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

Δελτίο 129
20 Σεπτέμβρη 2008

Researchers Build Malicious Facebook Application
IDG News Service (09/05/08), J. Kirk

Researchers from the Foundation for Research and Technology in Heraklion, Greece, and the Institute for Infocomm Research in Singapore, have built Facebot, a malicious program for Facebook as part of an experiment to demonstrate the dangers of social networking applications. The researchers developed a Photo of the Day application that provides a new National Geographic photograph daily, but every time the application is activated it sends a flood of traffic to a victim's Web site, causing a denial-of-service attack. The researchers uploaded the Facebot application to Facebook in January and nearly 1,000 people have installed it in their profiles. The researchers then monitored traffic on a Web site they established for a Photo of the Day attack. If the traffic patterns observed could be applied to a Facebook application with a million or more users, the researchers estimate that a victim's Web site could be flooded with as much as 23 megabits/sec of traffic. The researchers say Facebook applications have a highly-distributed platform, offering significant firepower for anyone that controls the applications. Facebook applications also can access users' personal data, making it possible to record and transfer personal data to a remote server. Social networking sites can take measures to prevent such malicious applications, by ensuring that applications cannot interact with hosts that are not a part of the social network, and by vigorously verifying new applications added to the social networking site.

Safer Skies for the Flying Public
EurekAlert (09/03/08)

University of Texas professor C. Caramanis is working with researchers at the MIT to develop a computer model that would serve as the foundation for an air traffic control system that optimizes the flow of air traffic. The system would be capable of taking thousands of variables into consideration and quickly changing flight recommendations without input from humans. The system would track weather conditions, current airplane locations, probable routes, and other variables. "The complicated nature of the process, and the need to make quick adjustments when changes occur, will best be addressed with a mathematical model that combines theories and calculations from probability, statistics, optimization modeling, economics and game theory," Caramanis says. "There is currently no unified decision-making framework for air traffic flow optimization." Timeframes for taking off and landing are provided by the federal government, and they are estimates that are based on a number of variables. The air traffic optimization model also will be designed to help reduce delays and flight cancellations.

U.N. Agency Eyes Curbs on Internet Anonymity
CNet (09/12/08), D. McCullagh

Technologists and privacy advocates are very concerned by the United Nations' (UN's) International Telecommunication Union's (ITU's) drafting of technical standards proposed by the Chinese government to define techniques of tracing the original source of Internet communi-

cations and potentially restricting the ability of users to maintain anonymity. "What's distressing is that it doesn't appear that there has been any real consideration of how this type of capability could be misused," says Electronic Privacy Information Center director M. Rotenberg. One of the most disturbing aspects of the initiative is that it could institutionalize a means for governments to suppress their opposition, which conflicts with the UN's Universal Declaration of Human Rights, notes Columbia University computer scientist S. Bellovin in a recent blog post. Countering distributed denial of service (DDoS) attacks is the most commonly cited rationale for IP tracebacks, but Bellovin says the method's usefulness in this regard has waned because few attacks employ spoofed addresses, there are too many sources in a DDoS attack to be useful, and the source computer inevitably would turn out to be compromised anyway. Technologist J. Appelbaum warns that a traceback system would offer malevolent hackers the ability to commit wrongdoing without being caught, thus abusing the very system that is designed to trace them. The official charter of the ITU's Q6/17 group states that it will work "in collaboration" with the Internet Engineering Task Force and the US Computer Emergency Response Team Coordination Center, which could supply a route toward widespread acceptance. A formal legal mandate to adopt IP traceback would likely be blocked by the First Amendment in the United States.

Standards for Accreditation of Labs That Test Voting Machines Inconsistent
NextGov.com (09/10/08), J. Aitoro

The National Institute of Standards and Technology (NIST) should have stronger standards for accrediting laboratories that test voting machines, concludes a Government Accountability Office (GAO) report. The report says NIST continues to use generic international standards to make sure people testing the voting machines were qualified, rather than following the requirements of the 2002 Help America Vote Act. Four labs have met NIST's standards through May 2008. NIST has only recently started to detail what the labs need to demonstrate to earn accreditation, but still does not disclose a number of self-imposed steps. GAO says NIST should make sure testers are qualified and trained properly, and document each laboratory review. Also, the Election Assistance Commission (EAC), which receives recommendations from NIST, should demand full documentation of accreditation steps, defined qualifications for accreditation reviewers, maintenance of appropriate records, and create standards for determining the financial stability of labs. "Opportunities exist for NIST and EAC to further define and implement their respective programs in ways that promote greater consistency, repeatability, and transparency--and thus improve the results achieved," the report says.

D.C. Election Glitch Blamed on Equipment
Washington Post (09/11/08) P. A1; N. Stewart; E. Silverman; P. Flaherty

DC election officials say that a defective computer memory cartridge is responsible for what appears to be thousands of write-in votes that officials say should not exist. The malfunction generated inaccurate results in several contests, including two high-profile council races. In the Republican at-large race the glitch caused 1,560 write-in votes at 9:50 p.m. to drop to 18 by 12:16 a.m., and thousands of votes were added to individual candidates, inflating vote totals. At 9:50 p.m., 8,246 ballots were recorded cast in the at-large Republican primary, but the number of ballots cast shrank to 3,735 by 12:16 a.m. Board spokesman D. Murphy says it was determined that a defective cartridge caused the vote totals to duplicate into multiple races on the summary report issued by the office; he says the board immediately caught and addressed the error. However, University of California, Berkeley professor H. Brady questions the explanation that a defective cartridge caused errors across multiple races. He also won-

ders why so many write-in votes were released even as an unofficial count on election night because any experienced election official should know that write-in votes are never that frequent. "It is strange that a single cartridge would cause results to double across the District, and it also would be strange to have that show up in one race," says Election Data Services president K. Brace. "Why wouldn't it have duplicated other contests in that precinct or more than one race?"

US Sees Six 'Disruptive Technologies' By 2025
Computerworld (09/11/08), P. Thibodeau

The Global Trends 2025 report, prepared by US intelligence agencies and expected in December, will likely include a list of six disruptive technologies expected to have a major impact on the world. The report defines a disruptive technology "as a technology with the potential to cause a noticeable--even if temporary--degradation or enhancement in one of the elements of US national power." Six technologies were identified to have that potential. Biogerontechnology involves technologies that improve lifespan, which will challenge the economy and social policy as people live longer. Energy storage systems, such as fuel cells and ultracapacitors, could replace fossil fuels. Crop-based biofuels and chemicals will reduce gasoline dependence. Clean coal technologies can improve electrical generation efficiency and reduce pollutants. Robots have the potential to replace humans in a variety of professions, ranging from the military to health care. Lastly, Internet pervasiveness will expand to everyday objects, such as food packages, furniture, and paper documents, streamlining supply chains, lowering costs, and reducing dependence on human labor.

Hackers Hit Large Hadron Collider Web Site
Computerworld (09/12/08), G. Keizer

The European Organization for Nuclear Research (CERN) says it has revived a Web site for the Large Hadron Collider (LHC) that was attacked by hackers, although it remains off limits to the public. CERN says the Web site was only defaced, as hackers temporarily replaced the Web site with a message. The network did not suffer any permanent damage, and no other files were installed on the science project's computers. "It was benign, but it reminds us that we need to be vigilant," says J. Gillies of CERN, which operates LHC. "And no harm was done to the experiment or its computer network." Turning on the LHC for a test search of particles that make up dark matter has generated some controversy, in that some people have argued that it would create a black hole that could destroy the planet. A report in the UK newspaper the Telegraph says a group called the Greek Security Team (GST) has claimed responsibility for the attack.

Putting a 'Korset' on the Spread of Computer Viruses
American Friends of Tel Aviv University (09/09/08)

Tel Aviv University professor A. Wool and graduate student O. Ben-Cohen have developed Korset, an open source antivirus program for Linux-based servers. "We modified the kernel in the system's operating system so that it monitors and tracks the behavior of the programs installed on it," Wool says. Wool says Korset provides a model for the operating system kernel that predicts how software on the server should run. If the kernel detects abnormal activity, it stops the program from working before malicious actions can occur. Wool says their solution is much more efficient and does not consume as many resources as traditional antivirus software. "There is an ongoing battle between computer security experts and the phenomenal

growth of viruses and network worms flooding the Internet," he says. "The fundamental problem with viruses remains unsolved and is getting worse every day." Wool's research was presented at the recent Black Hat Internet security conference.

Threat From DNS Bug Isn't Over, Experts Say
Dark Reading (09/08/08), T. Wilson

Security experts have only temporary solutions so far for the critical DNS flaw, which if exploited on a large scale could bring down the entire Internet. Since vendors simultaneously installed a patch after IOActive researcher D. Kaminsky discovered the flaw earlier this year, the number of servers vulnerable to an attack has dropped dramatically, from >85% to <30%. Still, experts warn that the patch is a temporary fix and only hinders attackers from exploiting the flaw. "What we've got out there so far are truly Band-Aids," says A. Shimel, chief strategy officer at StillSecure, the firm that has been monitoring the vulnerability since its discovery. "There are questions on how to move the solution to the firewall level. We need a new DNS." Attackers are already trying to find ways around the patch. MessageLabs analyst P. Wood has seen a surge in traffic by hackers searching out systems with unpatched vulnerabilities.

Critics: Homeland Security Unprepared for Cyber-threats
CNet (09/17/08), S. Condon

The US Dept. of Homeland Security (DHS) is being criticized for its lackluster cyber-security efforts on the grounds that it has proven to be inefficient, bureaucratic, and unable to monitor federal computer networks. Some have even suggested that DHS should no longer be trusted with its cybersecurity mission and another federal agency should be given the task. "While DHS has improved, oversight for cybersecurity must move elsewhere," says J. Lewis, a senior fellow at the Center for Strategic and International Studies. "This is now a serious national security problem and should be treated as such." Lewis testified at a recent hearing of the House Homeland Security's subcommittee on emerging threats, cybersecurity, and science and technology. Adding to public criticism of DHS are two reports published by the Government Accountability Office (GAO). Since 2005, the GAO has reported on DHS' cyber-security efforts and has made 30 recommendations to the department, but DHS "still has not fully satisfied any of them," says GAO director of information management issues D. Powner. The GAO's latest reports include descriptions of DHS' failure to fully address 15 key cyber-analysis and warning attributes related to activities such as monitoring government networks for unusual activity.

Voting Group Release Guidelines for E-Voting Checks
IDG News Service (09/15/08), G. Gross

About 20 US states using electronic-voting systems currently do not audit the results after elections, but there is still time to change that policy, according to a coalition of fair elections advocates and e-voting critics. The groups, including Common Cause, Verified Voting, and the Brennan Center for Justice, called on states to require post-election audits of e-voting systems, including touch-screen voting machines and optical-scan systems. The groups released a set of recommendations for election audit best practices, which calls on states to hand count paper records generated in conjunction with many e-voting systems. Verified Voting president P. Smith says audits can help restore voter confidence in elections. Since the 2000 US presidential election, e-voting machines have been blamed for lost votes in several elections.

In August, Ohio Secretary of State J. Brunner filed a lawsuit against Premier Election Solutions, saying the company should pay damages for dropped votes in the state's March primary election. Audits after the election found hundreds of uncounted votes. Premier first denied its machines were to blame, but later admitted that programming errors were at fault. "Audits really help to restore the public trust in our voting systems," says M. Toulouse Oliver, county clerk for Bernalillo County, N.M. "When there is a lack of trust in how that vote came out or how that transition took place, it can cast aspersions on our system of government."