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

Δελτίο 168
15 Φλεβάρη 2010

Hacking for Fun and Profit in China Underworld
New York Times (02/02/10), D. Barboza

Internet security experts say Chinese hackers are behind an escalating number of global attacks to steal credit card information, commit corporate espionage, and wage online warfare against other nations. In China, and in some parts of Eastern Europe and Russia, computer hacking has become a lucrative hobby for skilled hackers. "They make a lot of money selling viruses and Trojan horses to infect other people's computers," says author S. Henderson, who has spent years tracking Chinese hackers. There are conferences, training academies and magazines all devoted to providing information about hacking. In China, there is a loosely defined community of hackers who work independently, but who also sell their services to corporations and the military. One such hacker, going by the code name Majia, says he does not work for a major Chinese technology company because it would limit his freedom, so he must remain underground. Majia and other hackers keep a tight hold on their hacker secrets, including knowledge of software flaws such as zero-day vulnerabilities, for future use.

Google to Enlist NSA to Help It Ward Off Cyberattacks
Washington Post (02/04/10) P. A1; E. Nakashima

Google and the US National Security Agency (NSA) are collaborating to fortify defences against future cyberattacks. NSA will assist Google in studying an assault that allegedly originated in China and targeted Google's computer networks. The agreement also calls for NSA to aid Google in understanding whether it is deploying the proper security measures by assessing vulnerabilities in hardware and software and to calibrate the adversary's level of sophistication. Sources say the partnership will permit the two organizations to exchange crucial data without breaching Google's policies or statutes that shield the privacy of US citizens' online communications. NSA also reportedly is reaching out to other government agencies that play major cybersecurity roles and might be able to assist in the Google probe. "As a general matter, as part of its information-assurance mission, NSA works with a broad range of commercial partners and research associates to ensure the availability of secure tailored solutions for Dept. Defence and national security systems customers," says NSA's J. Emmel.

Code Defends Against "Stealthy" Computer Worms
Penn State Live (02/01/10), A. Messer

Pennsylvania State University (PSU) researchers have developed an algorithm that defends against the spread of local scanning worms that search for hosts in "local" spaces within networks or subnetworks. The algorithm works by estimating the size of the targeted host population and monitoring the occurrence of infections. It then sets a threshold value just equal to or below the average number of scans necessary to infect a host. "By applying the containment thresholds from our proposed algorithm, outbreaks can be blocked early," says PSU postdoctoral fellow Y.-H. Choi. The algorithm was tested and proved to be able to determine the size of the susceptible host population as well as an efficient estimator of worm virulence.

"Our evaluation showed that the algorithm is reliable in the very early propagation stage and is better than the state-of-the-art defence," Choi says.

US Oil Industry Hit by Cyberattacks: Was China Involved?
Christian Science Monitor (01/25/10), M. Clayton

Industrial espionage is shifting from traditional intelligence gathering methods to Internet intelligence capture, as evidenced by a series of cyberattacks against the oil industry that are believed to have been executed by foreign governments or their surrogates. Multiple sources say that Marathon Oil, ConocoPhillips and ExxonMobil were breached by attacks that used a combination of bogus emails and customized spyware programs to target specific data. This has led to speculation by experts that the parties behind the attacks were "Level 3" intruders who may have been connected to a foreign government. Still, it is difficult to prove infiltration, given many companies' unwillingness to admit to having been hacked. Furthermore, many corporate executives are not aware of the growing sophistication of espionage software and still resort to outdated electronic safeguards. Some of the cyberattacks on the oil giants were traced to China, but there is no definitive proof that the Chinese government or even Chinese nationals were responsible. On the other hand, the oil intrusions coincide with increasing numbers of coordinated assaults in the United States that experts do consider China to be accountable for. In the end, experts say it is less important for US industry to know who is responsible than to recognize and prepare for the expanding threat of cyberespionage.

'Rugged' Initiative Brings Secure Software Development to the Masses
DarkReading (02/05/10), K. J. Higgins

The Rugged Software Development Initiative (RSDI) was recently launched by security experts in an effort to ensure that the software writing process includes thinking about security from the very start. RSDI will encourage developers to create resilient software capable of withstanding attacks while performing its normal functions, says The 451 Group's J. Corman, who helped developed the initiative along with OWASP chair J. Williams and the Monterey Group's D. Rice. They describe RSDI as a value system for writing secure software, as opposed to a compliance program, and they hope to incorporate the tenets of rugged code development into computer science programs at universities. Unlike other security initiatives, RSDI does not include any new frameworks for secure coding. Instead, Corman says it will serve as an "on-ramp" for secure software development. He envisions the initiative leading to scenarios such as programmers voluntarily pledging to be Rugged software developers or developing an Underwriters Laboratory label for measuring a software's ruggedness.

Secure Radio Signal for Central Locking
Fraunhofer-Gesellschaft (02/10)

Fraunhofer Institute for Secure Information Technology (SIT) researchers have developed a prototype remote car key that is more secure than the existing central locking systems of auto manufacturers. SIT's remote key uses an asymmetric algorithm, which allows the key to have its own separate code, and also means the information no longer has to be embedded in the car. The SIT team used an asymmetric algorithm, even though they are associated with high levels of computation intensity and energy consumption. "We have built a small cryptographic chip, which is particularly energy-saving," says SIT scientist J. Heyszl. "In addition, we have developed a new, efficient protocol which minimizes computation effort and the amount of data that has to be transmitted." The prototype offers the same battery life and enc-

rypts the electronic immobilizer the same way as central locking systems that use symmetric algorithms.

In Cyber War, Most of U.S. Must Defend Itself
Defense News (02/01/10) Vol. 25, No. 5, P. 29; W. Matthews

There are concerns that the United States is extremely vulnerable to a full-scale cyberattack, and the US Cyber Command is not in a position to protect US civilian computer networks, as its primary responsibility is to defend military networks. R. Clarke, who served as the president's special cybersecurity adviser during the Bush era, recently wrote that the Dept. of Homeland Security "has neither a plan nor the capability" to protect very much of the US's cyber infrastructure. Furthermore, he said private-sector businesses "almost uniformly believe that they should fund as much corporate cybersecurity as is necessary to maintain profitability and no more." Meanwhile, US military networks are under constant cyberattack because they are such an appealing target, according to Deputy Defense Secretary W. Lynn. "And the frequency and sophistication of attacks are increasing exponentially," he notes. McAfee's D. Alperovitch says that a number of foreign governments, including China, France, Russia and Israel, are equipping themselves with advanced cyber-offensive technologies. McAfee hints at the possibility that countries are competing in a quiet cyber arms race, and communications systems, banks, and power grids are just as likely to be targets as military networks.

China Alarmed by Security Threat From Internet
New York Times (02/11/10), S. LaFraniere, J. Ansfield, J. Markoff

China is increasingly worried about threats to its security and political stability posed by the Internet. Both Chinese and US political analysts and technology experts say China's attempts to tightly control the Internet are partly fueled by the conviction that the West is trying to foment unrest in China and weaken the country from a military standpoint through the use of a wide range of communications innovations. US experts say China's cyberdefenses are more riddled with holes than those of the United States. New policies are being set up to replace foreign hardware and software with domestic systems, while officials also are broadening the reach and resources of state-controlled media outlets so they reign over Chinese cyberspace with their blogs, videos, and news. Unrest in Xinjiang and elsewhere, allegedly stoked by online warfare from the West, has prompted Chinese leaders to step up new efforts, including the closure of thousands of Web sites, tightening censorship of text messages for objectionable content, and planning a convergence of China's Internet, phone, and state TV networks. They also are nurturing domestic alternatives to foreign computer technologies and foreign-based Web sites such as YouTube, Facebook, and Twitter.

Federal Government Builds Secret Database to Fight Cyber-Terrorism
Computerworld Australia (02/11/10), D. Pauli

Australia's federal government has been given sensitive data from utilities, banks, and other organizations for the Critical Infrastructure Protection Modeling and Assessment (CIPMA) program. "Identifying, tracking the cascading effects of [critical infrastructure (CI)], and quantifying these consequences is a key rationale for establishing the CIPMA program," says a spokesperson from the Federal Attorney General's department. "Direct relationships with industry means that there is a high level of trust to enable the provision of accurate data for modeling and analysis." Approximately 4 TB of CI data will be warehoused in central databases, making it unnecessary to retrieve information from knowledge experts who may not

be accessible in a disaster. System dynamic models are employed to analyze stock and flow data in CI, such as network connectivity and the energy output of generators, to produce an amalgamated output to be fed into a People, Building, and Infrastructure profile. Data is then deconstructed into demographic, economic, and business profiles, and into statistical divisions to generate novel disruption footprints. The CIPMA program is one of numerous actions that authorities have recently taken to counter increasing numbers of cyberthreats.