in more than 200 countries, are now under the control of Conficker, giving the malicious program computing power far beyond the world's largest data centers. Computer security experts from industry, academia, and the government are working together in a highly unusual collaborative effort to stop the program. So far, their efforts have succeeded in decoding the program and developing antivirus software that removed the software from millions of computers. "It's using the best current practices and state of the art to communicate and to protect itself," says Conficker Working Group director R. Joffe. "We have not found the trick to take control back from the malware in any way." Researchers speculate that Conficker could be used for a variety of purposes, including sending massive amounts of spam, stealing information such as passwords and logins by capturing keystrokes, or delivering fake antivirus warnings to trick users into buying fake antivirus software. Perhaps the most concerning possibility is that the virus was not launched for criminal purposes, but rather by an intelligence agency or military in a foreign country looking to monitor or disable another country's computer network.

New Attack Cracks Common Wi-Fi Encryption in a Minute
IDG News Service (08/27/09), R. McMillan

Hiroshima University's T. Ohigashi and Kobe University's M. Morii say they have developed a way to break the Wi-Fi Protected Access (WPA) encryption system used in wireless routers in about one minute. Last November, researchers demonstrated how WPA could be broken, but the Japanese researchers have taken the attack to a new level. The first attack worked on a smaller range of WPA devices and required between 12 and 15 minutes to execute. Both attacks work only on WPA systems that use the Temporal Key Integrity Protocol (TKIP) algorithm, and neither work on newer WPA 2 devices or WPA systems that use the more secure Advanced Encryption Standard algorithm. Wi-Fi Alliance's K. Davis-Felner says WPA with TKIP was developed as a type of interim encryption method when Wi-Fi was first evolving, and Wi-Fi-certified products have had to support WPA 2 since March 2006. "There's certainly a decent amount of WPA with TKIP out in the installed base today, but a better alternative has been out for a long time," Davis-Felner says. Most enterprise Wi-Fi networks feature security software that would detect the man-in-the-middle attack described by the Japanese researchers, says Errata Security CEO R. Graham, but the development of a practical attack against WPA should give people a reason to dump WPA with TKIP.