Bitdefender®

H2 2012 E-Threat Landscape Report

Executive Summary

Second Half's Spotlights

- The discovery of the Flamer cyber-espionage tool in June 2012 has set new a new record in the complexity of malware used in state-sponsored attacks. Its discovery continued with other major security incidents throughout 2012 that affected regular PCs, OSX users and the Android operating system alike.

- For the first half of the year, zero-day vulnerabilities have played an essential role in the dissemination of malware with exploit packs as one of the favorite vectors of infection. The dangerous zero-day exploit in the Java Runtime Environment (CVE-2012-4681) has been documented and proof of concept was added to Metasploit, becoming public knowledge before a fix was made available.

- As a direct result, three billion devices running Java were vulnerable to remote code exploitation for roughly 48 hours. A secondary attack struck in September with the same cyber-criminal as the Java zero-day in control of dissemination. The exploit was aimed at Internet Explorer 9 and would allow remote compromise of the system those results in the installation of the Poison Ivy backdoor. Both zero-day exploits were used in advanced persistent attacks .

- 2012 saw some fluctuations in the amount of junk e-mails within the entire e-mail traffic. The year began with a slight decrease in the total of spam e-mails, but steadily going up towards the middle of the year. According to data gathered from the Bitdefender Antispam lab, the second half of the year saw a growth again with small variations towards the end of 2012. The increase in the number of junk e-mails was nonetheless minor, by only 5% leading to a rough value of 73% from the total amount of e-mails sent worldwide.

- Once again, **Trojan.AutorunInf** scores the top position in the global e-threat landscape with 4.2% of the total amount of infections. Although it is still first, its impact has significantly dropped to more than five percent as compared to the previous period of time. However, its downfall is compensated by the rise of aggressive adware.

E-Threat Predictions for 2013

The e-threat landscape is continuously shifting to take advantage of new opportunities opened by emerging technologies as well as to meet the increasingly complex demands of cyber-criminals. Apart from the threat trends that we have been observing for the past four years, 2013 will likely bring new dangers to the cyber-world as we know it.

Malware shifting to the legitimate software business model

Some of the modern groups of cyber-criminals are structured in a similar manner with legitimate software vendors. After successfully introducing R&D, testing, marketing and even tech support, cyber-criminals are now taking the game to a whole new level, by internationalization. Modern malware comes translated in multiple languages to cover larger geographic areas and to make the message easier to comprehend to the user. At the moment, there are some species of ransomware that use this technique and we expect to see this become a de-facto standard over the next year.

Attacks against the hypervisor

As virtualization becomes the next big thing for millions of customers worldwide, and businesses and services are moving to cloud-based virtual environments, cyber-criminals will try to find new ways to subvert the entire server and the virtual machines running on top of its hypervisor.

New mobile OS, new troubles

Android malware will continue its exponential boom throughout 2013. The next year will also bring the Firefox OS, a brand-new operating system built on open web-standards. According to estimations, Firefox OS will have a market share of about 2% by the end of the year – a user base that will be exposed to whatever design flaws the new OS might have.

Old threats going down, new threats surface

As Windows 7 has finally overtaken long-runner Windows XP in market share, the e-threat landscape will witness significant changes. Most likely, Autorun-based threats will go extinct in the last quarter of 2013, along with the notorious Downadup / Conficker worm. Their places will be claimed by generic – yet intrusive - adware and by rootkit-based infection mules such as the ZeroAccess.

Infected PCs, electronic currency miners

As Bitcoins are becoming increasingly important in the global economic ecosystem, cyber-criminals will likely envision novel approaches to Bitcoin mining on compromised computers.

Windows 8 and UEFI

The release of Windows 8 will likely translate in significant adoption of the UEFI technology, a BIOS replacement that has been around for years, but that failed to get traction until now. As more and more PCs and laptops are built on UEFI-based motherboards, cyber criminals will likely shift their attention to a much more permissive environment than the obsolete BIOS.

Windows 8 will also be a target in itself. Throughout 2013, Windows 8 is expected to overtake Windows Vista in terms of market share and cyber-criminals will likely go hunting for platform-specific vulnerabilities, be they at the kernel level or at the web-browser's surface. However, these specific vulnerabilities will not get used in the wild until the newest OS from Microsoft gains real traction.