

Microsoft Security Intelligence Report volume 7 (January through June 2009)

Key Findings Summary

Volume 7 of the Microsoft® Security Intelligence Report provides an in-depth perspective on malicious and potentially unwanted software, software exploits, security breaches and software vulnerabilities (both in Microsoft software and in third-party software). Microsoft developed these perspectives based on detailed analysis over the past several years, with a focus on the first half of 2009 (1H09)¹.

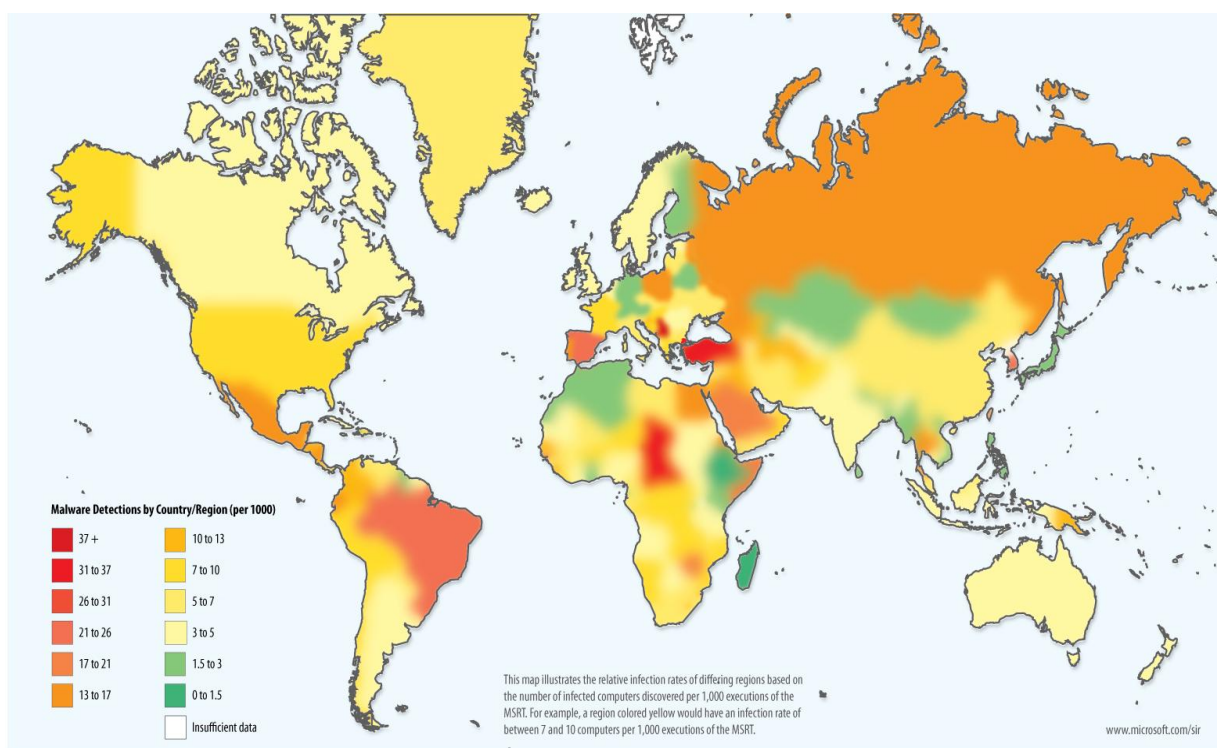
This document is a summary of the key findings of the report. The full Security Intelligence Report also offers strategies, mitigations, and countermeasures and can be downloaded from <http://www.microsoft.com/sir>.

Malicious and Potentially Unwanted Software

Geographic Trends

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

Figure 1. Infection rates by country/region, 1H09, expressed in CCM²

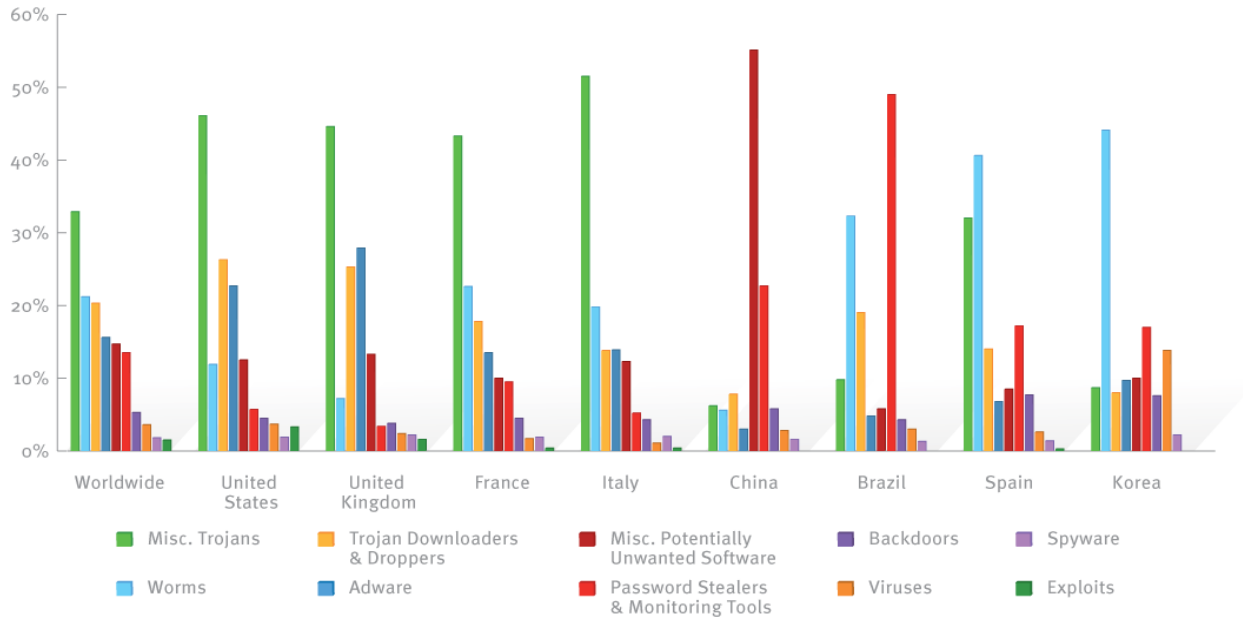


¹ The nomenclature used throughout the report to refer to different reporting periods is nHYY, where nH refers to either the first (1) or second (2) half of the year, and YY denotes the year. For example, 1H09 represents the period covering the first half of 2009 (January 1 through June 30), while 2H08 represents the period covering the second half of 2008 (July 1 through December 31).

² 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.

- In the **United States**, the **United Kingdom**, **France** and **Italy** trojans were the largest single category of threat; in **China**, several language-specific browser-based threats were prevalent; in **Brazil**, malware targeting online banking was widespread; in **Spain** and **Korea**, worms dominated, led by threats targeting online gamers. In-depth descriptions of the threats found in 18 countries are available in the full version of the [Security Intelligence Report](#).

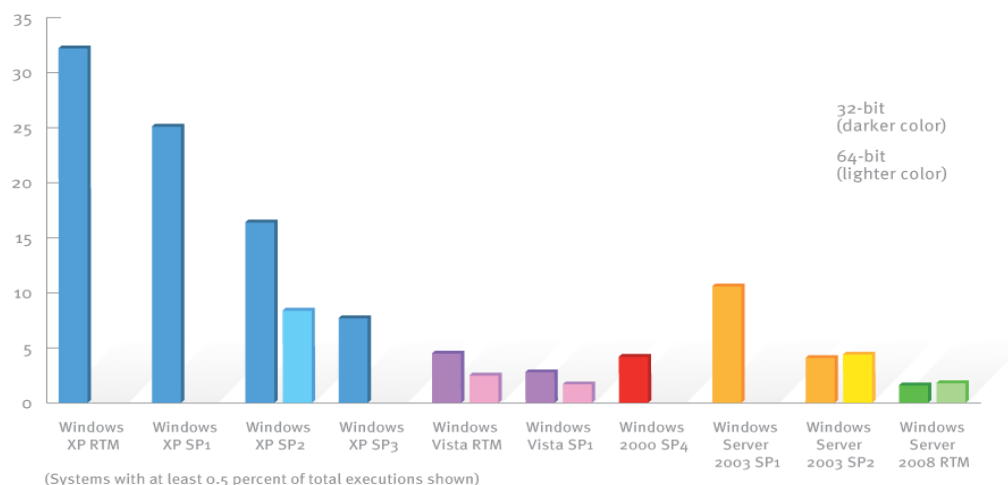
Figure 2. Threat categories worldwide and in the eight locations with the most computers cleaned, by incidence among all computers cleaned, 1H09



Operating System Trends

- Different Microsoft Windows operating system versions show differing rates of infection due to the different features and service packs that are available for each, and differences in the way people and organizations use each version (note that the infection rate for each version of Windows is calculated separately; the infection rate for a version is not affected by the number of computers running it).

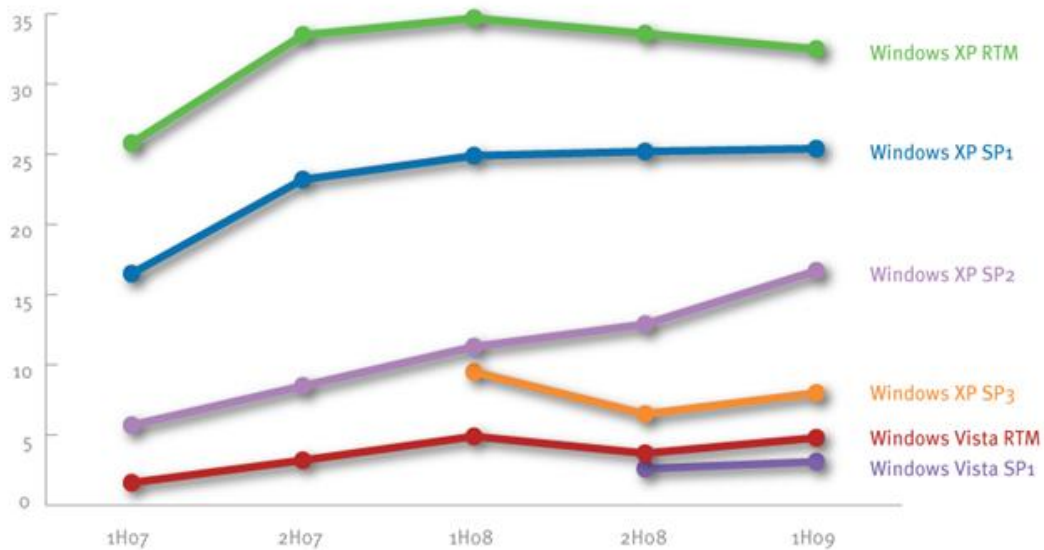
Figure 3. Number of computers cleaned for every 1,000 MSRT executions, by operating system, 1H09



- Infection rates for Windows Vista were significantly lower than Windows XP in all configurations in 1H09.
 - The infection rate of Windows Vista SP1 was 61.9 % less than Windows XP SP3.³
 - Comparing RTM versions, the infection rate of Windows Vista was 85.3 % less than Windows XP.
- The infection rate of Windows Server 2008 RTM was 52.6 % less than Windows Server 2003 SP2.
- The higher the service pack level, the lower the rate of infection:
 - Service packs include all previously released security updates at the time of issue. They can also include additional security features, mitigations, or changes to default settings to protect users.
 - Users who install service packs may generally maintain their computers better than users who do not install service packs and may also be more cautious in the way they browse the Internet, open attachments, and engage in other activities that can open computers to attack.
- Server versions of Windows typically display a lower infection rate on average than client versions. Servers tend to have a lower effective attack surface than computers running client operating systems because they are more likely to be used under controlled conditions by trained administrators and to be protected by one or more layers of security.

The figure below shows the consistency of these trends over time, showing infection rates for different versions of the 32-bit editions of Windows XP and Windows Vista for each six-month period between 1H07 and 1H09.

Figure 4. CCM trends for 32-bit versions of Windows Vista and Windows XP, 1H07-1H09

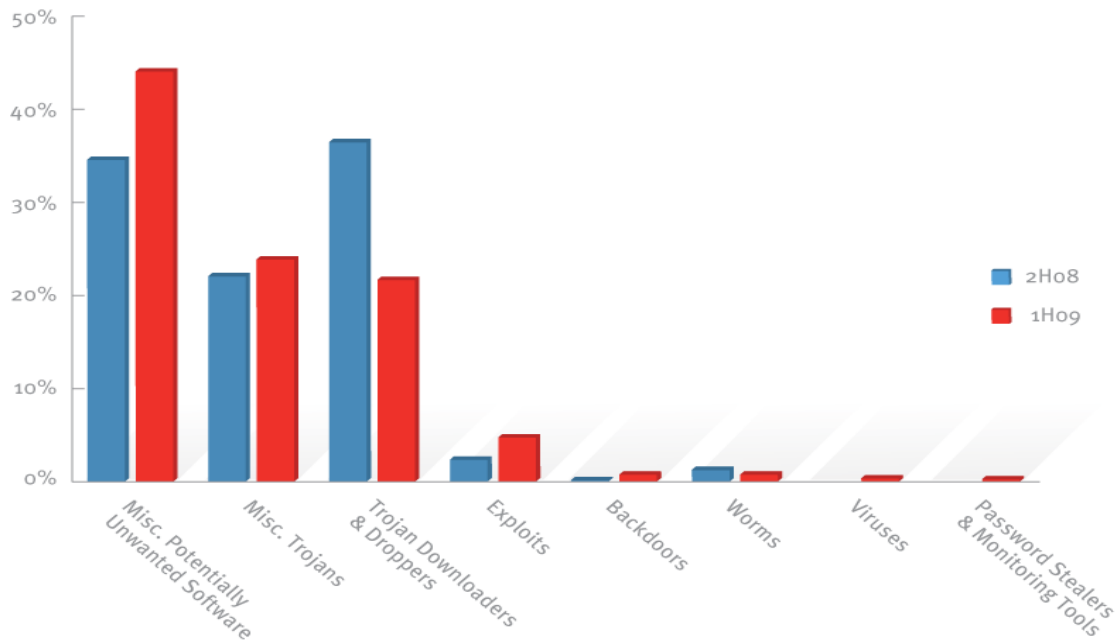


³ Windows Vista Service Pack 2 was released on June 30, the last day of 1H09, and is therefore not included in this analysis.

Analysis of Malware Hosts

- The SmartScreen Filter, introduced in Internet Explorer 8, provides phishing and anti-malware protection. The figure below details patterns of malware distribution detected by the SmartScreen Filter in 1H09.
- The Miscellaneous Potentially Unwanted Software category increased from 35.0 % of malware impressions in 2H08 to 44.5 % in 1H09, while the percentage of computers cleaned declined from 22.8 percent to 14.9 percent for the category. This suggests that SmartScreen and similar technologies may be successfully intercepting these threats before they are downloaded to computers.
- Miscellaneous Potentially Unwanted Software is disproportionately likely to be distributed over the Web - by contrast, worms are rarely distributed by malicious Web sites, accounting for just 1.2 percent of SmartScreen impressions, compared to 21.3 percent of computers cleaned.

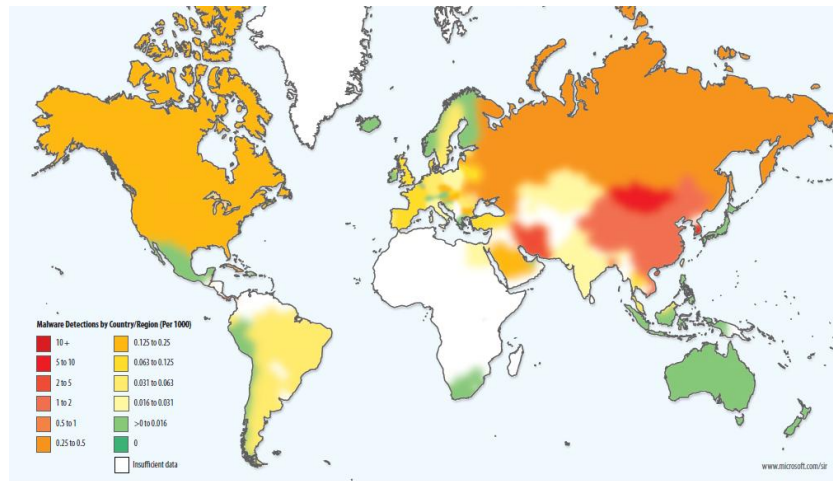
Figure 7. Threats hosted at URLs blocked by the SmartScreen Filter, by category



Geographic Distribution of Malware Hosting Sites

- More malware distribution sites are discovered on a daily basis than phishing sites
- Malware hosting tends to be more stable and less geographically diverse.
 - This is probably due to the relatively recent use of server takedowns and Web reputation as weapons in the fight against malware distribution, which means that malware distributors have not been forced to diversify their hosting arrangements, as phishers have.

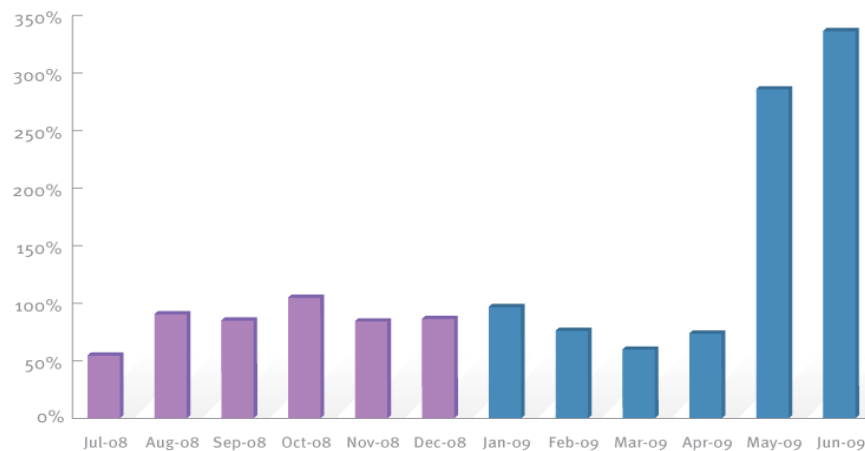
Figure 8. Malware distribution sites per 1,000 Internet hosts for locations around the world in 1H09



Analysis of Phishing Sites

- Phishing impressions rose significantly in 1H09, due primarily to a large increase in phishing attacks targeting social networking sites.
- Phishers continued to target a wider range of Web-site types than in the past, with gaming sites, portals, and the online presences of major corporations being some of the most frequently-targeted sites in 1H09.
- After remaining mostly consistent throughout 2H08 and through April of 2009, the number of impressions suddenly nearly quadrupled in May, and rose even higher in June due in part to a campaign or campaigns targeting social networks. More information on these trends can be found in the full [Security Intelligence Report](#).

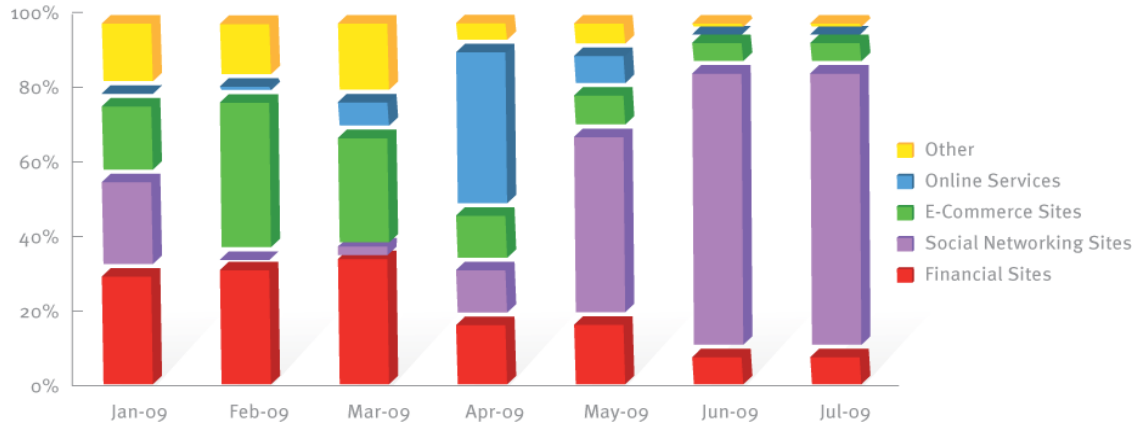
Figure 9. Phishing impressions tracked each month in 2H08 and 1H09, indexed to January 2009



Institutions

- Financial institutions, social networks and e-commerce sites remain favored targets for phishing attempts.
- Researchers also observed some diversification into other types of institutions, such as online gaming sites, Web portals, and large software and telecommunications companies.

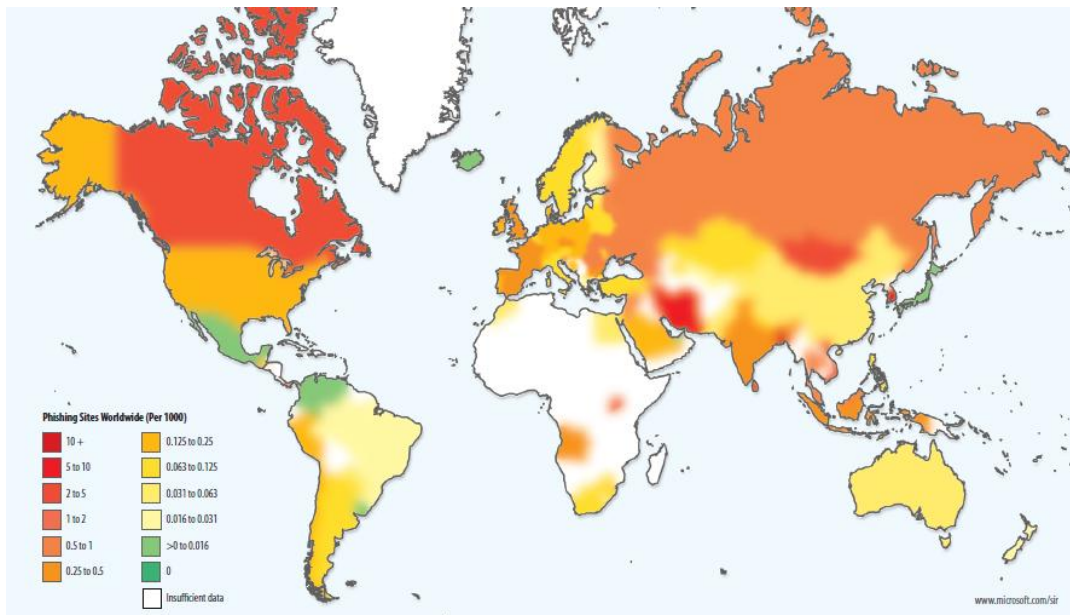
Figure 10. Impressions for each type of phishing site each month in 1H09



Geographic Distribution of Phishing Sites

- Phishing sites are hosted all over the world on free hosting sites, on compromised Web servers, and in numerous other contexts; performing geographic lookups on the IP addresses of the sites makes it possible to create maps showing the geographic distribution of sites and to analyze patterns.

Figure 11. Phishing sites per 1,000 Internet hosts for locations around the world in 1H09



E-mail Threats

- Forefront Online Protection for Exchange (FOPE) blocked 97.3% of all messages received at the network edge in 1H09, up from 92.2% in 2H08. In total, FOPE blocked more than 98% of all messages received.
- Spam in 1H09 was dominated by product advertisements, primarily pharmaceutical products. In total, product advertisements accounted for 69.2 % of spam in 2H08.
- The figure below shows the countries and regions around the world that originated the most spam, as detected by FOPE from March through June, 2009.
- A full list of countries and the number of spam messages originating from them can be found in the full [Security Intelligence Report](#).

Figure 12. Inbound messages blocked by FOPE content filters in 1H09, by category

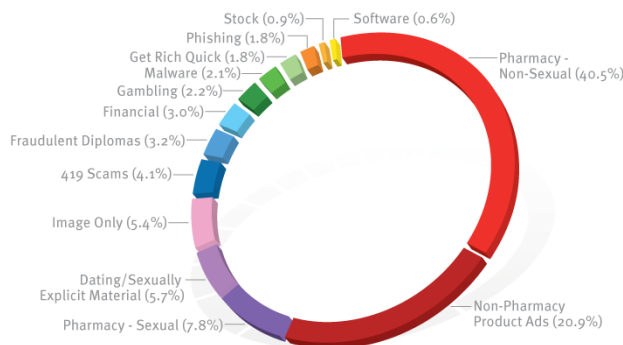
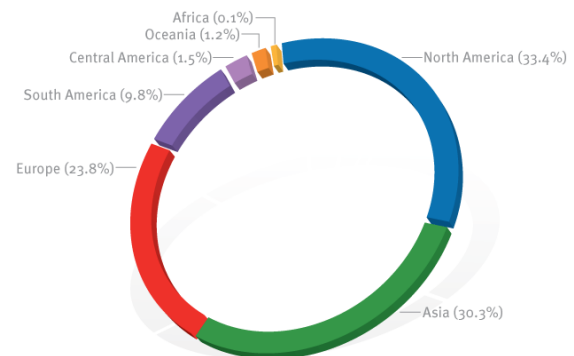


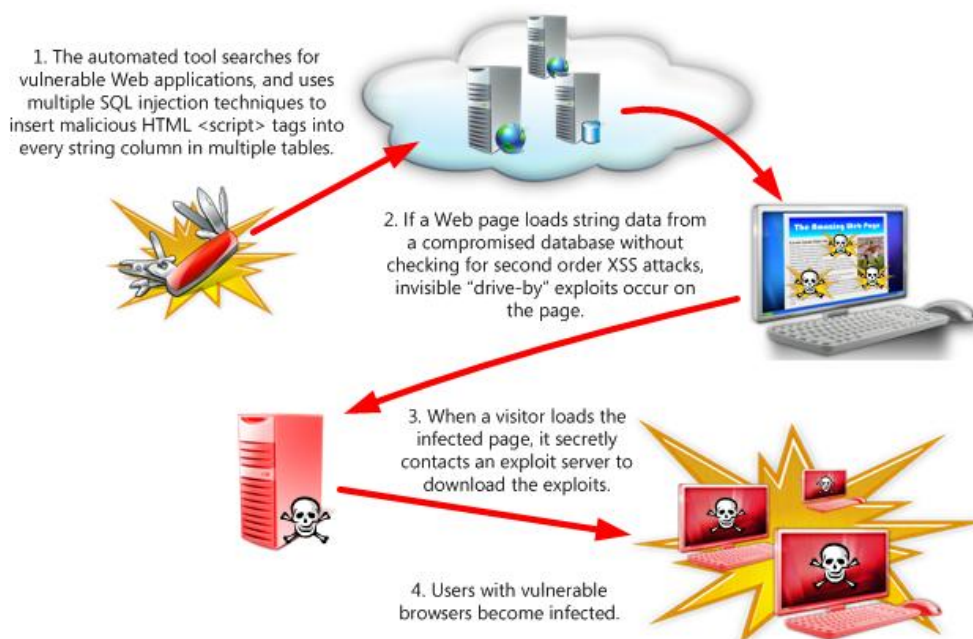
Figure 13. Geographic origins of spam in 1H09, by percentage of total spam sent



Automated SQL Injection Attacks

- *SQL injection* is a technique used by attackers to damage or steal data residing in databases that use Structured Query Language (SQL) syntax to control information storage and retrieval. Use of this technique was widely observed during 1H09.
- SQL injection usually involves directly passing malicious SQL code to a program or script that queries a database. If the program or script does not properly validate the input, the attacker may be able to execute arbitrary commands.
- Beginning in late 2007 attackers began to use automated tools to compromise large numbers of Web sites through SQL injection, in an attempt to spread malware. Web applications often construct pages dynamically as they are requested, by retrieving information from a database and using it to populate the page.

Figure 14. How a mass SQL injection tool works



- More details on SQL injection techniques and guidance on how to protect against them can be found in the [Security Intelligence Report](#).

Exploit Trends - Browser-Based Exploits

To assess the relative prevalence of browser-based exploits in 1H09, Microsoft analyzed a sample of data 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

- For browser-based attacks on Windows XP–based machines, Microsoft vulnerabilities accounted for 56.4% of the total. On Windows Vista–based machines, Microsoft vulnerabilities accounted for just 15.5% of the total.

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

Figure 15. Browser-based exploits targeting Microsoft and third-party software on computers running Windows XP, 1H09

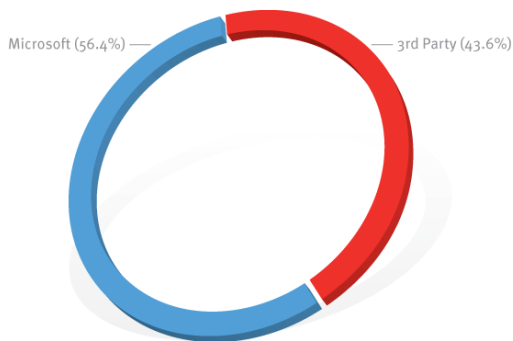
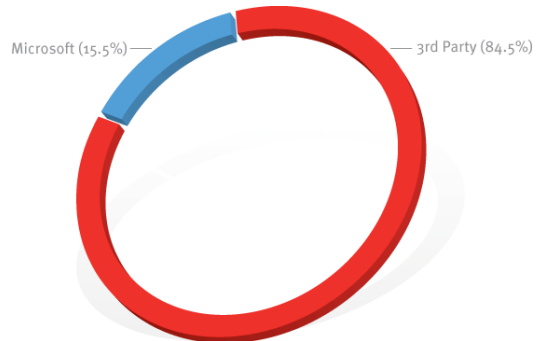


Figure 16. Browser-based exploits targeting Microsoft and third-party software on computers running Windows Vista, 1H09



- Microsoft software accounted for 6 of the top 10 browser-based vulnerabilities attacked on computers running Windows XP in 1H09, compared to only 1 on computers running Windows Vista. The vulnerabilities are referenced below by the relevant CVSS bulletin number or by Microsoft Security Bulletin number as appropriate.

Figure 17. Top 10 browser-based vulnerabilities exploited on computers running Windows XP, 1H09

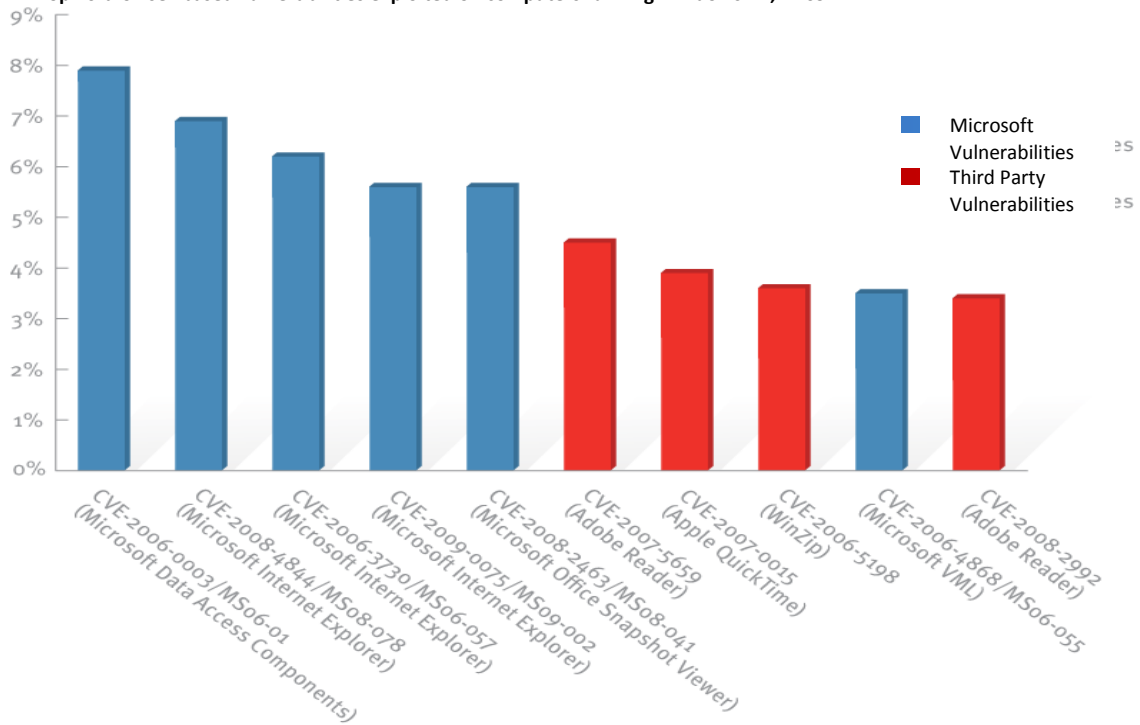
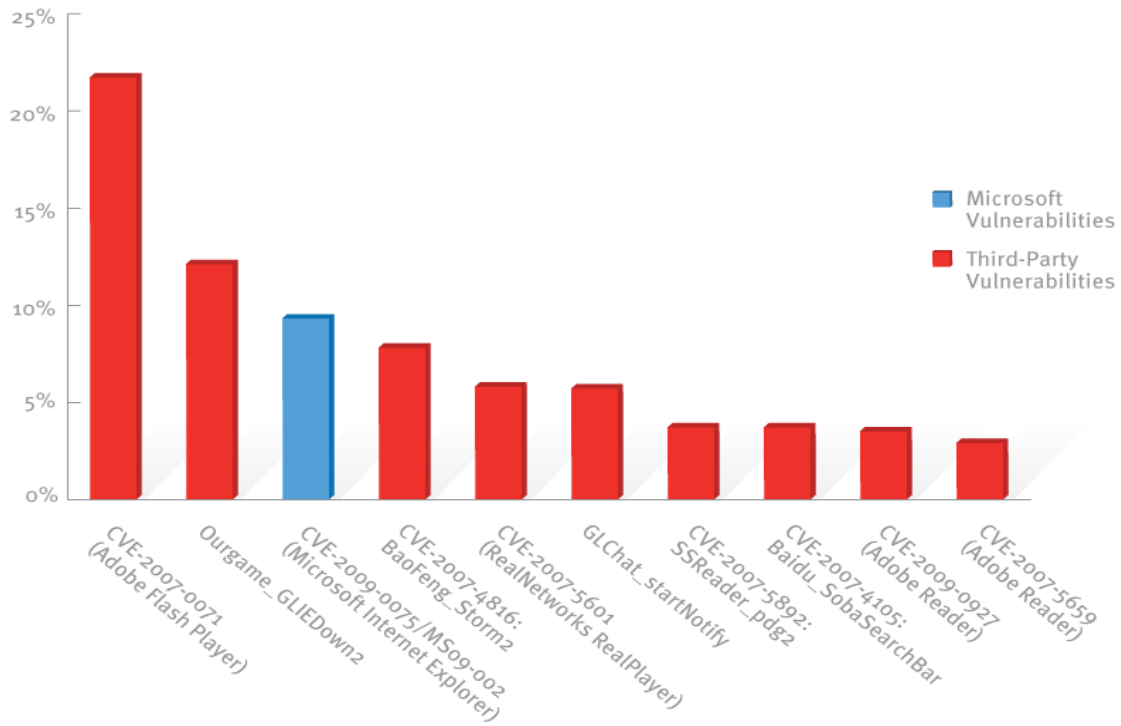


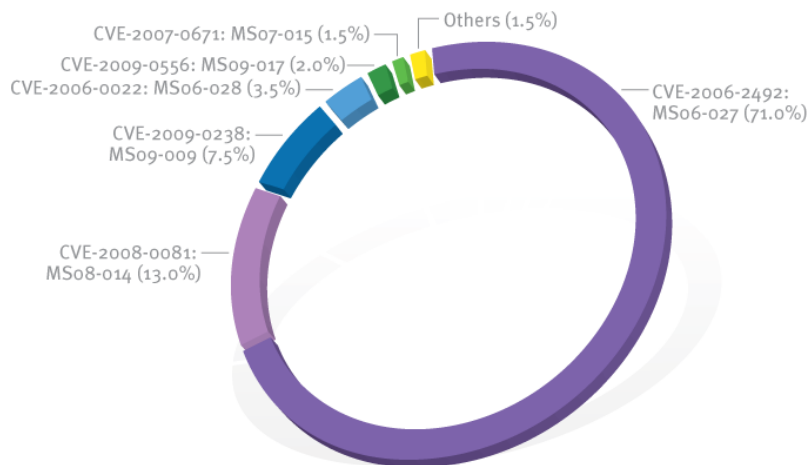
Figure 18. Top 10 browser-based vulnerabilities exploited on computers running Windows Vista, 1H09



Microsoft Office Format Files

- The most frequently-exploited vulnerabilities in Microsoft Office software during 1H09 were also some of the oldest. More than half of the vulnerabilities exploited were first identified and addressed by Microsoft security updates in 2006.
- 71.2% of the attacks exploited a single vulnerability for which a security update (MS06-027) had been available for three years. Computers which had this update applied were protected from all these attacks.

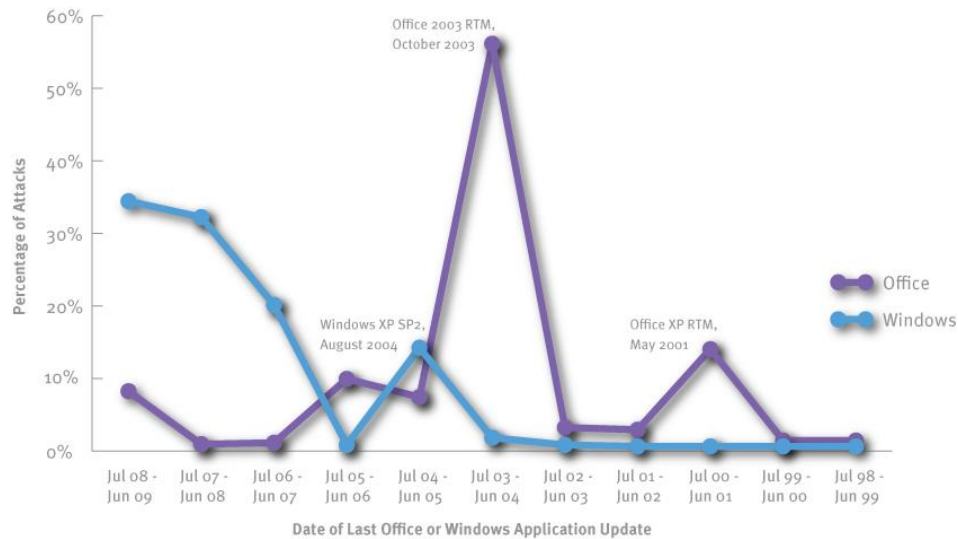
Figure 19. Microsoft Office file format exploits encountered in 1H09, by percentage



- The figure below shows the total attacks observed in the sample set against Microsoft Windows and Microsoft Office during 1H09. The horizontal axis shows the last date that the computers in the sample set were updated with security updates for Windows and Office.

- The majority of Office attacks observed in 1H09 (55.5 percent) affected Office program installations that had last been updated between July 2003 and June 2004. Most of these attacks affected Office 2003 users who had not applied a single service pack or other security update since the original release of Office 2003 in October 2003.
- By contrast, the computers in the sample set were significantly more likely to have had recent Windows security updates applied.
- Users who do not keep both their Office program installations and Windows operating systems up to date with service packs and security updates are at increased risk of attack.
- Microsoft recommends that computers are configured to use Microsoft Update to keep Windows operating systems and other Microsoft software updated.

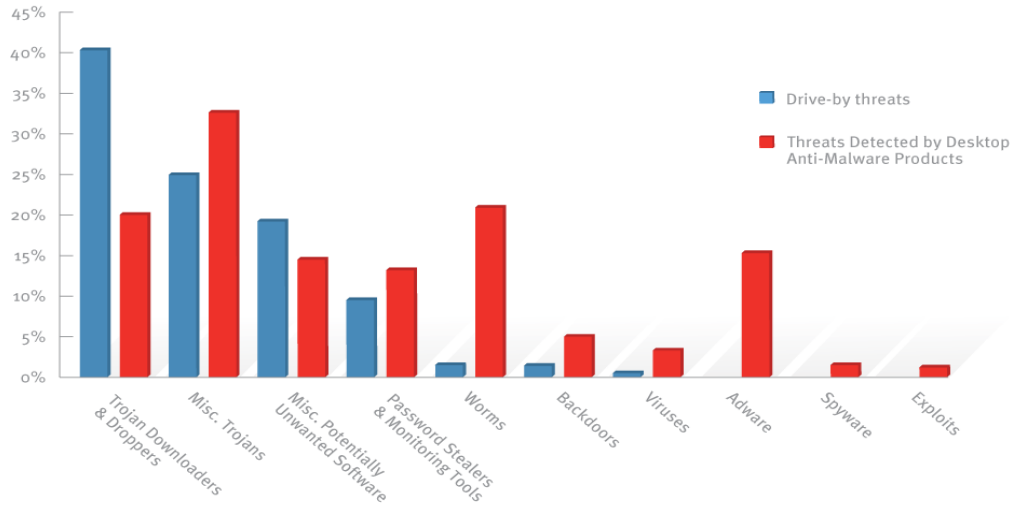
Figure 20. Microsoft Office file format exploits encountered in 1H09, by date of last Windows or Office security update



Analysis of Drive-by Download Pages

- The majority of drive-by download pages are hosted on compromised legitimate Web sites. Attackers gain access to legitimate sites through intrusion, or by posting malicious code to a poorly secured Web form, like a comment field on a blog.
- Compromised servers acting as exploit servers can have massive reach; one exploit server can be responsible for hundreds of thousands of infected web pages.
- Exploit servers in 2009 were able to infect many thousands of pages in a short period of time.

Figure 21. Types of threat payloads delivered through drive-by downloads in 1H09



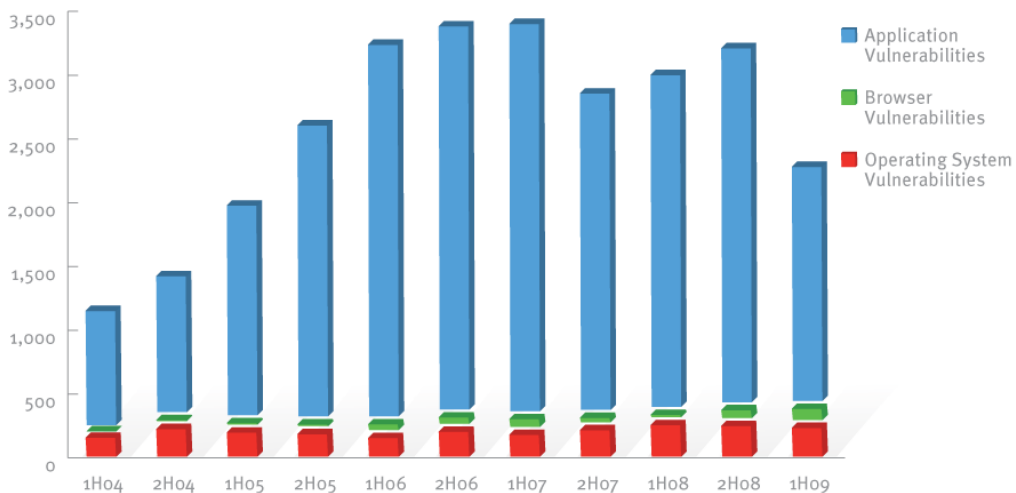
- The Trojan Downloaders & Droppers category was the most frequently-encountered category among drive-by download sites, with 40.7 % of the total. Trojan downloaders are well suited for delivery by drive-by download because they can be used to install other threats on infected computers.

Industry-Wide Vulnerability Disclosures

Vulnerabilities are 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 a compromised computer. Data in this section comes from third-party sources, published reports, and Microsoft’s own data.

- Total unique vulnerability disclosures across the industry decreased sharply in 1H09, down 28.4% from 2H08.
- While application vulnerabilities are down from 2H08, operating system vulnerabilities are roughly consistent with the previous period, and browser vulnerabilities actually increased slightly.

Figure 22. Industry-wide operating system, browser, and other vulnerabilities, 1H04-1H09



- Vulnerabilities rated as High severity by the Common Vulnerability Scoring System (CVSS)⁵ decreased 12.9% from 2H08; 46.0% of all vulnerabilities were rated as High severity.
- As with severity, the complexity trend in 1H09 is a generally positive one. 54.2 % of all vulnerabilities were Low complexity in 1H09, down from 57.7 % in 2H08, and down almost 30 percentage points over the last five years.

Figure 23. Industry-wide vulnerability disclosures by severity, 1H04-1H09

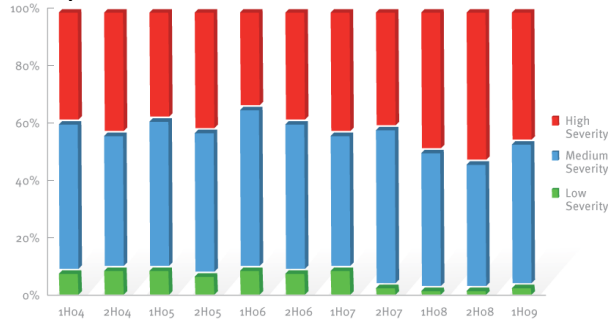
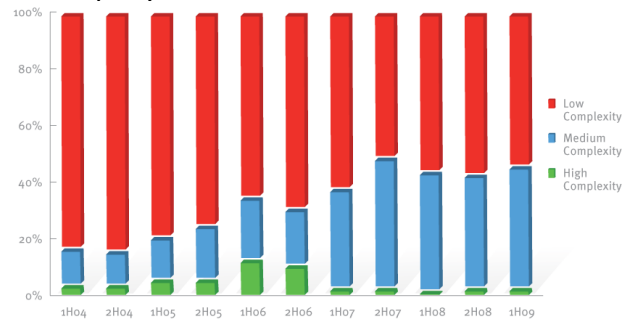
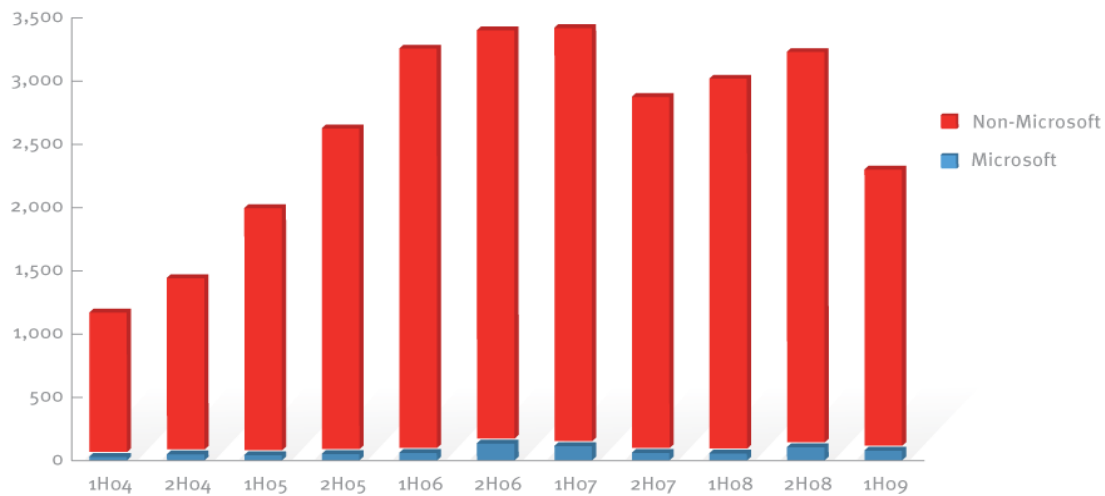


Figure 24: Industry-wide vulnerability disclosures by complexity, 1H04-1H09



- Microsoft vulnerability disclosures have mirrored those for the industry as a whole, though on a much smaller scale. Over the past five years, Microsoft vulnerability disclosures have consistently accounted for about 3–6 % of all disclosures industry-wide.

Figure 25. Vulnerability disclosures for Microsoft and non-Microsoft products, 1H04-1H09

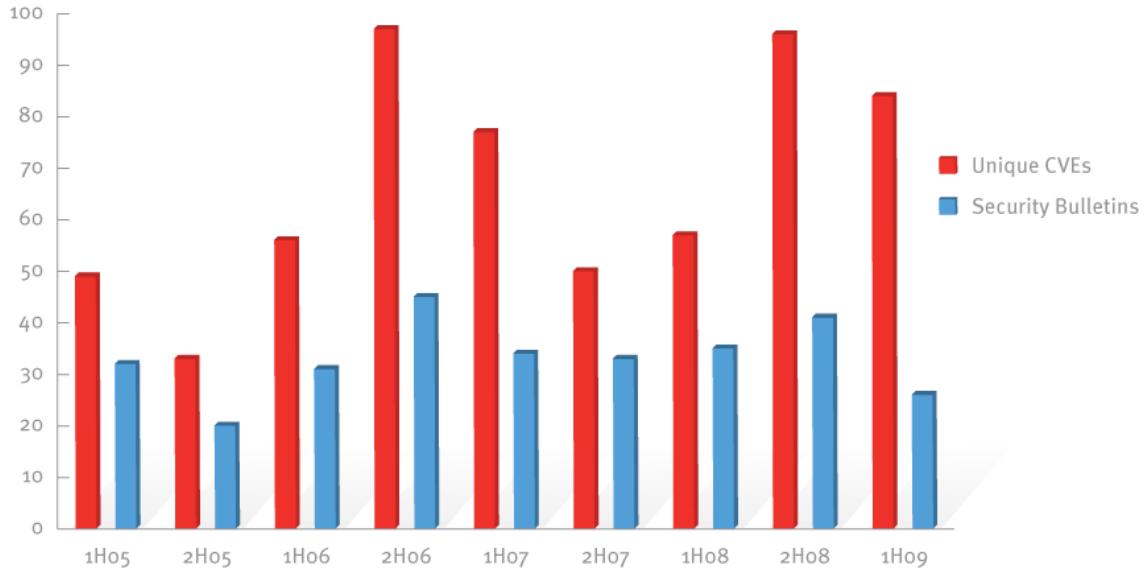


⁵ CVSS is an industry standard for assessing the severity of software vulnerabilities. See <http://www.first.org/cvss/> for more documentation and details.

Microsoft Vulnerability Details for 1H09

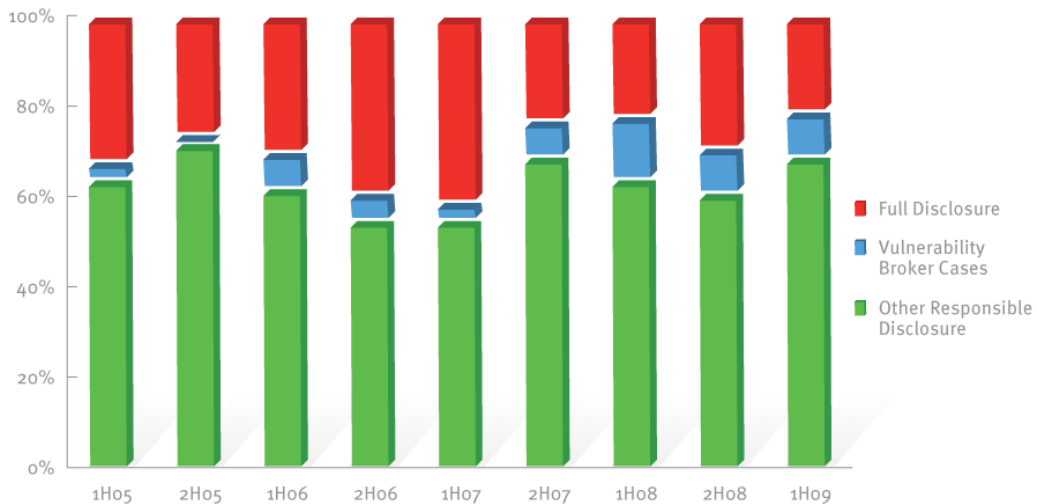
- In 1H09 Microsoft released 27 security bulletins, which addressed 85 individual CVE-identified vulnerabilities.

Figure 26. Security Bulletins released and CVEs addressed by half-year, 1H05-1H09



- *Responsible disclosure* means disclosing vulnerabilities privately to an affected vendor so it can develop a comprehensive security update to address the vulnerability before the details become public knowledge. This helps to keep users safer by preventing potential attackers from learning about newly discovered vulnerabilities before security updates are available.
- In 1H09, 79.5 % of vulnerabilities disclosed in Microsoft software adhered to responsible disclosure practices, up from 70.6 % in 2H08.

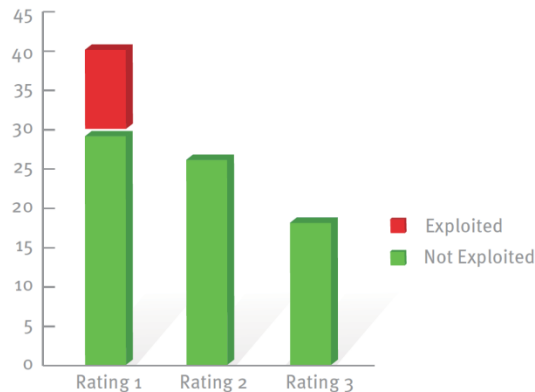
Figure 27. Responsible disclosures as a percentage of all disclosures involving Microsoft software, 1H05-1H09



Exploitability Index

- 41 vulnerabilities were assigned an Exploitability Index Rating of 1, meaning that they were considered the most likely to be exploited within 30 days of the associated security bulletin's release. Microsoft observed eleven of these vulnerabilities being exploited in the first 30 days.
- Of the 46 vulnerabilities that received Exploitability Index ratings of 2 or 3, indicating that exploitation would be unreliable or unlikely, none were identified to have been publicly exploited within 30 days.

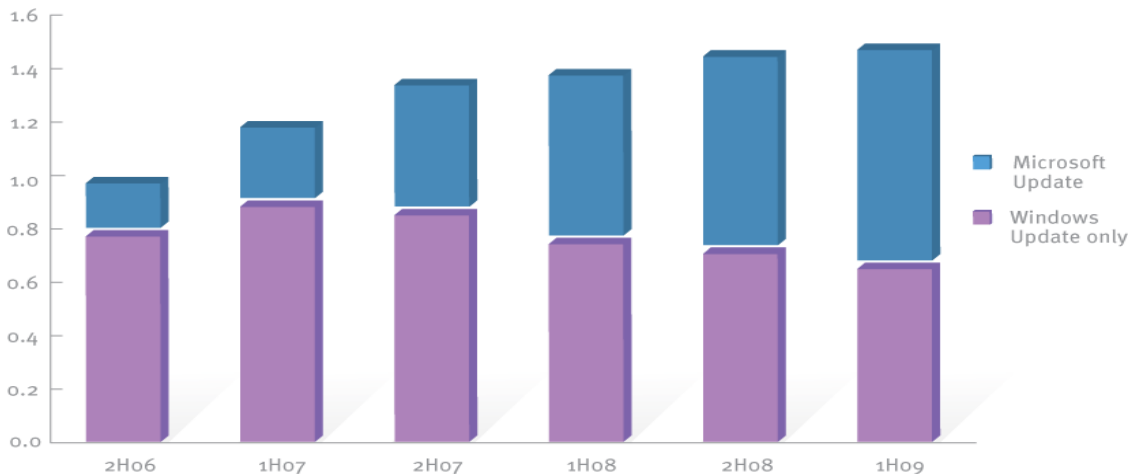
Figure 28. CVEs with exploits discovered within 30 days in 1H09, by Exploitability Index rating



Usage Trends for Windows Update and Microsoft Update

- The prompt adoption of security updates and other software upgrades can significantly mitigate the spread and impact of malware. Microsoft recommends that computers are configured to use Microsoft Update to keep Windows operating systems and other Microsoft software updated.
 - *Windows Update* provides updates for Windows components, for device drivers provided by Microsoft and other hardware vendors and also distributes signature updates for Microsoft anti-malware products, and the monthly release of the MSRT.
 - *Microsoft Update* provides all of the updates offered through Windows Update, and also provides updates for other Microsoft software, such as the Microsoft Office system.
- Microsoft Update adoption has risen significantly over the past several years, with increasing numbers of Windows Update users choosing to switch to the more comprehensive service.

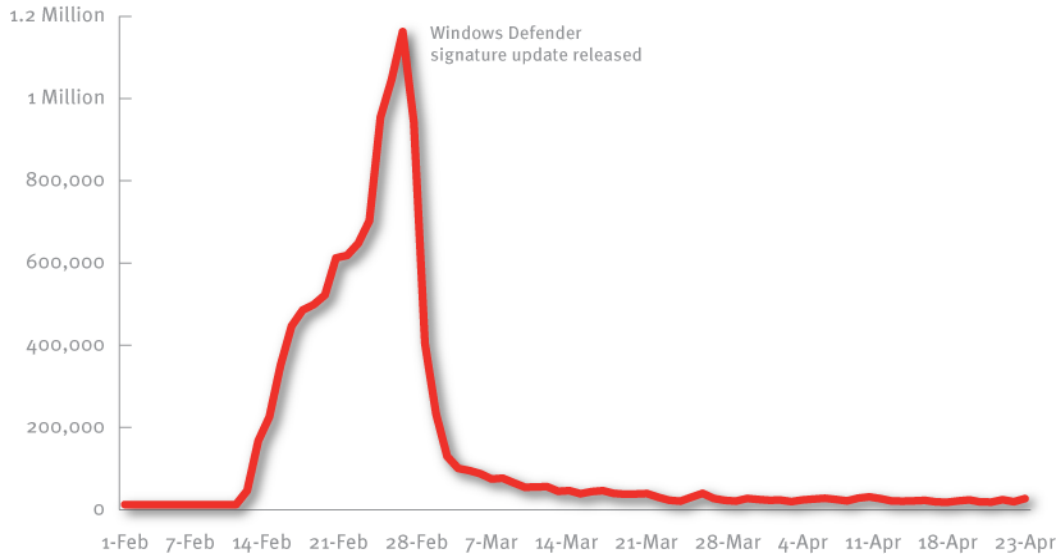
Figure 29. Usage of Windows Update and Microsoft Update, 2H06-1H09, indexed to 2H06 total usage



The Role of Automatic Updating

- Automatic updating is one of the most effective tools that users and organizations can utilize to help prevent the spread of malware.
- For example, in February 2007 the trojan downloader family Win32/Renos began infecting computers around the world. On February 27, Microsoft released a signature update for Windows Defender via Windows Update and Microsoft Update. Within three days, enough computers had received the new signature update to reduce the error reports from 1.2 million per day to less than 100,000 per day worldwide.

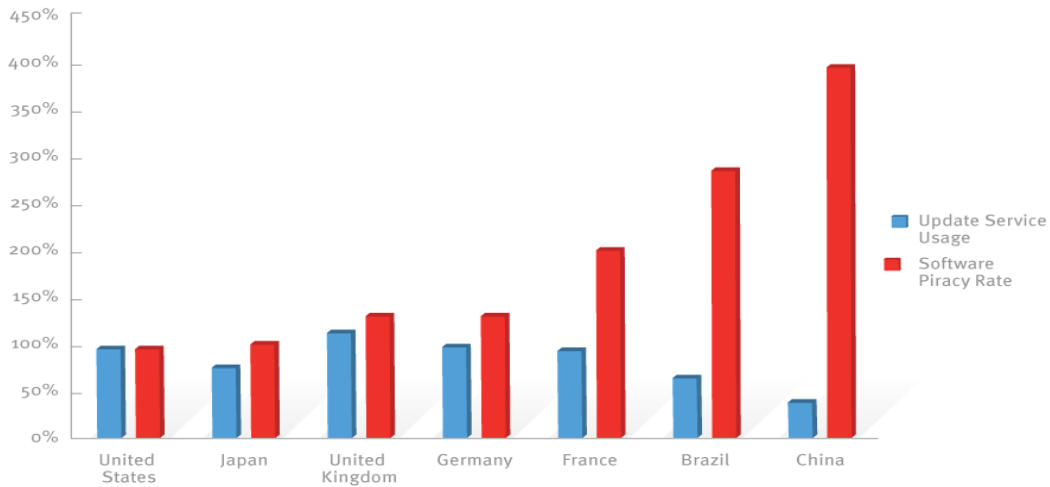
Figure 30. Windows error reports caused by Win32/Renos on Windows Vista, February - March 2007



Regional Variations in Update Service Usage

- Use of Microsoft online update services varies worldwide due to a number of factors, including broadband Internet connectivity, software piracy, and the percentage of computers managed in enterprise environments.
- The incidence of software piracy in a location tends to be strongly negatively correlated with usage of Windows Update and Microsoft Update.
- The figure below uses update service usage and software piracy rates in the United States to establish a baseline (shown as 100%) for each trend; other countries are displayed relative to the United States.

Figure 31. Update service usage and software piracy rates for seven locations worldwide, relative to the United States



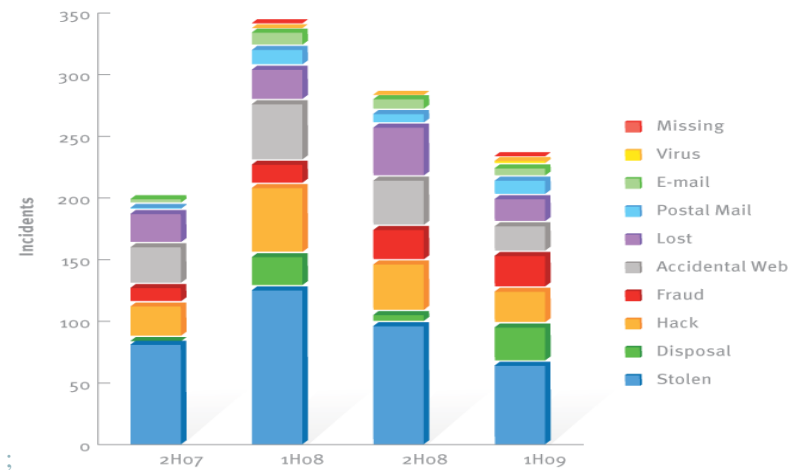
(Software piracy data from the Business Software Alliance, *Global Software Piracy Study*, 2008)
<http://global.bsa.org/globalpiracy2008/>

Security Breach Trends

This section examines security breach incidents from around the world with data provided by Open Security Foundation’s OSF Data Loss Database at <http://datalossdb.org>.

- The top category reported for data loss through a security breach in 1H09 continued to be stolen equipment, such as laptop computers (30.0% of all data-loss incidents reported), accounting for twice as many incidents as intrusion.
- Security breaches from “hacking” or malware incidents remain less than 15.0% of the total.

Figure 32. Security breach incidents, 2H07-1H09, by incident type



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 about 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

This summary is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS SUMMARY. No part of this summary may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this summary. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this summary does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2009 Microsoft Corporation. All rights reserved.

Microsoft, the Microsoft logo, Windows, Windows XP, Windows Vista, Bing and Microsoft Office are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.