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

Δελτίο 145
15 Απρίλη 2009

Vast Spy System Loots Computers in 103 Countries
New York Times (03/29/09), J. Markoff

Researchers at the University of Toronto's Munk Center for International Studies say a massive electronic spying operation has successfully stolen documents from hundreds of government and private offices around the world. The researchers say the system was controlled from computers almost exclusively in China, but they cannot conclusively say the Chinese government is involved. The researchers were asked by the office of the Dalai Lama to examine its computers for signs of malware and discovered a vast operation that, in less than 2 years, managed to infiltrate at least 1,295 computers in 103 countries, including computers belonging to many embassies, foreign ministries, other government offices, and the Dalai Lama's Tibetan exile centers in India, Brussels, London, and New York. The researchers say that in addition to spying on the Dalai Lama, the system, which they named GhostNet, also focused on governments in South Asian and Southeast Asian countries. GhostNet is by far the largest, in terms of the number of countries affected, spying operation to be exposed, and it is believed that this is the first time that researchers have been able to uncover the workings of a computer systems used for intrusions of such magnitude. The researchers say GhostNet continues to infect and monitor more than a dozen new computers a week. The malware not only "phishes" for unwary victims but also "whales" for specific, important targets. The malware can even turn on the video and audio features of an infected computer, enabling the malware's operators to see and hear what goes on in front of the computer. The researchers have notified international law enforcement agencies of the spying operation, which they believe exposes shortcomings in the legal structure of cyberspace.

Experts See Early Activity From the Conficker Worm
New York Times (04/01/09) P. A14; J. Markoff

An informal group of computer security experts said they have observed early attempts by the Conficker virus to communicate with a control server, but they are unsure if the attempts were successful. The Conficker malware, which has aggressively spread since October, is designed to unite infected machines into a botnet. Security researchers who have examined the most recent version of the malware, Conficker C, said it was ready to try to download commands from an unknown Internet location on April 1. Although the choice of April Fool's Day has led some experts to speculate that the program may be a hoax, others warn that Conficker, which has infected at least 12 million computers, could cause serious harm. Nevertheless, security specialists agree that it will most likely take several days before the purpose of the program can be determined. The program was intended to start contacting 50,000 Internet domains on April 1st. In a global effort, researchers created a system that will trap all of the attempted botnet communications, which involves monitoring the domains of 110 countries. A spokesperson for the Conficker Cabal, a security working group organized by computer security companies, says as of March 31st the group has no new information on the activity of Conficker. IBM says company researcher Mark Yason has decoded Conficker's internal communication protocol, which will make it easier for security teams to detect and interrupt the program's activities.

Intruder Alert: TAU's 'Smart Dew' Will Find You!
American Friends of Tel Aviv University (03/26/09)

Tel Aviv University researchers have developed Smart Dew, tiny sensors as small as dewdrops that can be arranged in a network. The inexpensive sensors are equipped with a controller and a radio-frequency transmitter/receiver. Tel Aviv University professor Y. Shapira says a Smart Dew network has no scale limitations, which would make it useful on farms or boarders where it would be too difficult and impractical to install fences or constantly send patrols. "Most people could never afford the manpower to guard such large properties," Shapira says. "Instead, we've created this Smart Dew to do the work. It's invisible to an intruder, and can provide an alarm that someone has entered the premises." Each sensor can detect an intrusion within a parameter of 50 meters at a cost of about 25 cents per sensor. A major benefit of Smart Dew is that it is nearly impossible to see. "Smart Dew is a covert monitoring system," Shapira says. "Because the sensors in the Smart Dew wireless network are so small, you would need bionic vision to notice them." Each Smart Dew sensor can be programmed to monitor a different condition. The sensors can detect the presence of metal, sounds, temperature changes, carbon monoxide emissions, vibrations, or light. Each sensor sends a radio signal to a base station, which collects and analyzes the data.

Advances in Data Safety Drawing Wider Attention
University of Texas at Dallas (03/25/09), D. Moore

University of Texas at Dallas (UTD) computer scientist B. Thuraisingham recently traveled to Australia and Taiwan to discuss the school's research in the field of assured information sharing. Thuraisingham is leading an effort, with UTD professors L. Khan, M. Kantarcioglu, and K. Hamlen, to develop an assured information-sharing lifecycle, with each researcher working on a different challenge. Thuraisingham has developed a prototype system for policy-based information sharing to handle untrustworthy partners, Kantarcioglu has developed techniques based on game theory to manage semi-trustworthy partners, Khan has developed data-mining techniques to obtain defensive information operations with untrustworthy partners, and Hamlen is examining program rewriting techniques that address offensive information operations executed by untrustworthy partners. "We are exploring the application of policy-based information sharing for health informatics and beginning collaborations with healthcare experts," Thuraisingham says. "We are also applying semantic Web technologies for information sharing and have projects with the National Science Foundation, the Intelligence Advanced Research Projects Activity, and the National Geospatial-Intelligence Agency."

Senate Legislation Would Federalize Cybersecurity
The Washington Post (04/01/09), J. Warrick; W. Pincus

The US Senate is considering legislation that would give the federal government an unprecedented amount of control over the security of the nation's information technology (IT) networks. The bill would broaden the US government's cybersecurity efforts to include private IT systems that control important infrastructure, such as the electric grid and water systems. In addition, the legislation would create the Office of the National Cybersecurity Adviser, which would report directly to the president and oversee cybersecurity efforts across all federal agencies. The bill also calls on the National Institute of Standards and Technology to create measurable and auditable cybersecurity standards that both the government and private companies would be forced to meet. The legislation also contains several other provisions, including one that calls for an ongoing, quadrennial assessment of the US's cyberdefenses. The introduction of the legislation comes amid concerns that a sustained attack on the nation's private computer networks could compromise or shut down the IT systems used by banks, utilities, transportation companies, and other essential service providers. "People say this is a military or intelligence concern, but it's a lot more than that," says J. Rockefeller IV (D-W.Va.), one of the bill's cosponsors. "It suddenly gets into the realm of traffic lights and rail networks and water and electricity."

Purdue, Rutgers Will Lead $30 Million U.S. Homeland Security Research Center
Purdue University News (04/02/09), F. Fiorini

Purdue University and Rutgers University will lead an international research and education group in a six-year, $30 million US Dept. of Homeland Security project dedicated to creating methods and tools for the analysis and management of massive amounts of information generated by missions in all areas of homeland security. Homeland Security's new Center of Excellence in Command, Control, and Interoperability will include Purdue and Rutgers teams, which will contribute to developing new methods to assist Homeland Security personnel in preparing for, detecting, preventing, responding to, and recovering from terrorist attacks and natural and man-made disasters. Purdue and 14 other universities will focus on visualization sciences, and Rutgers will explore data sciences. Already the center has formed partnerships with local, state, and national groups to provide university researchers with real-world examples to test and refine technology. Purdue professor and center director D. Ebert says turning vast amounts of data into manageable information is vital to homeland security. "For example, in the event of a catastrophe such as a chemical spill, natural disaster, disease outbreak or a terrorist attack, information will be coming from many sources, including camera images, data from sensors and simulations, and text documents from police and health-care agencies," he says. "The amount of information gathered during a crisis can be crushing if not managed correctly." Ebert says his team will expand on previous work by the Purdue University Regional Visualization and Analytics Center.

French Lawmakers Reject Internet Piracy Bill
Associated Press (04/09/09), S. Sayare

French lawmakers have unexpectedly rejected a bill that would have created the world's first surveillance system for Internet piracy, forcing Internet Service Providers to disconnect customers accused of making illegal downloads in certain cases. The proposed law would have allowed music and film industry associations to hire companies to analyze the downloads of individual users to detect piracy, and report violations to a new agency overseeing copyright protection. The agency would have been permitted to use the downloading computer's unique Internet Protocol address to trace illegal downloads to individuals. After the first violation the agency would send a warning by email, while a second violation within three months would warrant a second warning by certified mail, and a third violation within a year would allow the agency to force the service provider to terminate service. Music labels, film distributors, and artists say that the bill is a decisive step toward eliminating online piracy. An earlier version of the bill was passed by the French Senate, but when the bill was presented to a near-empty National Assembly, it was rejected by a vote of 21 to 15. The government plans to resubmit the measure to both houses of parliament after the legislators return on April 27. Some French activists say that the law represents a Big Brother intrusion on civil liberties, and say that users downloading from public Wi-Fi hotspots or masked IP addresses could be impossible to trace.

Researchers Enhance Spam Call Filtering
Helsinki University of Technology (04/02/09)

Helsinki Institute for Information Technology (HIIT) researchers are developing a new system for filtering spam calls for Internet-based telephony. Internet-based telephone services such Skype, which offers free calls using peer-to-peer networks, are rapidly growing in popularity, but they carry with them an increased risk of spam calls. HIIT researchers J. Koskela, J. Heikkila and A. Gurtov have developed a system for filtering calls on peer-to-peer networks with more flexibility. The new system allows users to accept calls from people who are unknown to the user, but are in the contacts of that user's friends, or even friends of those friends, instead of only accepting phone calls from immediate friends or accepting all calls. Users can be alerted about unknown callers before they answer as well. The increased flexibility makes spam call prevention more practical, and makes it easier to filter unwanted calls. The objective of the new system is to implement an application integrating Host Identity Protocol and Peer-to-Peer Session Initiation Protocol, which provides VoIP and IM capabilities using trust chains to prevent spam calls. A challenge the system faces is finding a way to form trust chains from call trace data without violating privacy. HIIT, a joint research institute of the Helsinki University of Technology and the University of Helsinki, focuses on future Internet research and basic and strategic research in information technology.

Should Online Scofflaws Be Denied Web Access?
New York Times (04/13/09) P. B4; E. Pfanner

Policy makers attempting to make Internet access widely available while deterring digital piracy face the dilemma of defining such access as either a basic human right or a privilege earned by good behavior. This issue was raised recently by French lawmakers' rejection of a plan advocated by President Nicolas Sarkozy, which called for terminating Internet access for people who disregard repeated warnings to stop using unauthorized file-sharing services. "There's increasing understanding that broadband is fundamental to basic economic and social participation," says Organization for Economic Cooperation and Development economist S. Wunsch-Vincent. "Some people wonder whether this is consistent with cutting off Internet connections." In March, the European Parliament adopted a nonbinding resolution defining Web access as a fundamental freedom that could only be restricted by a court of law. Envisional's D. Price says that although file sharing by peer-to-peer networks seemed to be flattening worldwide, sites that offered alternatives to downloading, such as streaming of pirated movies, were quickly proliferating. Pirates also are resorting to file-hosting services that let users upload files that are too large to email, to be downloaded by others.

Cyber Spying a Threat, and Everyone Is in on It
Associated Press (04/09/09), P. Haven

The computers of Tibetan exiles and the US electrical grid were recently breached by hackers, highlighting the growing threat of cyber espionage. The White House is currently finishing a 60-day review of how the federal government can better use technology to protect electronic information such as the US's electrical grid, the stock market, tax data, airline flight systems, and even nuclear weapon launch codes. The US Dept. of Homeland Security reports that in 2008 there were 5,499 known breaches of US government computers by malicious software, a big jump from the 3,928 known breaches in 2007 and 2,172 in 2006. A former US government official says the hackers who compromised the electrical grid could have left behind computer programs that will allow them to disrupt service. He also says the sophistication of the attack indicates that it was state-sponsored and the government does not know the extent of the attack because federal officials cannot monitor the entire grid. "We expect that the attacks we've seen are only the tip of the iceberg," say the official, who requested anonymity because he was not authorized to discuss details. "We follow the attacks to their source, and many come from China."

A New Technology to Secure Integrated Systems and Circuits
Centre National de la Recherche Scientifique (04/02/09), L. Louis

The Laboratoire d'Informatique de Robotique et de Microelectronique de Montpellier (LIRMM) has developed Secure Triple Track Logic (STTL), technology that reduces data leakage in integrated circuits during electronic transactions. STTL can protect the integrated circuits in smart cards, SIM cards, processors, and other pieces of hardware that need both data authentication and confidentiality. STTL reduces data leakage from integrated circuits by up to 95%, compared to conventional logic circuits, through two distinctive features. STTL has constant computation time and keeps the circuit's power consumption at a steady level. LIRMM also has developed a framework for a collection of small components, using STTL logic, capable of performing basic functions.