10-06-2009

Please be cautious when surfing the Internet! Please read article below.

Internet Has Never Been More Dangerous, Report Says
By Thomas Claburn
Read the Original Article at **InformationWeek**

The proliferation of malware online keeps setting new records and security experts are worried. Between January and June this year, the number of fake antivirus programs detected grew by 585%, according to a report released on Wednesday by the Anti-Phishing Working Group. During the same period, the number of banking trojans, designed to steal account information for financial sites, increased 186%. The number of phishing Web sites reached 49,084, the second highest number recorded since the record of 55,643 in April, 2007. And the number of hijacked brands hit an all-time high of 310 in March and remained at a high level through June. "The Internet has never been more dangerous," said APWG Chairman David Jevans in a statement. "In the first half of 2009, phishing escalated to some of the highest levels we've ever seen. Of even greater concern is the skyrocketing sophistication and proliferation of malicious software designed to steal online passwords and user names. New malicious software such as the Zeus trojan, exhibit a level of sophistication that would make the best software programmers envious." According to the APWG report, the number of infected computers rose by more than 66% between Q4 2008 and the end of June 2009 to reach almost 12 million, 54% of the computers scanned. The Zeus trojan figures prominently in another security report released on Wednesday. Finjan's Cybercrime Intelligence Report examines the increasing sophistication of software designed for online banking theft and notes that some of these programs, such as the URLzone trojan, have developed anti-forensic techniques to conceal account looting from automated anti-fraud systems and from the eyes of victims. "The cybergang knows, that once the victim reports the fraudulent money transfer to his/her bank, their 'business' will end then and there," Finjan's report states. "To minimize this risk, the Trojan creates a forged bank report page that is then presented to the victim, effectively hiding the fraudulent transaction." The report says that, in addition to their own malicious Web sites, cybercriminals have been using the LuckySploit cybercrime toolkit to compromise legitimate Web sites to infect the computers of Web site visitors. Based on screenshots the company obtained of one criminal gang's LuckySploit control panel, the gang managed to attract 90,000 visitors in 22 days and to infect 6,400 of them -- a 7.5% success rate. Finjan says the gang it tracked earned about $438,000 (300,000 Euros) during this 22 day period and estimates that it could make $7.3 million annually at that rate. The tech industry's response to these trends can be seen in initiatives like Microsoft's online anti-scam campaign, it's newly released free Security Essentials software, and calls for greater industry cooperation. No doubt there's more to be done.

Jerry Rodriguez
Managing Director, Information Technology
Texas Tech University Health Sciences Center El Paso