Trusteer
an IBM Company

5 DANGERS MOST DANGEROUS MALWARE TRENDS OF 2014

1 SOURCE CODE LEAKS WILL ACCELERATE MALWARE RELEASE CYCLES

The release of the Carberp source code in June 2013 provides cybercriminals with yet another set of building blocks to create new malware variants. We saw the same development after the release of the Zeus 2.0.8.9 source code in May 2011 leading to Ice IX and Citadel malware.

WHY IT'S DANGEROUS

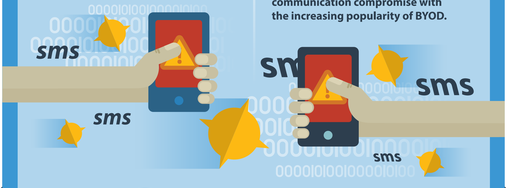
New malware variants contain new characteristics, signatures, evasive capabilities, and other modules never seen before. This makes it next to impossible for standard anti virus/anti-malware platforms to identify the malware.

2 MOBILE SMS-FORWARDING MALWARE WILL BECOME UBIQUITOUS

The capability to forward mobile SMS messages will be a standard feature in virtually all major malware families, with stand-alone SMS forwarding malware readily available.

WHY IT'S DANGEROUS

Mobile SMS verification is rendered all but useless as an out-of-band authentication method. Furthermore, enterprises must be wary of the real potential for SMS communication compromise with the increasing popularity of BYOD.

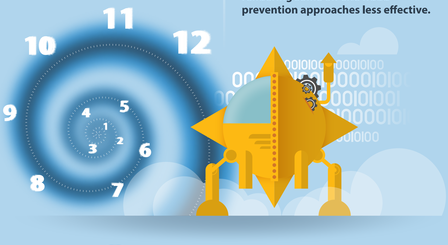


3 OLD SCHOOL MALWARE TECHNIQUES WILL MAKE A COMEBACK

As security products become available to detect new cybercrime techniques, malware authors revert back to more manual and time consuming approaches that can bypass many of these advanced detection and mitigation solutions.

WHY IT'S DANGEROUS

Anomaly detection and device ID solutions can now be easily circumvented by very basic cybercrime techniques. For example, we found several malware variants that prevent the user from interacting with the genuine site, thereby rendering some on-site fraud prevention approaches less effective.



4 ACCOUNT TAKEOVER WILL MOVE TO THE VICTIM'S DEVICE

Instead of the fraudster using his own machine to perpetrate account takeover attacks, he accesses the account via the victim's machine using various remote access technologies. This approach bypasses many device-fingerprinting technologies because the fraudster uses the (genuine) victim's device.

WHY IT'S DANGEROUS

Device fingerprinting is used to ascertain whether the account access is taking place from the client's known device or a different device. When access comes from the client's device, it appears to device-fingerprinting solutions that the legitimate customer is accessing his account.

5 MALWARE RESEARCHER EVASION WILL BECOME MORE POPULAR

Modern malware use a variety of techniques to avoid endpoint and network-based security software detection platforms. Now, however, we're increasingly seeing malware that use a variety of techniques (including advanced encryption, and virtual machine and debug software evasion) to avoid analysis by malware researchers. Researcher evasion will become a standard component of most malware offerings.

WHY IT'S DANGEROUS

Security solutions are updated with counter measures based on malware research. If malware cannot be researched, counter measures cannot be developed. Taking the fight to an even earlier stage – malware authors are heavily investing in making sure researchers cannot scrutinize their software.