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

Δελτίο 100
28 Δεκέμβρη 2007

DNS Attack Could Signal Phishing 2.0
IDG News Service (12/11/07), R. McMillan

Researchers at the Georgia Institute of Technology and Google are examining "open recursive" DNS servers, which translate domain names into Internet Protocol addresses to tell computers how to locate each other on the Internet. Open-recursive DNS servers reply to all DNS lookup appeals, which makes them valuable to hackers. Researchers estimate that 17 million open-recursive DNS servers currently exist on the Internet, 0.4% of which are acting maliciously by returning incorrect answers to DNS queries. An additional 2% of such servers are supplying questionable results. Together, these servers are beginning to undercut the Internet's trustworthiness, researchers say. "These hosts are like carnival barkers," says Georgia Tech researcher D. Dagon. "No matter what you ask them, they'll happily direct you to the red light store, or to a Web server that does nothing more than spray your eyeballs with ads." Criminals have been attacking DNS systems for at least four years by using computer viruses to change DNS settings in victim's computers. However, only recently have the criminals possessed the expertise and technology, such as Web-based malware, to consistently mount open-recursive DNS attacks in a pervasive way, the researchers report. "It's really the ultimate back door," says IBM's C. Rouland. "All the stuff we've deployed in the enterprise, it's not going to look for this."

Gold Medalist Computer Scientist Boosts ID Security
Frederick News-Post (MD) (12/10/07), S. Boin

National Institute of Standards and Technology computer scientist J. Dray received his third gold medal from the US Dept. of Commerce for developing a secure government identification card with a computer chip that contains secret information. "Nothing is 100% foolproof, but these are essentially unforgeable," Dray says. Dray developed the card for Homeland Security Presidential Directive 12, which called for the development of a common identifycation standard for federal workers and contractors. The card was approved under the personal identification program enacted in August 2004 and will be issued to all government employees, contractors, and military personal within a few years. The card contains an electronic chip that will be customized for the person who carries it. "This is a tremendous step forward for secure identification," Dray says. "It will fit all government agencies." Dray says the practice of encoding information so only the person it is intended for can read it is becoming the foundation of anything online in a computer system. "Identification in the online world is kind of a fundamental societal issue," he says. "It doesn't look like it's going to go away."

We're All at Risk' of Attack, Cyber Chief Says
Technology Daily (12/11/07), L. Viana

G. Garcia, the Homeland Security assistant secretary, spoke to the New York City Metro InfraGard Alliance on Tuesday regarding the importance of cybersecurity. InfraGard is an alliance between the private sector, the FBI, and local law enforcement striving to safeguard key infrastructures, including technology systems. Garcia pointed out that over 85% of the nation's critical infrastructures are owned and operated by private industry, which "means the federal government cannot address these cyber threats alone." Though roughly $6 trillion passes through the US financial system on a daily basis, major companies continue to leave their networks vulnerable to data theft and infiltration. The federal government depends on organizations such as InfraGard and information-sharing centers to drive industry to take cyber safety measures. The collaborations are becoming increasingly valuable as hackers grow more sophisticated and as the market for cybercrime surges. On the government end, the Homeland Security Department's Einstein network scans systems for intrusions or irregularrities and distributes threat data within hours. Currently, 13 agencies use Einstein, but Garcia urges all agencies to participate. Garcia also advises industry to take into consideration the physical threats, such as a pandemic flu outbreak, that could impact networks, and to incorporate such scenarios into their contingency network plans. In March 2008, the department will administer Cyber Storm II, an exercise to rehearse synchronized responses to simulated strings of cyberattacks involving all levels of industry and government.

NIST Looks to Cook Up a New Hash
Government Computer News (12/10/07) Vol. 26, No. 30, W. Jackson

The National Institute of Standards and Technology has launched a competition for a new crypto algorithm for digital signatures and message authentication, and is accepting submissions for what will become the Secure Hashing Algorithm-3. The algorithms currently in use, SHA-1 and SHA-2, have not been broken, but weaknesses are starting to appear, says NIST security technology group manager W. Burr. The two current standards likely still have several years of use left, and Burr says it is prudent to find a new algorithm. Developing a new algorithm that meets the requirements will be difficult, as it needs to be at least as secure as the algorithms in use but more efficient regarding speed and computational resources required to run it. The new algorithm must also be similar enough to SHA-2 that it can directly substitute for it in any application, but must be different enough that a successful attack against SHA-2 will not affect the new algorithm. The selection process will be radically different from previous secure hashing algorithm development and selection, which tool place behind close doors. NIST will examine and test algorithms, but submissions will also be made public so outside evaluators can test the submissions for weaknesses.

ACM Group Honors Computer Security Experts for Innovation and Service
AScribe Newswire (12/14/07)

ACM's Special Interest Group on Security, Audit and Control (SIGSAC) has award its top honors to the University of California, Santa Cruz's Dr. Martin Abadi and George Mason University's Dr. Sushil Jajodia for their work in computer security technologies. Abadi received the SIGSAC Outstanding Innovation Award for his fundamental contributions to the application of logic and probability to information security, while Jajodia received the SIGSAC Outstanding Contributions Award for his research and teaching contributions to the information security field and his service to ACM SIGSAC and the computing community. Abadi, a Principle Researcher at Microsoft Research, contributed to authentication in distributed computer systems as well as the design and analysis of security protocols for authentication. Jajodia, a former SIGSAC chair and founding co-editor-in-chief of the Journal of Computer Security, made fundamental contributions to access control, information flow, multilevel security, and critical infrastructure protection.

Vote of No Confidence

Columbus Dispatch (OH) (12/15/07), M. Niquette

A nearly $2 million review of Ohio's voting systems found "critical security failures" across the board, prompting Democratic Secretary of State J. Brunner to propose a sweeping replacement of electronic touch-screens and optical-scan systems with a system that uses a paper ballot scanned at a central site. Her proposal also involves the elimination of voting in neighborhood precincts in favor of large "vote centers" where voters from five to 10 precincts would cast their ballots, with voting beginning 15 days prior to an election. The review determined that vote results could be compromised with "fairly simple techniques," while county elections officials chosen to review the part of the study by a group of academic experts reported that the findings are "generally based on pure supposition and bias." Brunner counters that the systems fail to meet minimum industry standards for computer security, and admits that making significant changes before Ohio's March 4 primary in all but one county is unlikely. However, she wants the statewide revamping complete by the next presidential election, and P. Rosenfeld with the League of Women Voters of Ohio agrees that the state must make an overhaul. The voting-system vendors whose products are used in Ohio released statements insisting that their devices are reliable and accurate. Brunner's proposal faces the scrutiny of a Republican-led legislature, while Ohio State University law professor D. Tokaji argues that her plan will create more problems than it solves.

Cyber Security Should Be Personal Priority for All Leaders
Government Technology (12/13/07)

Cyber security must become a top concern for CEOs, according to a new report from the British-North American Committee and the Atlantic Council of the United States. CEOs who fail to prioritize cyber security leave their companies vulnerable to industrial espionage, as illustrated by the recent cyber attacks on Royal Dutch Shell, Rolls-Royce, and other large companies. "As enterprise on the Internet has become more sophisticated, so have cyber criminals," says ICANN President P. Twomey, one of the report's authors. "The message of this report is clear--senior government figures and leaders of corporations need to make cyber security a personal priority." The report, "Cyber Attack: A Risk Management Primer for CEOs and Directors," describes information security threats and common data security mistakes. The report also offers suggestions for controlling cyber security risks, such as developing a wide-ranging information security policy to be carried out by senior management. Conducting an enterprise-wide security audit, regularly testing security measures, and staying current on security best practices are other recommendations advanced in the report. "Much work is needed to increase the security of the Internet and its connected computers and to make the environment more reliable for everyone," warned former ICANN president V. Cerf in the report. "Security is a mesh of actions and features and mechanisms. No one thing makes you secure."

E-Voting Machines Rejected in Colorado
Associated Press (12/19/07), G. Merritt

Colorado's Secretary of State M. Coffman recently declared many of Colorado's electronic voting machines to be unreliable, decertifying three of the four voting-equipment manufactures certified in the state. Coffman said some of the machines could still be used in November if a software patch can be installed, and other machines could be replaced with equipment certified for use in other states, but both of these solutions would require the approval of state legislature. Six of Colorado's 10 most populous counties, including Denver, will be affected by Coffman's decision, which cited problems with accuracy and security. The machines previously certified in Colorado were built by Premier Election Solutions, formerly known as Diebold Election Systems, Hart InterCivic, Sequoia Voting Systems, and Election Systems and Software. Only Premier had all of its equipment pass the recertification process. ES&S' K. Fields said the decertification was based on recently imposed additional requirements, and Hart InterCivic's P. Lichtenheld said Hart InterCivic plans on appealing based on how Colorado conducted the tests and maintenance of its machines. In his announcement decertifying the machines, Coffman said Colorado's actions will have national repercussions, and that the federal certification process is inadequate.

Malware Flood Driving New AV
InfoWorld (12/14/07), M. Hines

Symantec security experts watched as customers participating in a research project downloaded approximately 65,000 new applications during a week-long period in November 2007. The experts analyzed the software and identified as many as 60 percent of the applications as malicious. The statistics illustrate a worrying trend--that malicious applications are outstripping legitimate programs on the Web--which may compel Symantec to alter its strategy for fending off threats. Malware criminals find gaps in popular applications such as Web browsers using fuzzing tools, and then check their attacks against anti-virus products to ensure their efficacy. As a result, "most new malware is going undetected by commercial security products," explains C. Nachenberg of Symantec. Moreover, malware authors are increasingly using server-side polymorphism, which hooks many victims by "producing a copy for as few as two or three people and then re-writing it; so, if we get one version we can remove it from a few computers, but not all the variants," says Nachenberg. Accordingly, standard countermeasures will have to be supplemented with new strategies. One new tactic involves using distributed data collection capabilities to study usage patterns of various applications. Such patterns could help security vendors distinguish malware from valid software, and would allow vendors to suggest that individuals avoid questionable programs. However, if the number of new malware programs continues to exceed the production of legal programs, anti-virus vendors may have to adopt a white-listing approach to spot good applications rather than attempting to pursue all the bad applications.

Hackers Have Poor Nations' PCs in Their Sights
New Scientist (12/15/07)No. 2634, P. 22; M. Reilly

Cybersecurity remains an untamed frontier in developing countries, allowing hackers to operate and wreak havoc with near-total impunity. "All in all, you have a perfect recipe for botnet attacks in the developing world," notes E. Zuckerman of the Berkman Center for Internet and Society. He observes that hacker activity rises dramatically once a country achieves 10-15% Internet penetration. The International Telecommunications Union (ITU) is rolling out a global effort to implement cybersecurity measures that the developed world uses within the Third World, but it will be a formidable challenge. Poorer nations do not possess the funds for countermeasures nor the technical training to erect effective cyberdefenses, partly because the cost of Internet connectivity is much higher than it is in industrialized countries. Africa, which is already beset with economic turmoil and computer vulnerability, could become even more ripe for cyber-exploitation as cheap, streamlined computers become widely available through initiatives such as the One Laptop Per Child program. International cooperation is essential to the improvement of developing nations' cyberdefenses, says the University of Cologne's M. Gercke. Seymour Goodman of the Georgia Institute of Technology cites the importance of organizing national computer emergency response teams (CERTs), which would analyze the type of attack and the required countermeasures while also informing ISPs, and the ITU wants to supply the expertise and training to set up CERTs in all developing countries.