Microsoft Security Intelligence Report

January through June 2008

Key Findings Summary

Microsoft

Table of Contents

Microsoft Security Intelligence Report (January through June 2008)

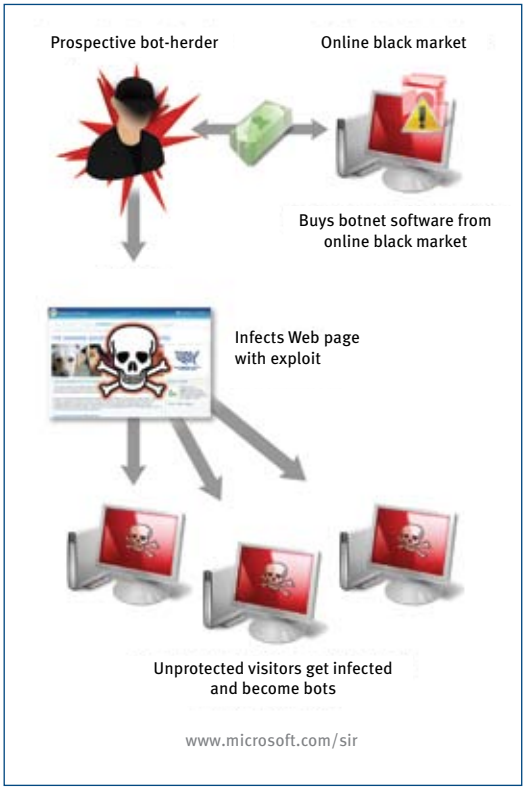
Key Findings Summary

The Microsoft® Security Intelligence Report (January through June 2008) provides an in-depth perspective on software vulnerabilities (both in Microsoft software and in third-party software), software exploits, and malicious and potentially unwanted software observed by Microsoft during the past several years, with a focus on the first half of 2008 (1H08)[1]. The Report also contains new information on browser-based exploits and updated information on security and privacy breaches.

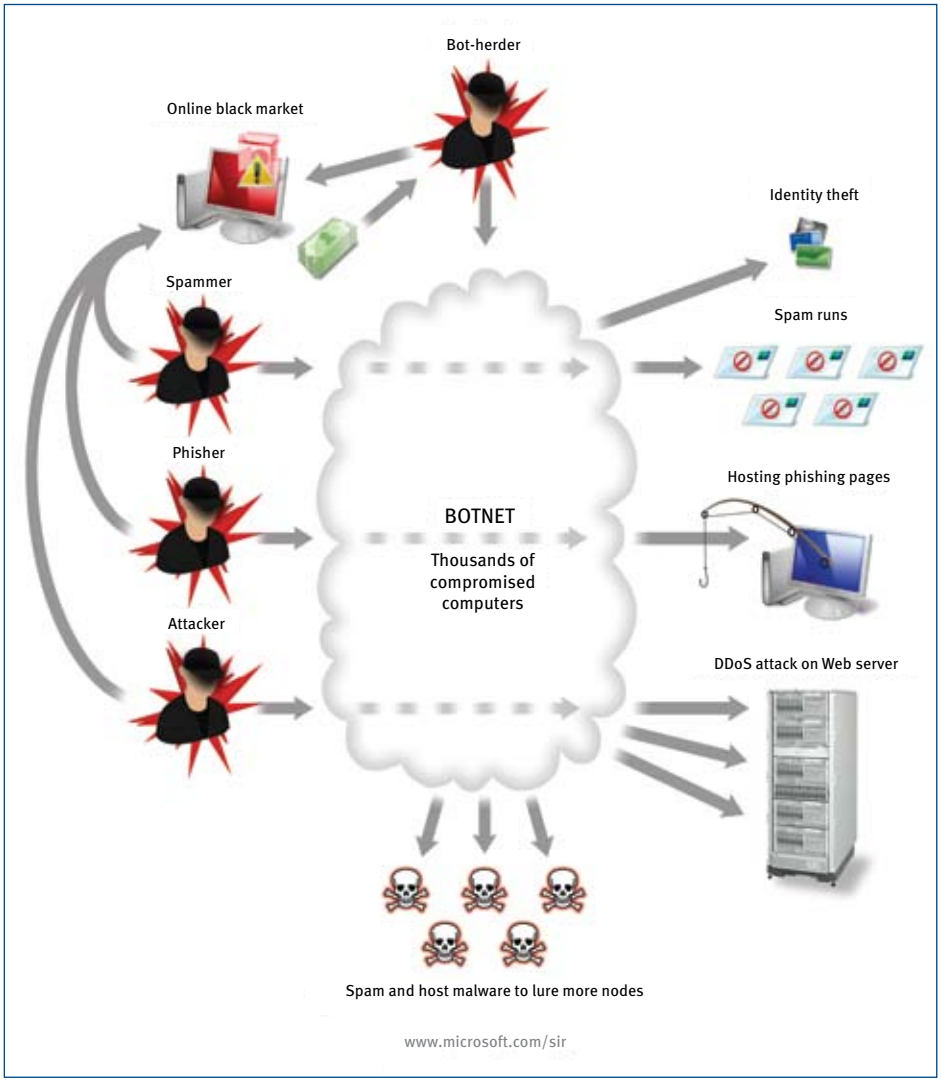
This document is a summary of the key findings of the report. The full Security Intelligence Report also offers strategies, mitigations, and countermeasures, and it can be downloaded from http://www.microsoft.com/sir.

The Threat Ecosystem

The latest Security Intelligence Report includes a detailed examination of the threat ecosystem and the evolution of threats and countermeasures. With a focus on "botnets" the report describes the various parties involved in creating and distributing malware and potentially unwanted software, explaining key techniques and technologies used to attack and compromise users, and giving insight into the underground economy behind many of these attacks, the Report aims to give the reader a unique perspective on the threat ecosystem in action. Please download the full Report to get the story behind this illustration and the one on the following page.



[1] The nomenclature used throughout the report to refer to different reporting periods is nHYY, where nH refers to either the first (1) or second (2) half of the year, and YY denotes the year. For example, 1H08 represents the period covering the first half of 2008 (January 1 through June 30), while 2H07 represents the period covering the second half of 2007 (July 1 through December 31).



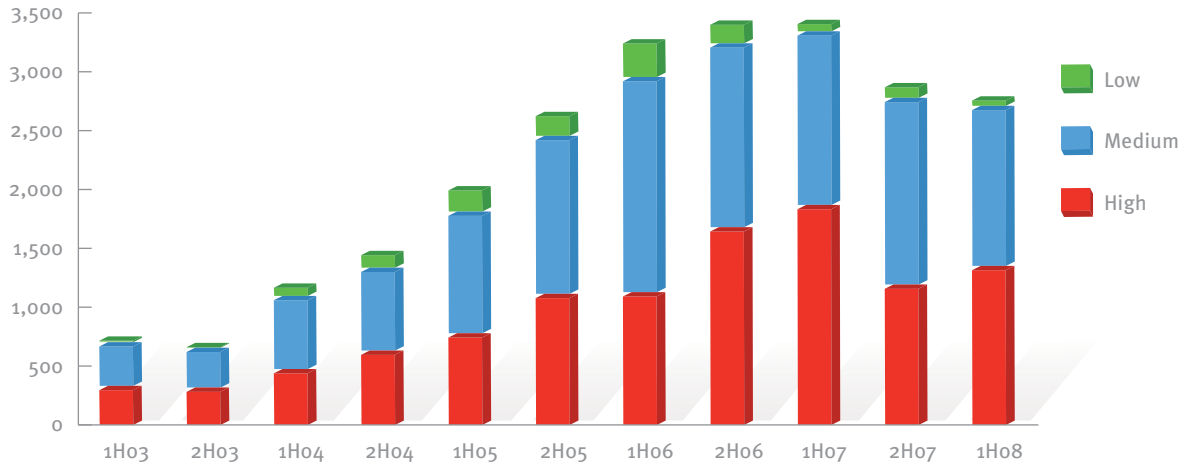
Industry Vulnerability Disclosures

Vulnerabilities are defined as weaknesses in software that allow an attacker to compromise the integrity, availability, or confidentiality of that software. Some of the worst vulnerabilities allow attackers to run arbitrary code on compromised systems. Vulnerability data in this section was gathered from third-party sources, including the National Institute of Standards (NIST), published reports, and Microsoft's own data.

- The total number of unique vulnerability disclosures across the industry again decreased in 1H08, down 4% from 2H07 and down 19% from 1H07.

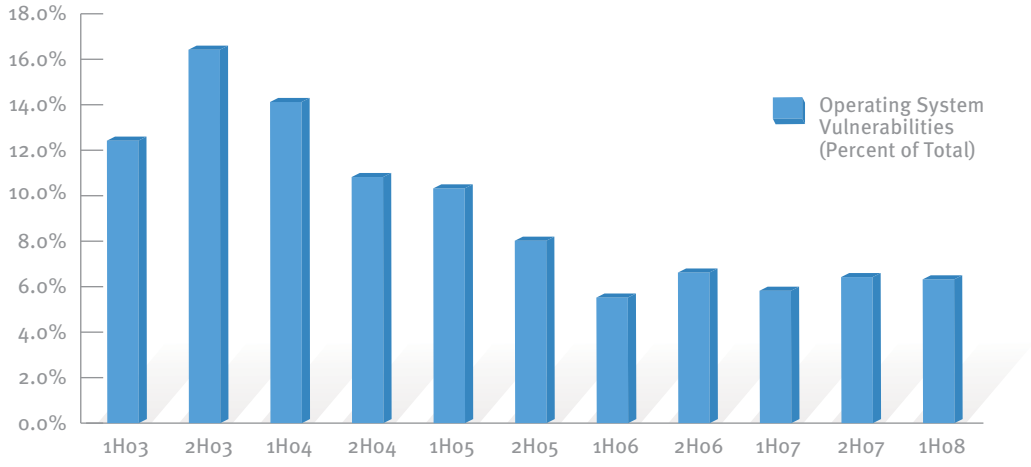
- In contrast to the decrease in total disclosures across the entire industry, vulnerabilities rated as High severity by the Common Vulnerability Scoring System (CVSS)[2] increased 13% over 2H07, with roughly 48% of all vulnerabilities receiving a rating of High severity. This is still a 28% decline from 1H07.

FIGURE 1. Industry-wide vulnerability disclosures by CVSSv2 severity, by half-year, 1H03–1H08



- Compounding the seriousness of the High severity vulnerabilities, across the entire industry the percentage of disclosed vulnerabilities that are easiest to exploit also increased, with 56% requiring a Low complexity exploit[3].
- The proportion of vulnerabilities disclosed in operating systems continues to decline; more than 90% of vulnerabilities disclosed in 1H08 affected applications.

FIGURE 2. Operating system vulnerabilities as a percentage of all disclosures, by half-year, 1H03–1H08

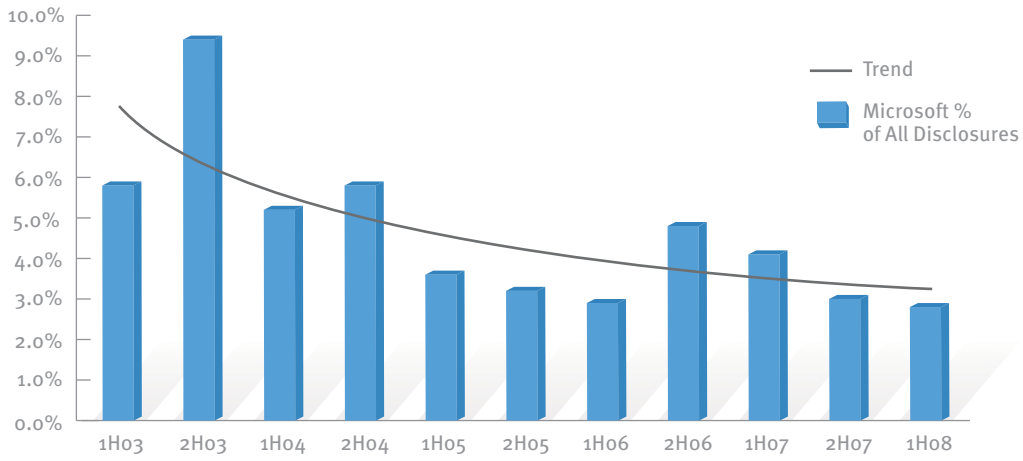


[2] CVSS is an industry standard for assessing the severity of software vulnerabilities. See http://www.first.org/cvss/ for more documentation and details.

[3] Definition from: Mell, Peter, Karen Scarfone, and Sasha Romanosky. "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," (http://www.first.org/cvss/cvss-guide.html) section 2.1.2.

- Vulnerability disclosures in Microsoft software in 1H08 continued a multi-period downward trend, both in terms of all disclosures and relative to total industry disclosures. The figure below shows the share of vulnerability disclosures attributed to Microsoft since 1H03, and illustrates the downwards trend.

FIGURE 3. Microsoft vulnerability disclosures as a percentage of all industry disclosures, by half-year, 1H03–1H08



Vulnerability Exploit Details

When vulnerabilities are disclosed in software, some security researchers or malware authors may develop and publish code that exploits those vulnerabilities. This publicly available exploit code may be intended for positive reasons (for example, for IT professionals to test against their systems) but its very existence makes it more likely that malware will be developed and released.

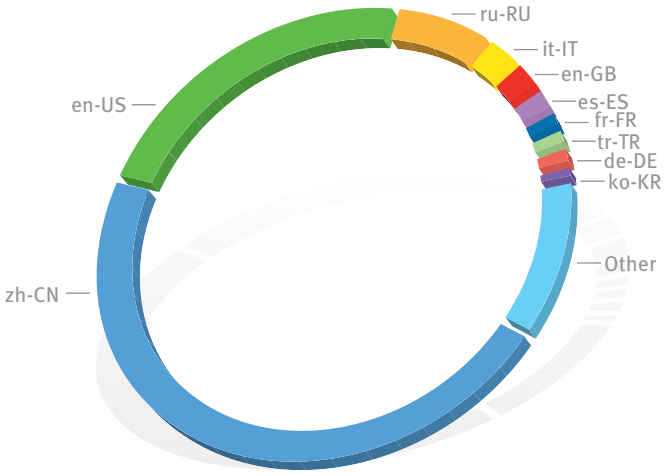
- In 1H08, 32% (or, 25 out of 77) of vulnerabilities disclosed in Microsoft software had publicly available exploit code, consistent with the trends observed in previous volumes of this report.
- In testing the reliability of the software vulnerability exploits released, only 10.4% of vulnerabilities had publicly available exploit code that could consistently exploit the vulnerability; the rest were either unreliable or ineffective.

Browser-Based Exploits

To assess the relative prevalence of browser-based exploits in 1H08, Microsoft analyzed a sample of data obtained from customer-reported incidents, submissions of malicious code, and Microsoft Windows® error reports. The data encompasses multiple operating systems and browser versions, from Windows XP to Windows Vista®. It also includes data from third-party browsers that host the Internet Explorer rendering engine, called Trident.[4]

- The most common system locale for victims of browser-based exploits was Chinese, accounting for 47% of all incidents, followed by US English with 23% of incidents.

FIGURE 4. Browser-based exploits encountered by system locale, 1H08



de-DE: German language, Germany
en-GB: English language, United Kingdom
en-US: English language, United States
es-ES: Spanish language, Spain
fr-FR: French language, France
it-IT: Italian language, Italy
ko-KR: Korean language, Korea
ru-RU: Russian language, Russia
tr-TR: Turkish language, Turkey
zh-CN: Chinese language, China

[4] See http://msdn.microsoft.com/en-us/library/aa939274.aspx for more information on Trident.

- For browser-based attacks on Windows XP–based machines, Microsoft vulnerabilities accounted for 42% of the total. On Windows Vista–based machines, however, the proportion of vulnerabilities attacked in Microsoft software was much smaller, accounting for just 6% of the total.

FIGURE 5. Browser-based exploits targeting Microsoft and third-party software on computers running Windows XP, 1H08

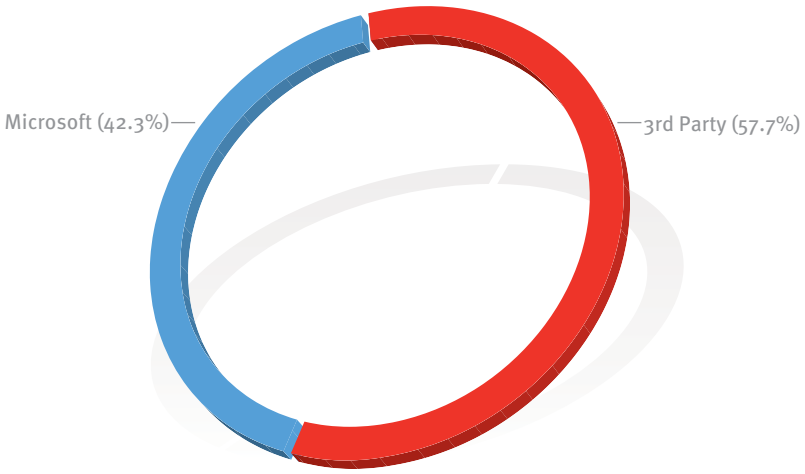
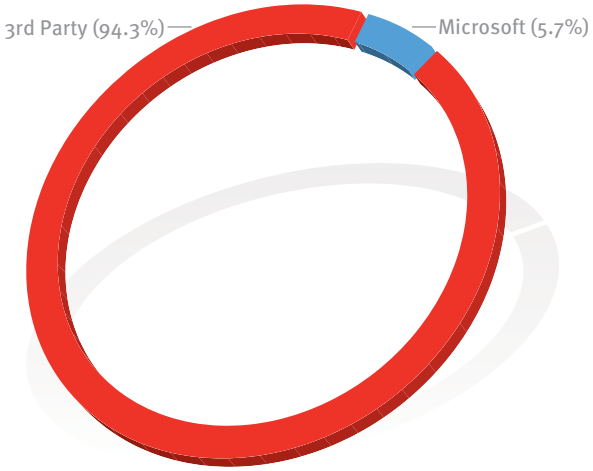


FIGURE 6. Browser-based exploits targeting Microsoft and third-party software on computers running Windows Vista, 1H08



- Microsoft software accounted for 5 of the top 10 browser-based vulnerabilities attacked on computers running Windows XP in 1H08, compared to zero on computers running Windows Vista. The figures below detail the top 10 browser-based vulnerabilities attacked on Windows XP-based machines and Windows Vista-based machines (on the next page). The vulnerabilities are referenced by the relevant CVSS bulletin number or by Microsoft Security Bulletin number as appropriate.

FIGURE 7. Top 10 browser-based vulnerabilities exploited on computers running Windows XP, 1H08

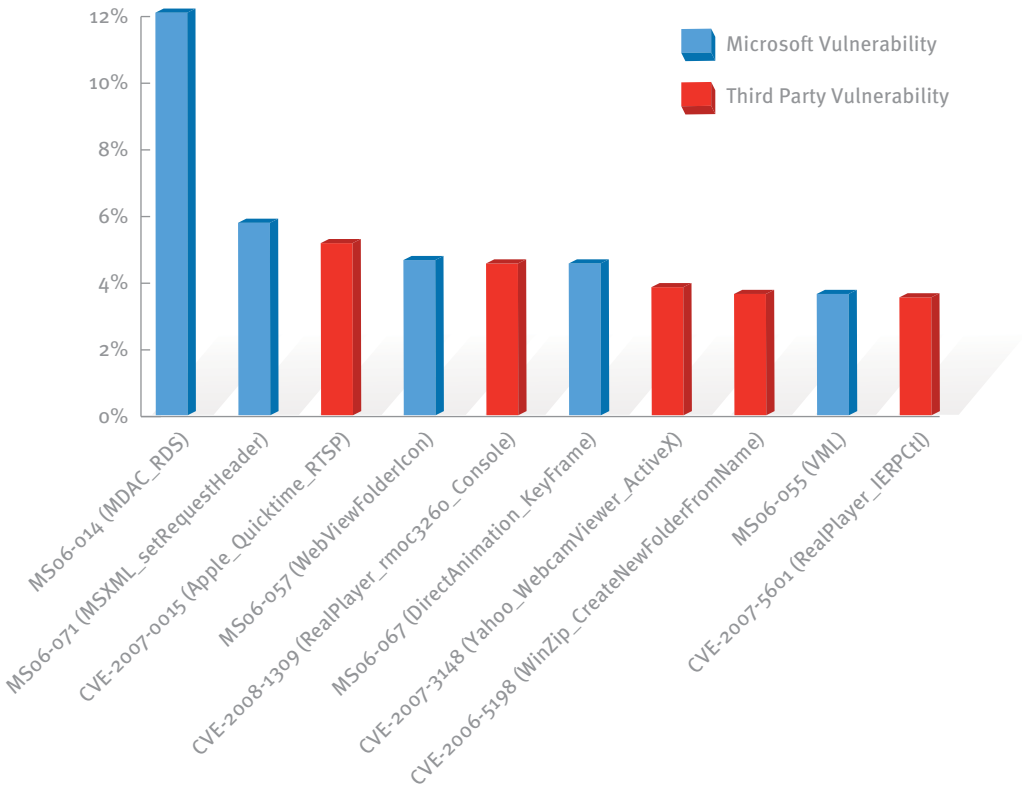
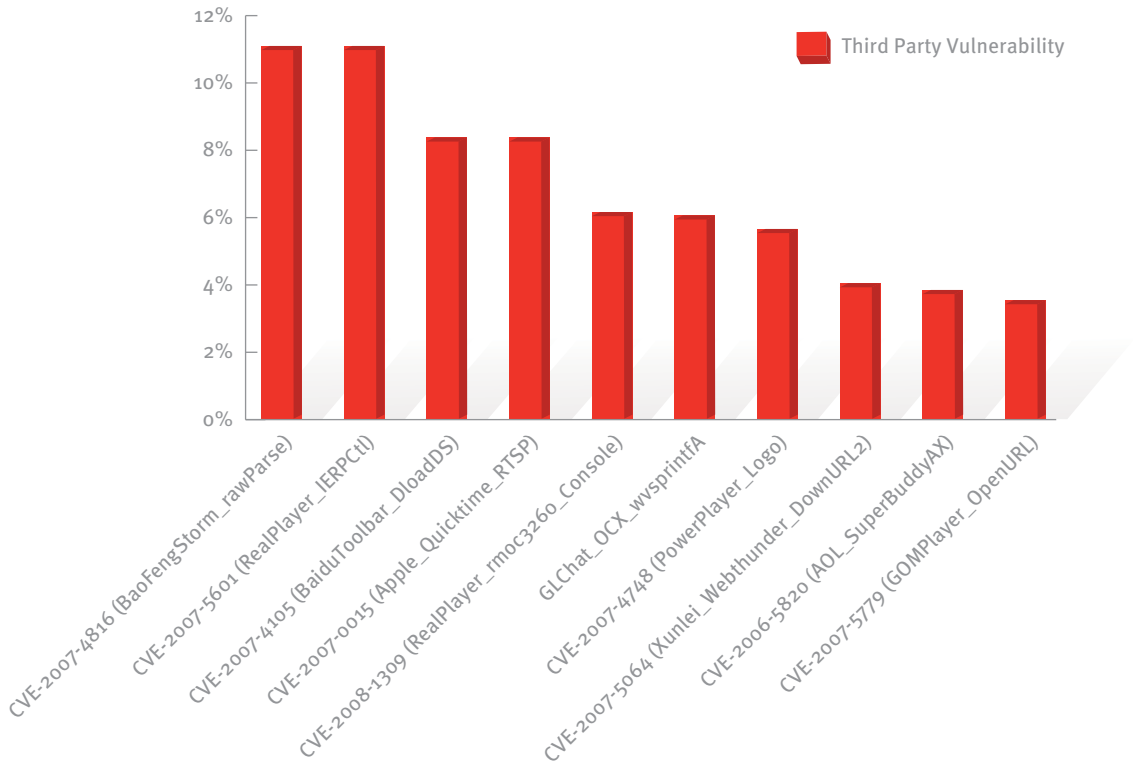


FIGURE 8. Top 10 browser-based vulnerabilities exploited on computers running Windows Vista, 1H08

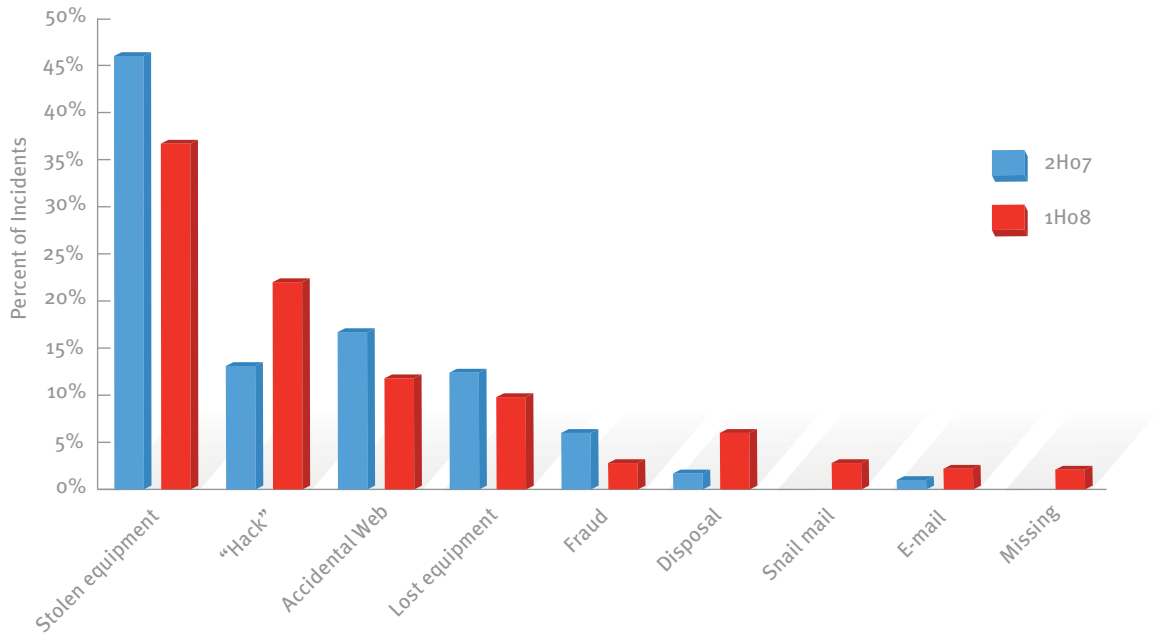


Security Breach Trends

This section of the report examines the details of security breach incidents from around the world via data provided by the Open Security Foundation's OSF Data Loss Database at http://datalossdb.org.

- The top reason reported for data loss through a security breach in 1H08 continued to be stolen equipment such as laptop computers (37.2% of all data-loss incidents reported).
- Although showing a slight increase over 2H07, less than 23% of reported security breaches in 1H08 resulted from incidents classified as "hack" attacks.

FIGURE 9. Security breach incidents by type, expressed as percentages of the total, 2H07 and 1H08



Malicious and Potentially Unwanted Software

Global Trends

Microsoft security products gather, with user consent, data from hundreds of millions of computer systems worldwide and from some of the Internet's busiest online services. The analysis of this data gives a comprehensive and unique perspective on malware and potentially unwanted software activity around the world.

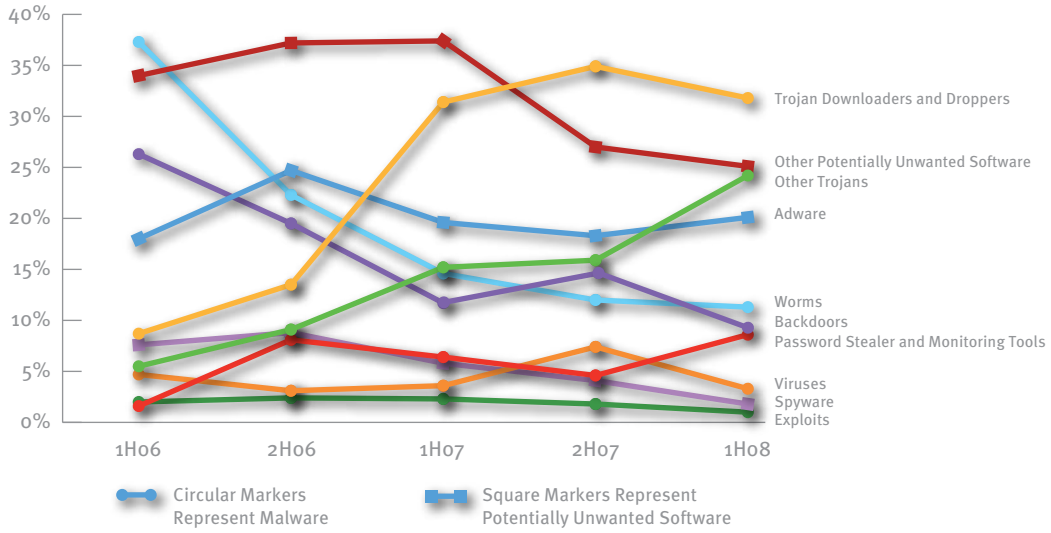
- In 1H08, the total amount of malware and potentially unwanted software removed from computers worldwide increased more than 43% compared to 2H07.
- Patterns of malware detected and removed by Microsoft security products varied across countries and regions; however, trojan downloaders and droppers constituted more than 30% of all malware removed by Microsoft security products worldwide.

[5] See previous volumes of the Microsoft Security Intelligence Report at http://www.microsoft.com/sir

This trend builds on the significant increases in the volume of trojan downloaders and droppers detected over the past several years.[5]

- As in 2H07, downloaders/droppers remained the most prevalent category of threat, due in large part to the fact that some of the families use a variety of social engineering techniques to spread. Two such families, Win32/Zlob[6] and Win32/Renos, were responsible for more than 96% of the computers cleaned in this category.

FIGURE 10. Computers cleaned by threat category, in percentages, 1H06–1H08

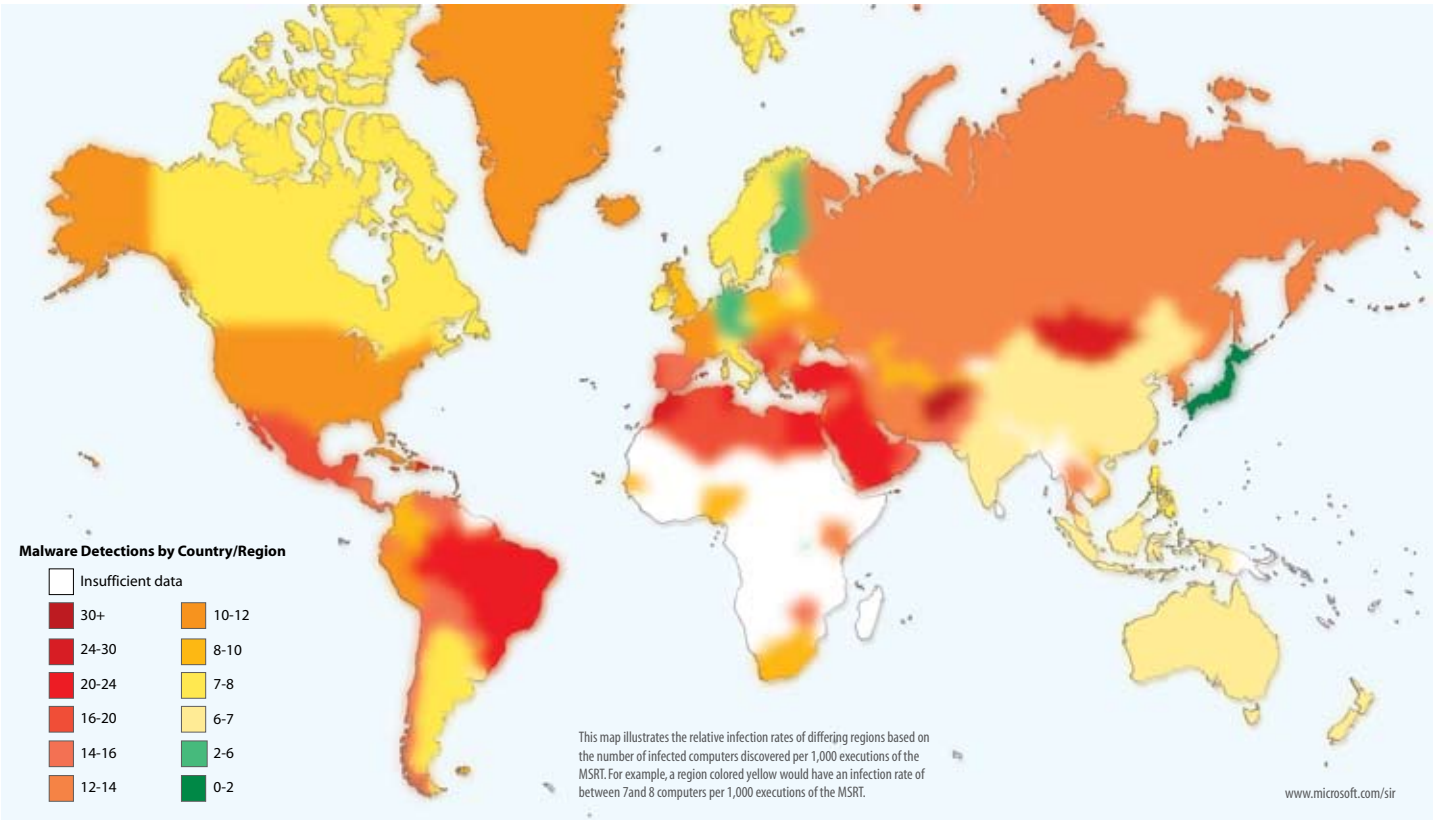


[6] See the Microsoft Malware Protection Center Encyclopedia at http://www.microsoft.com/av for additional information on this and other families listed in this section.

[7] Infection rates in this report are expressed using a metric called Computers Cleaned per Mil (CCM) that represents the number of computers cleaned per thousand executions of the MSRT.

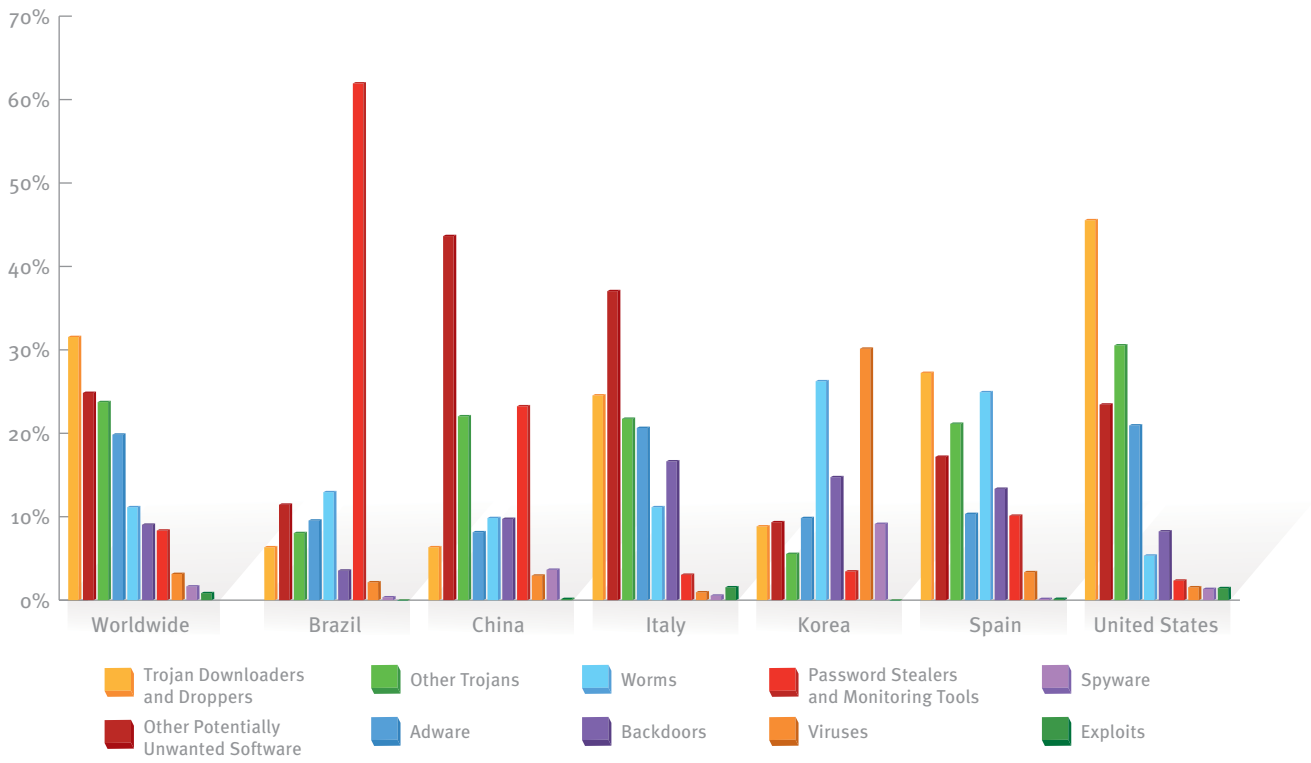
As a general rule, infection rates tend to be higher in developing countries/regions than in developed countries/regions, as reported by the Malicious Software Removal Tool (MSRT). The following map illustrates the infection rates of locations around the world, expressed in CCM[7].

FIGURE 11. Infection rates by country/region, 1H08



- Infection data gathered from some of the most populous regions around the world by several Microsoft security products demonstrates the highly localized nature of malware and potentially unwanted software. The following figure shows the relative prevalence of different categories of malware and potentially unwanted software in different regions in 1H08, expressed as a percentage of the total number of computers cleaned in each region.

FIGURE 12. Threat categories in six locations around the world, by incidence among all computers cleaned, 1H08



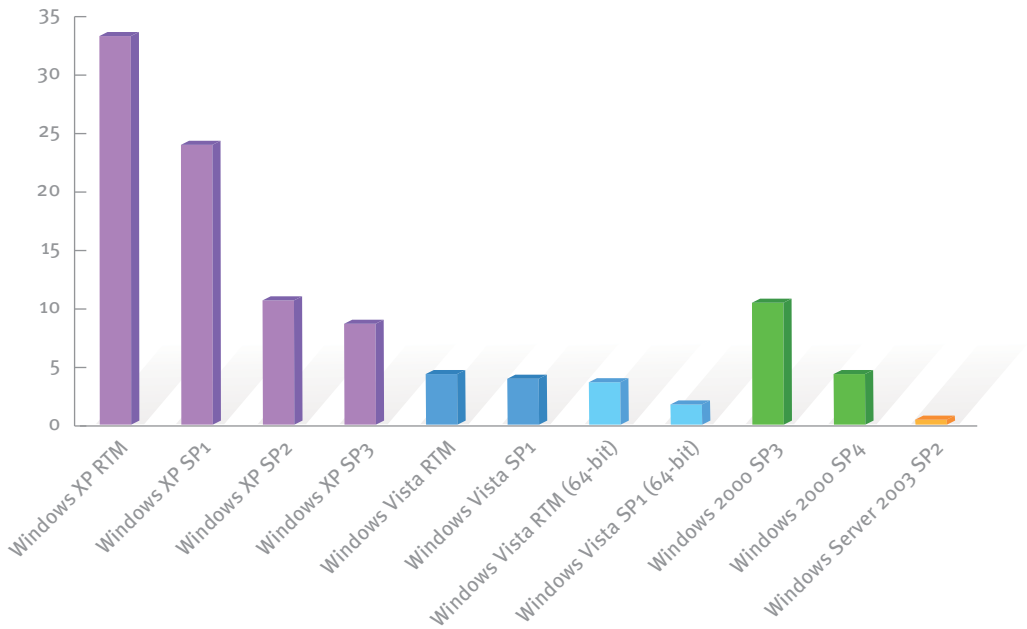
- In **Brazil**, password stealers, such as Win32/Bancos, dominate by an overwhelming margin, being detected on more than 60% of all Brazilian computers where malware or potentially unwanted software was detected in 1H08.
- **China** is dominated by potentially unwanted software that targets the Chinese-language market, notably pop-up advertisement toolbars, like Win32/Sogou, and browser modifiers, like Win32/BaiduSobar and Win32/CNNIC. Many of the most common families in China are Chinese-language threats that don't appear in the list of top threats for any other location.

- In **Italy**, potentially unwanted software is the largest category of threat, led by the peer-to-peer (P2P) client Win32/BearShare and the advertising toolbar Win32/Hotbar.
- In **Korea**, viruses are the largest category of threat, led by Win32/Virut and Win32/Parite. Viruses often spread through P2P networks and community sites where files are exchanged. Korea has one of the highest levels of broadband Internet access penetration per capita in the world, and this may contribute to the spread of infected files.
- In **Spain**, worms remain a prominent threat, led by Win32/Taterf.
- In the **United States**, trojan downloaders, like Win32/Zlob, account for the largest single category of threat.

Infection Rates by Operating System Version

- The following graph shows the CCM for each Microsoft Windows operating system/service pack combination in 1H08 worldwide.

FIGURE 13. CCM (number of computers cleaned for every 1,000 MSRT executions), by operating system, 1H08



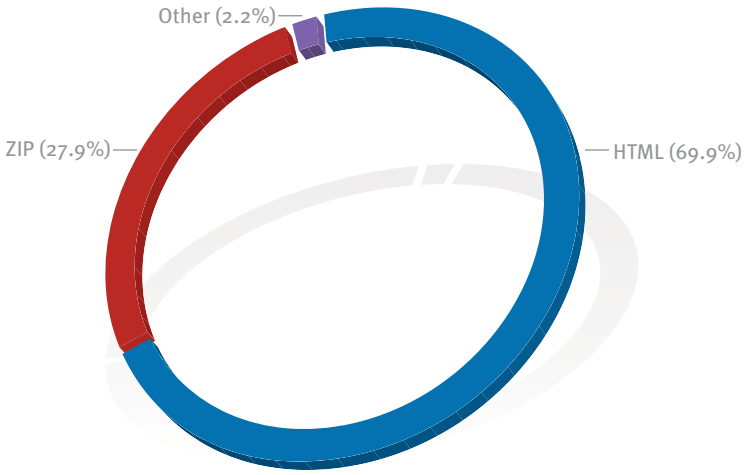
- The infection rate for Windows Vista is significantly lower than that of its predecessor, Windows XP, at any service pack level.
- The infection rates for the 64-bit editions of Windows Vista were both lower than those of their 32-bit counterparts.

- For each version of the operating system, the higher the service pack level, the lower the rate of infection. This trend can be observed consistently across client and server operating systems half-year period over half-year period. There are several reasons for this:
  - Service packs include fixes for all security vulnerabilities fixed in security updates at the time of issue, and sometimes they include additional security features and/or changes to default settings that help to protect users.
- Server versions of Windows typically display a lower infection rate, on average, than client versions, especially when comparing the latest service pack version for each operating system.

E-Mail Threats

- Many e-mail systems block incoming attached files of types that are often used to transmit malware. In 1H08, eight extensions accounted for 99.8% of the attachments blocked by Microsoft Exchange Hosted Services, with just two extensions—.html and .zip—accounting for 97.8% of blocked attachments.

FIGURE 14. Messages with file attachments blocked by Exchange Hosted Services, by extension, 1H08



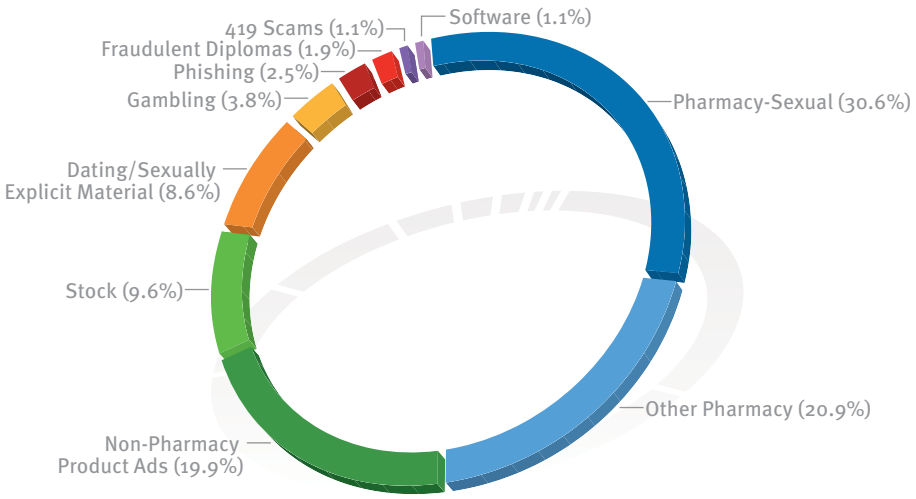
- The threat most blocked by Exchange Hosted Services in 1H08—by a wide margin—was HTML/IframeRef, which was blocked more than seven times as often as the second-most prevalent threat. The security update that addresses the particular vulnerability targeted by this exploit was released by Microsoft in December 2004[8].

[8] For more information on the HTML/IframeRef patch, see http://www.microsoft.com/technet/security/Bulletin/MS04-040.mspx

Spam and Phishing Trends

Microsoft Exchange Hosted Services blocked more than 90% of messages received over the Internet in 1H08, similar to the trend observed in 2H07.

FIGURE 15. Inbound messages blocked by Exchange Hosted Services, by category, 1H08



- Advertisements for pharmaceutical products accounted for 51.5% of the spam messages blocked by Exchange Hosted Services in 1H08, with advertisements mentioning products, such as Viagra and Cialis, accounting for the majority of those (30.6% of the overall total); in most cases, the advertisements are fraudulent. Non-pharmaceutical product advertisements account for another 19.9% of the total.
- Of the remainder, most involve overt scams, like "pump and dump" stock schemes and fraudulent university diplomas.
- Phishing attacks only accounted for 2.5% of the total number of e-mail messages blocked.
- The total number of active phishing pages at any one time remained roughly consistent throughout 1H08.
- Though U.S.-based financial institutions remain the most frequent target for phishing attempts, Microsoft phishing researchers have seen a gradual move toward targets located in other English-speaking countries, notably the United Kingdom and India.

Help Microsoft improve the Security Intelligence Report

Thank you for taking the time to read the latest volume of the Microsoft Security Intelligence Report. We want to ensure that this report remains as usable and relevant as possible for our customers. If you have any feedback on this volume of the report, or if you have suggestions as to how we can improve future volumes, please let us know by sending an e-mail message to sirfb@microsoft.com.

Thanks and best regards,
Microsoft Trustworthy Computing