Security Spotlight
December 9, 2010

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

TREND MICRO THREAT PREDICTIONS FOR 2011

With the growing diversity of operating systems among companies, as well as the growing use of mobile devices, cybercriminals should have a very profitable 2011. Their tactic will be to put a new spin on social engineering by way of "malware campaigns," by bombarding recipients with email that drop downloaders containing malware. All this will largely be made possible because of the Internet. Already, Trend Micro threat researchers have found that more than 80 percent of the top malware use the Web to arrive on users' systems and every second, 3.5 new threats are released by cybercriminals.

Below we outline Trend Micro's primary threat predictions as we head toward the end of 2010 and 2011 unfolds.

Security demands on cloud service providers will increase.

- Proof of concept attacks against cloud infrastructure and virtualized systems will emerge in 2011. Diversity of operating systems at the endpoints forces the bad guys to focus more on critical cloud services and server infrastructures.

More targeted attacks and cyber espionage.

- Mid-sized companies will be targeted in cyber-espionage. The growth of targeted and localized attacks will continue both against big name brands and/or critical infrastructure.

Further consolidation in the cybercrime underground.

- Groups will merge and/or join forces—e.g., ZeuS/SpyEye—as global, public attention for cyber attacks grows.

Clever malware campaigning.

- It's all about social engineering. Less infiltrated websites, more cleverly crafted and localized HTML emails with URLs pointing to the infection source. Malware campaigning will ensure fast and reliable spreading of the downloader, the downloader then downloads randomly generated binaries to avoid detection.

Evolution of malware attacks.

- Increasing use of stolen or legitimate digital certificates in malware attacks to avoid detection. Huge growth in use of complex domain generation algorithms (as used by Conficker and LICAT) in advanced persistent threats and increase in Java-based attacks.

Evolving use of vulnerabilities and exploits.

- Growth in exploits for alternative operating systems, programs, and Web browsers, combined with tremendous growth in the use of application vulnerabilities (*Flash,* etc.).

> Already, Trend Micro threat researchers have found that more than 80 percent of the top malware use the Web to arrive on users' systems and every second, 3.5 new threats are released by cybercriminals.

TREND MICRO™

Security Spotlight
December 9, 2010

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Security vendors brands are targeted.

- Security vendors' brands will increasingly be targeted by criminals looking to cause confusion and insecurity among users.

More mobile device attacks.

- More proof of concept, and some successful attacks on mobile devices, but not yet mainstream.

Old malware (re)infections.

- Some security vendors will run into trouble with local signatures, not being able to store all the threat information. They will retire old signatures which will lead to infections with old/outdated malware.

Vulnerable legacy systems.

- Targeted attacks on "unpatchable" (but widely used) legacy systems—*Windows 2000/Windows XP SP2,* embedded systems like telecom switchboards, etc.