SECURITY Oct 14, 2011 3:10 pm

SpyEye Malware Continues to Plague Computers

By Jeremy Kirk, IDG News

The SpyEye banking malware continues to plague computers across the world and is proving to be a difficult foe to detect and remove from infected Windows PCs, according to two researchers from EMC's RSA security division.

SIMILAR ARTICLES:

SpyEye Patch Source Code Is a Double-Edged Sword

SpyEye Trojan Targets Online Banking Security Systems

Speedy Malware Infects More than 6 Million Web Pages

Protect Yourself From DNSChanger

Remove Hard-to-Kill Malware

Malware Destroyed My Data

Uri Rivner, who is head of new technologies for consumer identity protection, and Jason Rader, chief security strategist, both donned white lab coats for their session at the RSA security conference in London on Thursday for a technical tear-down and review of SpyEye.

The two researchers also changed their titles: Rivner became part of the dangerous malware department at RSA General Hospital and Rader the head of research for the malware epidemic division of the U.S. CDC (Centers for Disease Control and Prevention).

SpyEye has been around for more than a year and is the successor to the Zeus banking malware. SpyEye emerged after the author of Zeus, who went by the screen name "Slavik," stopped developing it. But another person by the name "Harderman" took over the project, Rivner said.

SpyEye is a kit that is sold to other online criminals. It's easy to use, and people need a high level of technical skills to conduct an attack.

A potential cybercriminal who buys the kit can use the nice graphical interface set up so-called "drop zones," or servers to receive stolen online banking credentials. SpyEye also has configuration files customized for attacking most online banking websites. For example, it can inject extra fields over a bank's Web page, asking for information other than a login and password, such as the victim's credit card number and PIN.

Those fields appear to be a seamless part of the legitimate Web site but actually are fake, exporting the entered data to the server in the cybercriminal's drop zone.

People are unlikely to notice they've been infected SpyEye, Rivner said. "Getting infected is very, very easy," he said.

One way people get infected is by visiting a website that has been tampered with by hackers. The site will contain a 1x1 pixel that pulls JavaScript from a different server and begins testing to see if the victim's computer has unpatched software, Rivner said. Last year, the U.S. Treasury's website was modified in such a way to deliver the Zeus trojan.

SpyEye uses a variety of tricks to stay hidden, Rader said. It will inject itself in DLLs, or dynamic link libraries -- code libraries used by applications -- that are legitimate. SpyEye can also delete its own installation files. "It stays persistent," Rader said.

On Wednesday, Microsoft said it was updating its Malicious Software Removal Tool to detect malware in the SpyEye family.

The move is undoubtedly good for users, but the MSRT might have a hard time: Rader said full-featured antivirus security suites often miss new variants of SpyEye, taking an average of 45 days to add detect for fresh variants.

The MSRT also can only detect malware if it is actually running on the machine and also cannot prevent a Windows computer from being infected by SpyEye, which some antivirus suites may be able to stop.

Send news tips and comments to jeremy_kirk@idg.com

Comments (0)