Microsoft Security Intelligence Report

Volume 10

An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in 2010, with new data covering July through December

KEY FINDINGS

Microsoft

Microsoft Security Intelligence Report

Table of Contents

Key Findings Summary

Volume 10 of the *Microsoft® Security Intelligence Report* (*SIRv10*) provides in-depth perspectives on software vulnerabilities, software vulnerability exploits, malicious and potentially unwanted software, and security breaches in both Microsoft and third party software. Microsoft developed these perspectives based on detailed trend analysis over the past several years, with a focus on 2010.

This document summarizes the key findings of the report. The full *SIRv10* also includes deep analysis of trends found in 117 countries/regions around the world and offers ways to manage risks to your organization, software, and people.

The full *SIRv10*, as well as previous volumes of the report and related videos, can be downloaded from www.microsoft.com/sir.

Vulnerability Disclosures

- Vulnerabilities in applications versus operating systems or web browsers continued to account for a large majority of all vulnerabilities in 2010, although the total number of application vulnerabilities declined 22.2 percent from 2009.

- Industry vulnerability disclosure trends continue an overall trend of moderate declines since 2006. This trend is likely because of better development practices and quality control throughout the industry, which result in more secure software and fewer vulnerabilities.

- Vulnerability disclosures for Microsoft products increased slightly in 2010 but have generally remained stable over the past several periods.

Exploits

- The exploitation of Java vulnerabilities sharply increased in the second quarter of 2010 and surpassed every other exploitation category that the

MMPC tracks, including generic HTML/scripting exploits, operating system exploits, and document exploits.

- Exploits that use HTML and JavaScript steadily increased throughout the year and continue to represent a large portion of exploits. The most prevalent type of attack in this category involved malicious IFrames.
- The number of Adobe Acrobat and Adobe Reader exploits dropped by more than half after the first quarter, and remained near this reduced level throughout the remainder of the year.

Document Exploits

- Exploits that affected Adobe Acrobat and Adobe Reader accounted for most document format exploits detected throughout 2010. Almost all of these exploits involved the generic exploit family Win32/Pdfjsc.

- The number of Adobe Acrobat and Adobe Reader exploits dropped by more than half after the first quarter and remained near this reduced level throughout the remainder of the year.

- Microsoft Office file format exploits accounted for between 0.5 and 2.8 percent of the document format exploits that were detected each quarter in 2010.

Malware and Potentially Unwanted Software

- Except where specified, the information in this section was compiled from telemetry data that was generated from more than 600 million computers worldwide and some of the busiest online servuces on the Internet.

Operating System Infection Rates

- As in previous periods, infection rates for more recently released Microsoft operating systems and service packs are consistently lower than older ones, for both client and server platforms. Windows 7 and Windows Server 2008 R2, the most recently released Windows client and server versions, respectively, have the lowest infection rates.

- Infection rates for the 64-bit versions of Windows Vista® and Windows 7 are lower than for the corresponding 32-bit versions of those operating

systems. One reason may be that 64-bit versions of Windows still appeal to a more technically savvy audience than their 32-bit counterparts, despite increasing sales of 64-bit Windows versions among the general computing population. Kernel Patch Protection (KPP), a feature of 64-bit versions of Windows that protects the kernel from unauthorized modification, may also contribute to the difference by preventing certain types of malware from operating.

Threat Families

- JS/Pornpop, the most commonly detected family in 4Q10, is a detection for specially crafted JavaScript-enabled objects that attempt to display pop-under advertisements in users' web browsers, usually with adult content.

- Detections and removals of Win32/Autorun, a generic detection for worms that spread between mounted volumes using the Autorun feature of Windows, increased significantly in 4Q10, although Autorun dropped to second place because of the spread of Pornpop.

- Win32/Taterf, the most prevalent threat in 2Q10, dropped to third by 4Q10. Taterf belongs to a category of threats that are designed to steal passwords for popular online computer games and transmit them to the attackers. See "Online Gaming-Related Families" on page 62 of *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)* for more information about these threats.

Home and Enterprise Threats

- Seven malware families are common to home and enterprise network environments, although they are ordered differently and in different proportions. The worm family Win32/Conficker, which uses several methods of propagation that work more effectively within a typical enterprise network environment than they do over the public Internet, leads the domain-joined list by a significant margin, but ranks ninth on the non-domain list.

- On non-domain computers, JS/Pornpop was the most commonly detected family in 4Q10 and the fourth most commonly detected family

in 2010 overall. By contrast, this family was detected much less often on domain-joined computers. Pornpop is often found on websites that host illegal or illicit content, which users in domain environments are often restricted from accessing by organizational policy or blocking software.

Email Threats

- After increasing gradually and then reaching a plateau through the first eight months of 2010, the number of spam messages received and blocked by Microsoft Forefront® Online Protection for Exchange (FOPE) dropped abruptly in September, and again in December. These drops can be correlated with events involving two of the world's most significant spam-sending botnets:
    - During the last week of August 2010, researchers affiliated with the security firm LastLine spearheaded a coordinated takedown of command-and-control (C&C) servers associated with the Win32/Cutwail spambot. In the days following the takedown, FOPE recorded a significant drop in the average daily volume of messages blocked.
    - On or about December 25, 2010, spam researchers around the world recorded an almost complete cessation of spam originating from the large Rustock botnet, with some spam trackers reporting a drop in the global spam rate as high as 50 percent or more. During the final week of December, the number of messages blocked by FOPE was almost 30 percent less than in the prior week, compared to a drop of less than two percent between the final two weeks of 2009. The Rustock botnet subsequently began sending spam again in mid-January, and the number of messages blocked by FOPE has risen accordingly. The reasons for this hiatus are still being investigated.

Spam Types

- Advertisements for nonsexual pharmaceutical products accounted for 32.4 percent of the spam messages blocked by FOPE content filters in 2010.

- Together with nonpharmaceutical product ads (18.3 percent of the total) and advertisements for sexual performance products (3.3 percent), product advertisements accounted for 54.0 percent of spam in 2010, which is down from 69.2 percent a year ago.

Malicious Websites

- In the first half of 2010, phishers showed signs of targeting online gaming sites with increasing frequency, although this push appeared to have dwindled as social networks came under increased attack. Impressions that targeted gaming sites reached a high of 16.7 percent of all impressions in June before dropping to a more typical 2.1 percent in December.

- Phishing sites that target social networks routinely receive the highest number of impressions per active phishing site. The percentage of active phishing sites that targeted social networks increased during the final months of the year, but still only accounted for 4.2 percent of active sites in December, despite receiving 84.5 percent of impressions that month. Nevertheless, the number of active sites targeting gaming sites remained relatively high during the second half of the year, which suggests that more campaigns may be coming.

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security