Microsoft | Security Intelligence Report

The evolution of malware and the threat landscape – a 10-year review

KEY FINDINGS

Microsoft Security Intelligence Report: Special Edition

February, 2012

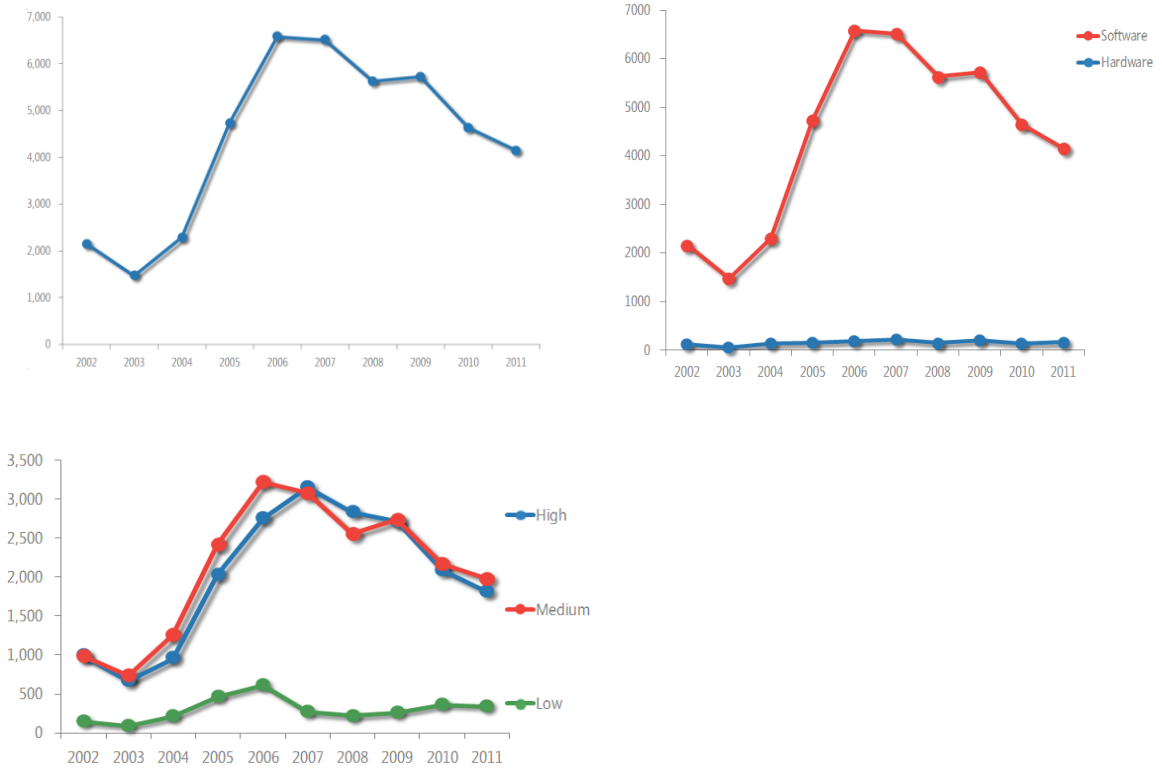
MICROSOFT SECURITY INTELLIGENCE REPORT: SPECIAL EDITION

Vulnerabilities

Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of that software or the data it processes. Some of the worst vulnerabilities allow attackers to exploit a compromised computer, causing it to run arbitrary code without the user's knowledge.

The past 10 years represent a very interesting timeframe for reviewing vulnerability disclosures and ensuing changes that continue to affect risk management in IT organizations around the world.

Figure 1. Industry-wide vulnerability disclosures since 2002 including hardware, software, and severity trends



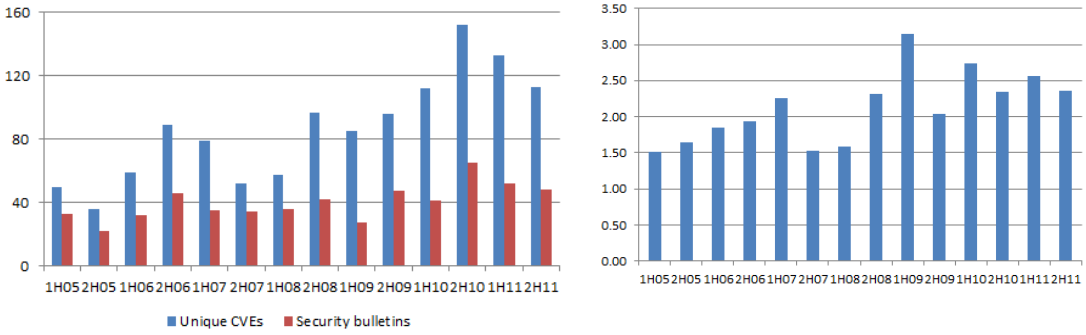
Vulnerability disclosure trends:

- Vulnerability disclosures across the industry in 2011 were down 11.8 percent from 2010.
- The overall vulnerability severity trend has been a positive one. Medium and High severity vulnerabilities have steadily decreased since their high points in 2006 and 2007.

Exploit trends and security bulletins

The Microsoft Security Response Center (MSRC) identifies, monitors, resolves, and responds to Microsoft software security vulnerabilities. The MSRC releases security bulletins each month to address vulnerabilities in Microsoft software. Security bulletins are numbered serially within each calendar year. For example, "MS11-057" refers to the 57th security bulletin released in 2011.

Figure 2. Number of MSRC security bulletins and CVE-identified vulnerabilities addressed, and average number of CVEs addressed per security bulletin



- In 2011 the MSRC released 100 security bulletins that addressed 236 individual CVE–identified vulnerabilities, decreases of 7% and 6%, respectively, from 2010. As the chart on the right shows, the average number of CVEs addressed by each security bulletin has increased over time, from 1.5 in 1H05 to 2.4 in 2H11.

Malware and potentially unwanted software trends

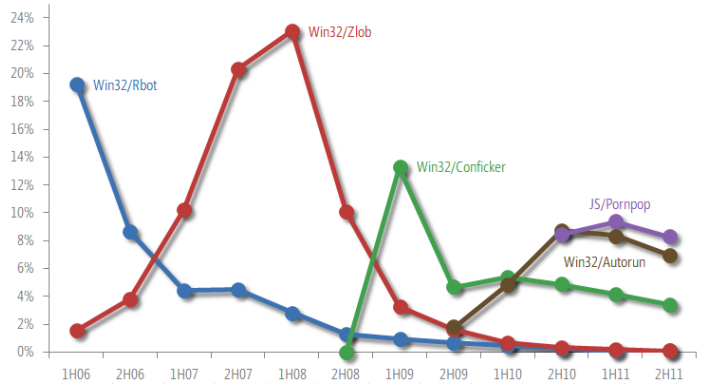
Malware continues to evolve, and the fluctuations in detections of different forms of malware sometimes indicate the successes at given points in time of the software industry's persistent antimalware efforts versus the efforts of malware developers.

How threats have evolved over time

When viewed from a multi-year perspective, some malware and potentially unwanted software families tend to peak, or become quite prevalent, for short periods of time as antimalware vendors focus their efforts on detecting and removing these threats. These peak periods are followed by periods of decline as attackers change their tactics and move on. The following figure illustrates this phenomenon. (The vertical axis in all of the remaining charts represents the percentage of all

computers that were infected with malware.)

Figure 3. Malware and potentially unwanted software families that have peaked and declined since 2006



Win32/Rbot was an early botnet family that gained notoriety in 2004 and 2005 after a number of high profile outbreak incidents that affected media and government networks, among others. Rbot is a "kit" family

Win32/Conficker is a worm family discovered in November 2008 that initially spread by exploiting a vulnerability addressed by security update MS08-067,

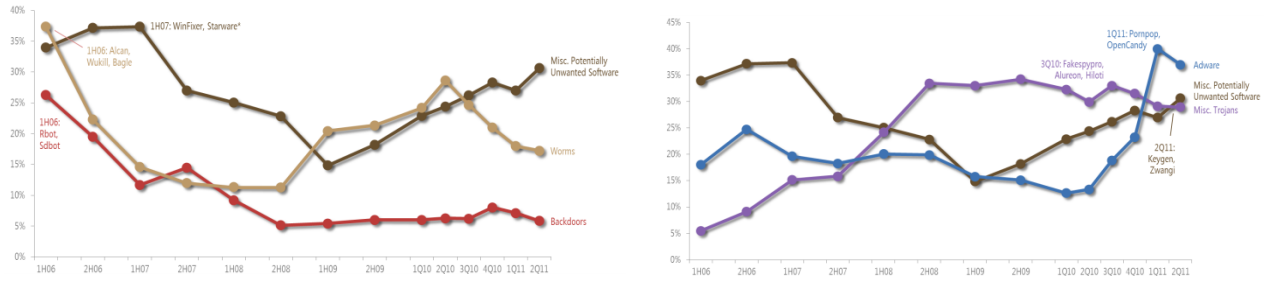
JS/Pornpop is adware that consists of specially crafted JavaScript-enabled objects that attempt to display pop-under advertisements. First detected in August 2010, it was the second most commonly detected family in 2H10 and 1H11, and is likely to be the most commonly detected family in 2H11.

Win32/Autorun is a generic detection for worms that attempt to spread between mounted computer volumes by misusing the AutoRun feature in Windows. Detections of Win32/Autorun increased gradually for several periods before peaking in 2H10 as the most commonly detected family during that period.

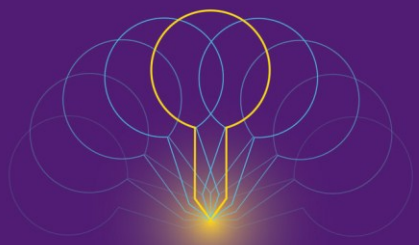
Different threats at different times

The following figure illustrates the relative prevalence of six different categories of malware found on computers since 2006.

Figure 4. Worms, Backdoors, and Miscellaneous Potentially Unwanted Software categories since 2006 (left) and Adware, Miscellaneous Potentially Unwanted Software, and Miscellaneous Trojans categories since 2006 (right)



- Most of the prevalent worms in 2006 were mass-mailers, such as Win32/Wukill and Win32/Bagle, which spread by emailing copies of themselves to addresses discovered on infected computers.
- Prevalent backdoors included a pair of related botnet families, Win32/Rbot and Win32/Sdbot. Variants in these families are built from botnet construction kits that are traded in the underground market for malware, and are used to control infected computers over Internet Relay Chat (IRC).
- Prevalent trojan families in 2006 and 2007 included Win32/WinFixer, an early rogue security software family, and the browser toolbar Win32/Starware.
- The Adware, Miscellaneous Potentially Unwanted Software, and Miscellaneous Trojans categories were the most commonly detected categories in 2010 and 2011. Adware detections increased significantly in 1H11, including the adware families Win32/OpenCandy and JS/Pornpop.
- Significant families in this category in 2Q11 were Win32/Keygen, a generic detection for tools that generate product keys for illegally obtained versions of various software products, and Win32/Zwangi, a program that runs as a service in the background and modifies web browser settings to visit a specific website.
- A number of rogue security software families fall into this category, such as Win32/FakeSpyPro, the most commonly detected rogue security software family in 2010. Other prevalent families in this category include Win32/Alureon, the data-stealing trojan, and Win32/Hiloti, which interferes with an affected user's browsing habits and downloads and executes arbitrary files.


TwC Next