IT Security Threats in 2011 – How to Prepare

ATLANTA -- (BUSINESS WIRE) -- Stonesoft, an innovative provider of integrated network security and business continuity solutions, reveals what organizations should prepare for in 2011. With more than 20 years of experience in network security, Stonesoft's predictions shed light on the end of Apple OS invulnerability, the evolution of Stuxnet and advanced evasion techniques (AETs).

"The bearing themes in 2010 were definitely Stuxnet, social engineering attacks and advanced evasion techniques, and I am pretty confident that the threats of 2011 will evolve around these themes as well," says Joona Airamo, chief information security officer at Stonesoft.

Stonesoft's predictions include:

1. An Apple OS targeted virus. As the Apple OS becomes more commonly used, there will be a nasty worm or virus specifically targeted to this operating system.

2. Increased malware attacks for social media. There will be an increase in the number of malware related attacks through social networking sites like Facebook and Twitter, with a single attack affecting thousands (or even millions) of people. Just like the old email scams, the malicious file will look like it has been sent from the initial target so recipients will trust the source.

3. Political cyber warfare. We can expect to see more "information warfare"-type attacks on nation states. The political motivation in the attacks will increase, even though the attacks with a financial motivation will clearly remain dominative.

4. Social engineering against the enterprise. There will be a rise in targeted 'social engineering' attacks. Sophisticated hackers will undertake thorough investigations of people in order to penetrate corporate networks for significant financial gain.

5. Stuxnet-like attack proliferation. We will see more attacks like Stuxnet. The target will be critical infrastructure, such as government and military systems. The attacks will remain rare because hackers need to be very well resourced in order to build a virus of this magnitude. Stuxnet was made up of four zero-day vulnerabilities and the one used also by the Conficker worm. Its complexity and the expense of developing the virus both point in the direction of it being a government sponsored attack.

6. Smartphone takes center stage. The smartphone is set to become a more prominent target for hackers, and understandably so. The number of smartphones sold may soon bypass the number of PCs sold.

7. Viruses become more sophisticated. Hackers will be even more promiscuous in quickly spreading viruses far and wide. They will try to improve their "return of

investment" by making sure no vulnerability is left unused and by utilizing the full window of opportunity when the security patches are not yet installed.

8. Advanced evasion techniques will grow if ignored by the network security vendor community. Stonesoft's recent discovery of Advanced Evasion Techniques (AETs) means that the whole Intrusion Prevention System (IPS) vendor community will have to unite in order to build sufficient protection to mitigate against this new method of attack.

For information on how to protect against these threats, please visit: http://cts.businesswire.com/ct/CT?id=smartlink&url=http%3A%2F%2Fwww.stonesoft.com&esheet=6574397&lan=en-US&anchor=www.stonesoft.com&index=1&md5=70f3e68c31ed7d8a0782f6cf3fe3ca31