itbusiness.ca
Business Advantage through Technology

Print

6 weird malware tricks hackers use to bypass security

Security experts presenting in the upcoming SecTor conference reveal six new tactics that cyber criminals are employing to circumvent security and avoid detection.
9/26/2011 6:00:00 AM
by Nestor E. Arellano

The mobile malware deluge everybody has been warning about may not be upon us – yet. But a couple of security experts say this should not lull businesses into a false sense of security.

Tablets, smartphones, laptops and desktops are primary targets of cybercriminals and they continue to change their tactics and arsenal to avoid detection, according to Nicholas Percoco and Jibran Ilyas.

Percoco, is senior vice president of SpiderLabs, a team of ethical hackers and researchers at Trustwave, a Chicago-based data security and payment card industry compliance management software company. Ilyas, is senior security consultant for forensics at Trustwave. Percoco and Ilyas will be speaking in a forum titled Malware Freak Show at the upcoming SecTor security conference in Toronto next month.

In a talk with ITBusiness.ca recently, Ilyas and Percoco outlined six new tactics that cyber criminals are currently employing to circumvent anti-malware tools and to avoid detection.

The days when hackers and cyber criminals launched a one shot attack with a single weapon are long gone, according to Percoco, who has more than 14 years of information technology security experience under his belt. “Much like legitimate software developers, malware coders now follow a software life cycle development pattern,” he said.

“Malware is created with future variants already in mind so as to make it harder for anti-malware tools and security researchers to zero in on the attackers,” Ilyas said.

Here are six cyber tricks that have become popular in the last two years:

Impersonation – As recently as 2009, attackers were fond of using off-the-shelf malware with names that actually identified them as malware, according to Ilyas. “Forensic experts investigating an infected machine would find embedded malware named something like networksniffer.exe or keylogger.exe. It was pretty easy to identify them as malicious.”

Increasingly, however, malware developers have been naming their creations so that they appear as legitimate files. For example, some malware are coded to appear like real Windows files, said Ilyas.

One solution is to concentrate of the behaviour of the suspect file, he says. “Stalk the process not the label. Find out how the suspect file is behaving and what it is doing to the system.”

Stealing data in transit – With the increasing awareness of the need to encrypt data, attackers are now more frequently going after data in transit when more often than not, encryption is not used, said Percoco. Data in temporary storage such as credit card and is also generally not encrypted until they are stored in back-end servers.

“The attackers have a very small window of opportunity before the data is encrypted so they go for it with all they've got,” he said.

Crooks now using encryption – Two can play the encryption game, according to the Trustwave experts. Up until two years ago, researchers could tell if data was being stolen by hackers because the information being transited out of the system was in plain text. But sometime last year, some attackers have begun using encryption as well, preventing investigators from identifying the data.

Time stamping backwards – A quick way of identifying a malicious code was to find out the latest files downloaded to a machine. However, recently cyber criminals have been using executable malware that have the ability to alter their time stamp. "This means, hackers can load a malware today, which to an investigator would appear to have been installed with the operating system when the machine was bought a year ago," said Percoco.

Seeking a new port of exit – Because IT security administrators are likely to block or schedule access to certain ports known to be use by attackers to transit data out of the system, cyber criminals are using ports commonly employed by users when conducting Web searches.

"Ports 80 and 443, which is frequently used for Web searches and queries are almost always open so they are the best ports to exfiltrate stolen data," said Percoco.

Automated exfiltration - At some time many computers are likely to go into an auto update mode where updates to its software are loaded onto the machine at a time when IT administrators believe the computer is not in heavy use.

Ilyas said, cyber criminals have adopted this technique when transporting stolen data out of their victim's network. "Attackers no longer go back steal more data. They just program the target machine to automatically send out data at predetermined intervals or even randomly."

If you want to learn more about the current cyber threats and how to protect your business against them check the SecTor security conference set for Oct 18 and 19 at the Metro Toronto Convention Centre.

During the session entitled Malware Freakshow, Percoco and Ilyas will demonstrate how four types of malware infiltrate and wreak havoc to a business's system.

The presentation includes a blow-by-blow demo of how a network sniffer targets a grocery, how a memory dumper steals data from business, how a DLL (dynamic link library) malware file the size of only 10 kilobytes damages an office network and how a variant of the Zeus Trojan grabs hold of an Android mobile device.

Nestor Arellano is a Senior Writer at ITBusiness.ca. Follow him on Twitter, read his blog, and join the IT Business Facebook Page.

Print

Close Window