Microsoft Security Intelligence Report
Volume 8 (July through December 2009)
Key Findings Summary

Introduction

Volume 8 of the *Microsoft® Security Intelligence Report* provides in-depth perspectives on malicious and potentially unwanted software, software exploits, security breaches, and software vulnerabilities in both Microsoft and third party software. Microsoft developed these perspectives based on detailed analysis over the past several years, with a focus on the second half of 2009 (2H09)[1].

This document summarizes the key findings of the report. The full *Security Intelligence Report* also includes deep analysis of trends found in more than 26 countries/regions around the world and offers strategies, mitigations, and countermeasures that can be used to manage the threats that are documented in the report.

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

The computer threat landscape changes constantly. As threats continue to evolve from mischievous hackers who pursue notoriety to organized criminals who steal data for monetary gain, public concern continues to escalate. Microsoft formed Trustworthy Computing (TwC) in 2002 to commit itself to a strategy of providing more secure, private, and reliable computing experiences for our customers.

TwC Security includes three technology centers that work closely together to address security issues and supply the services, information, and responses that are needed to better understand the evolving threat landscape, help protect customers from online threats, and share knowledge with the broader security ecosystem. These three security centers include:

- The Microsoft Malware Protection Center
- The Microsoft Security Response Center
- The Microsoft Security Engineering Center

The blogs of these three security centers, as well as other blogs like the Data Privacy Imperative blog, can be found at www.microsoft.com/twc/blogs.

The data and analysis in this *Key Findings Summary* and in the full *Security Intelligence Report* are presented from the perspective of these three centers and their partners in the various Microsoft product groups.

[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, 2H09 represents the period covering the second half of 2009 (July 1 through December 31), and 2H08 represents the period covering the second half of 2008 (July 1 through December 31).

Key Findings from the Microsoft Malware Protection Center

Global Malicious and Potentially Unwanted Software Trends

Microsoft security products obtain user consent to gather data from more than 500 million computers worldwide and from some of the Internet's busiest online services. Analysis of this data provides a comprehensive and unique perspective on malware and potentially unwanted software activity around the world.

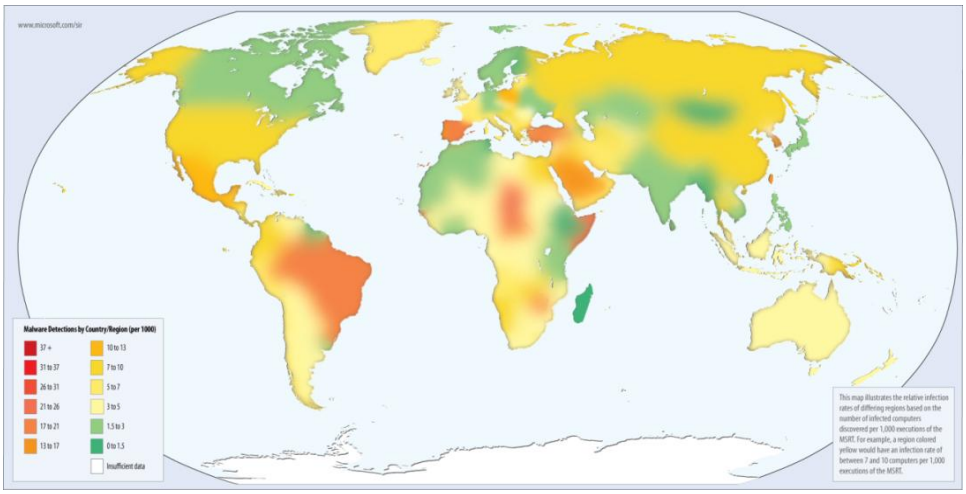
Geographic Trends

Figure 1: The top 15 locations with the most computers cleaned by Microsoft desktop anti-malware products in 2H09 (the full *SIR* includes the top 25 locations)

	Country/Region	Computers Cleaned (2H09)	Computers Cleaned (1H09)	Change
1	United States	15,383,476	13,971,056	10.1% ▲
2	China	3,333,368	2,799,456	19.1% ▲
3	Brazil	2,496,674	2,156,259	15.8% ▲
4	United Kingdom	2,016,132	2,043,431	-1.3% ▼
5	Spain	1,650,440	1,853,234	-10.9% ▼
6	France	1,538,749	1,703,225	-9.7% ▼
7	Korea	1,367,266	1,619,135	-15.6% ▼
8	Germany	1,130,632	1,086,473	4.1% ▲
9	Canada	967,381	942,826	2.6% ▲
10	Italy	954,617	1,192,867	-20.0% ▼
11	Mexico	915,786	957,697	-4.4% ▼
12	Turkey	857,463	1,161,133	-26.2% ▼
13	Russia	677,601	581,601	16.5% ▲
14	Taiwan	628,202	781,214	-19.6% ▼
15	Japan	609,066	553,417	10.1% ▲
	Worldwide	41,024,375	39,328,515	4.3% ▲

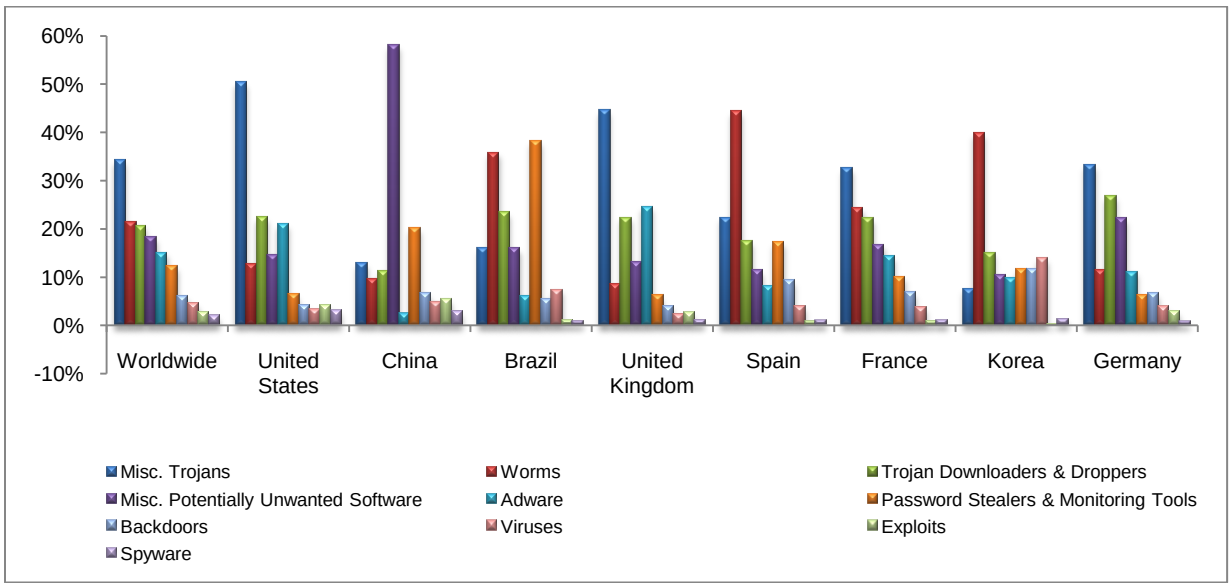
- Two of the largest increases in the number of computers cleaned were experienced by China and Brazil, which increased 19.1 percent and 15.8 percent from 1H09, respectively. Much of this increase was caused by the September 2009 release of Microsoft Security Essentials, an anti-malware solution for home computers that is available at no charge to licensed users of Windows. China and Brazil have both been significant early adopters of Security Essentials.
- A number of locations experienced significant decreases in infection rates:
  - The largest decline in the number of computers cleaned is the 26.2 percent decrease in Turkey, which can be mainly attributed to the decreased prevalence of Win32/Taterf and Win32/Frethog, two password stealers that target players of online games.
  - The decreased prevalence of Taterf and Frethog is largely responsible for a 19.6 percent decrease for Taiwan.
  - Italy's 20.0 percent decline is mostly the result of a steep decline in detections of the Trojan family Win32/Wintrim

Figure 2: Infection rates by country/region in 2H09, expressed in CCM[2], for locations around the world with at least 1 million average monthly MSRT executions in 2H09



CCM for 200+ countries/regions are available in the full *SIR*.

Figure 3: Threat categories worldwide and in the eight locations with the most infected computers, by incidence among all computers cleaned by Microsoft desktop anti-malware products, in 2H09



- The threat environments in the United States and the United Kingdom are very similar. Both locations have nearly the same proportion of threat categories, and 7 of the top 10 families in each location are the same. Miscellaneous Trojans account for the largest single threat category. Families such as Win32/FakeXPA, Win32/Renos, and Win32/Alureon rank high in both locations.
- In China, many of the most prevalent threats are localized families that don't appear in the list of top threats for any other location. These include some versions of Win32/BaiduSobar, a Chinese-language browser

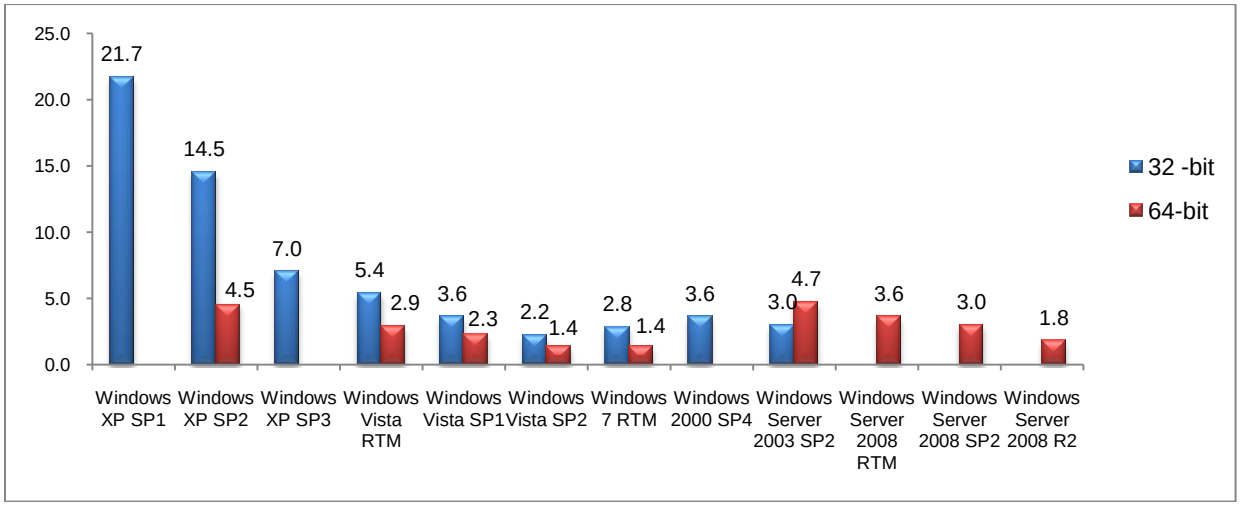
[2] To produce a consistent measure of infection that can be used to compare populations of computers in different locations to each other, infection rates in this report are expressed using a metric called computers cleaned per thousand, or CCM, which represents the number of reported computers cleaned for every 1,000 executions of the MSRT. (The M in CCM stands for mille, the Latin word for thousand.)

toolbar, and password stealers such as Win32/Lolyda and Win32/Ceekat that target several popular online games in China.

- In Brazil, Password Stealers & Monitoring Tools is the most common category primarily because of a number of Portuguese-language password stealers that target online users of Brazilian banks. Win32/Bancos is the most common of these password stealers.
- Korea is dominated by worms, primarily Win32/Taterf, which targets players of online games. The prevalence of Taterf in Korea might be caused in part by the worm's propensity to spread easily in Internet cafés and LAN gaming centers, which are popular in Korea.

Operating System Trends

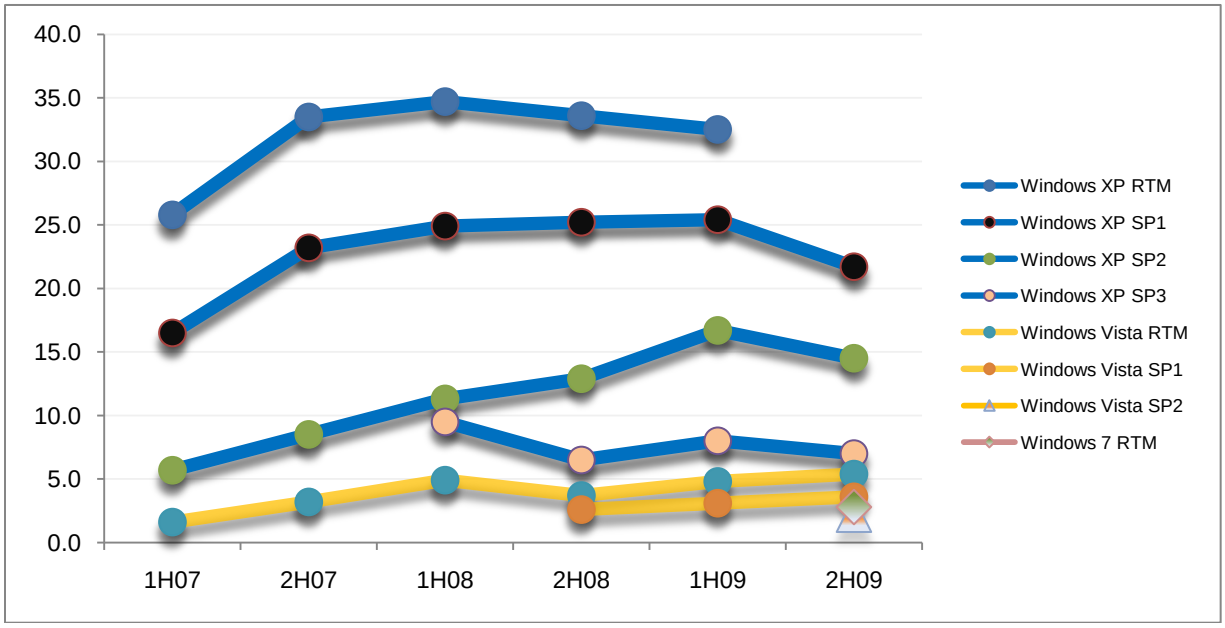
Figure 4: Number of computers cleaned for every 1,000 MSRT executions, by operating system, in 2H09



- As in previous periods, infection rates for more recently released operating systems and service packs are consistently lower than previous ones, for both client and server platforms.
- Windows 7, which was released in 2H09, and Windows Vista® with Service Pack 2 have the lowest infection rates of any platform on the chart.
  - The 64-bit versions of Windows 7 and Windows Vista SP2 had lower infection rates (1.4 for both) than any other operating system configuration in 2H09, although the 32-bit versions both had infection rates that were less than half of Windows XP with its most up-to-date service pack, SP3.
- For operating systems with service packs, each successive service pack has a lower infection rate than the one before it.
  - The infection rate for Windows XP with SP3 is less than half of that for SP2, and less than a third of that for SP1.
  - Similarly, Windows Vista SP2 has a lower infection rate than SP1, which has a lower infection rate than Windows Vista RTM.
  - For server operating systems, the infection rate for Windows Server® 2008 with SP2 is 3.0, which is 20 percent less than that of its predecessor, Windows Server 2008 RTM.

The following figure illustrates the consistency of these trends over time; it shows infection rates for different versions of the 32-bit editions of Windows XP and Windows Vista for each six-month period between 1H07 and 2H09.

Figure 5: CCM trends for 32-bit versions of Windows XP and Windows Vista, 1H07–2H09



Worldwide Category Trends

Figure 6: Top 10 malware and potentially unwanted software families detected by Microsoft anti-malware desktop products in 2H09 (the full *SIR* includes the top 25 families)

	Family	Most Significant Category	Computers Cleaned (2H09)
1	Win32/Taterf	Worms	3,921,963
2	Win32/Renos†	Trojan Downloaders & Droppers	3,640,697
3	Win32/FakeXPA*	Miscellaneous Trojans	2,939,542
4	Win32/Alureon†	Miscellaneous Trojans	2,694,128
5	Win32/Conficker†	Worms	1,919,333 [3]
6	Win32/Frethog	Password Stealers & Monitoring Tools	1,823,066
7	Win32/Agent	Miscellaneous Trojans	1,621,051
8	Win32/BaiduSobar	Misc. Potentially Unwanted Software	1,602,230
9	Win32/GameVance	Adware	1,553,646
10	Win32/Hotbar	Adware	1,476,838

Asterisks (*) indicate rogue security software families.
Daggers (†) indicate families that have been observed to download rogue security software.

- Overall, detections of the top threats are down by a considerable margin from the first half of 2009.
  - In 1H09, seven families were removed from at least 2 million computers by Microsoft desktop anti-malware tools, compared to just four families in 2H09.
  - Even Win32/Taterf, 2H09's top family, was removed from nearly 1 million fewer computers this period than in 1H09.
  - The 3.9 million computers infected by Taterf in 2H09 is significantly less than 1H09's top family, Win32/Zlob, which was removed from 9.0 million computers during that period.

[3] The Shadowserver Foundation, which tracks active Win32/Conficker infections, reported that 4.6 million Conficker-infected computers were being tracked by Shadowserver-operated sinkholes on the last day of 2H09, down from 5.2 million on the last day of 1H09. Counting the amount of malware found and cleaned by anti-malware software can sometimes yield figures that are very different from estimates produced through observations of active infected comptuers, and there is no widespread agreement about which method is preferable.

- Many attackers use Trojan downloaders and Trojan droppers, such as Win32/Renos and ASX/Wimad (the second and eleventh most prevalent families in 2H09, respectively) to distribute other threats, such as botnets, rogues, and password stealers, to computers.

- In general, the malware landscape in 2H09 is marked by a greater diversity of moderately prevalent families, with fewer single families dominating the top of the list with very large numbers of removals. The rapid adoption of Microsoft Security Essentials may also be partially responsible for the decline in removals.

Trends in Sample Proliferation

Malware authors attempt to evade detection by continually releasing new variants in an effort to outpace the release of new signatures by antivirus vendors. One way to determine which families and categories of malware are currently most active is to count unique samples.

Figure 7: Unique samples submitted to the MMPC by category, 1H09–2H09

Category	2H09	1H09	Difference
Viruses	71,991,221	68,008,496	5.9% ▲
Miscellaneous Trojans	26,881,574	23,474,539	14.5% ▲
Trojan Downloaders & Droppers	9,107,556	6,251,286	45.7% ▲
Misc. Potentially Unwanted Software	4,674,336	2,753,008	69.8% ▲
Adware	3,492,743	3,402,224	2.7% ▲
Exploits	3,341,427	1,311,250	154.8% ▲
Worms	3,006,966	2,707,560	11.1% ▲
Password Stealers & Monitoring Tools	2,217,902	7,087,141	-68.7% ▼
Backdoors	812,256	589,747	37.7% ▲
Spyware	678,273	269,556	151.6% ▲
Total	**126,204,254**	**115,854,807**	**8.9%**

- More than 126 million malicious samples were detected in the wild in 2H09.
- The decrease in the Password Stealers & Monitoring Tools category was primarily caused by Win32/Lolyda, which declined from 5.7 million samples in 1H09 to less than 100,000 in 2H09.
- The increase in the Spyware category was primarily caused by Win32/ShopAtHome, which had nearly five times as many unique samples in 2H09 as in the prior period.
- The large number of virus samples is caused by the fact that viruses can infect many different files, each of which is a unique sample. Sample counts for viruses should therefore not be considered an indication of large numbers of true variants for these families.

Rogue Security Software

Rogue security software—software that displays false or misleading alerts about infections or vulnerabilities on the victim's computer and offers to fix the supposed problems for a price—has become one of the most common methods that attackers use to swindle money from victims.

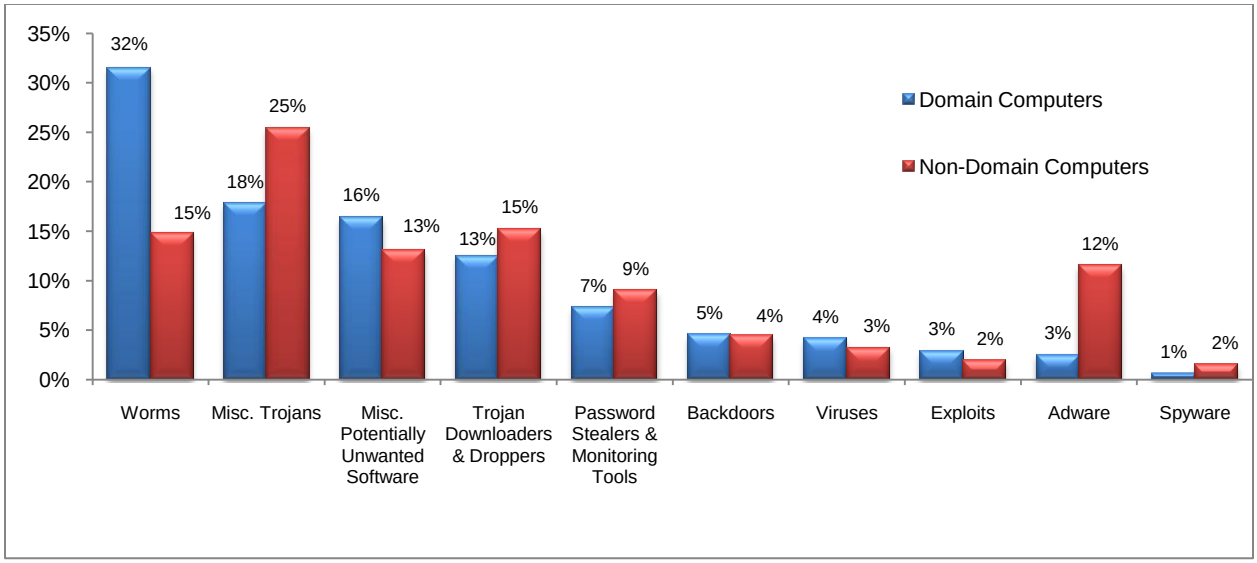
Figure 8: Fake "security scans" from variants of Win32/FakeXPA, the most prevalent rogue security software family in 2H09

- Microsoft security products cleaned rogue security software–related malware on 7.8 million computers in 2H09, up from 5.3 million computers in 1H09—an increase of 46.5 percent, which suggests that rogue security software provides its distributors with large payoffs relative to some other, less prevalent kinds of threats.
- A rogue security software family, Win32/FakeXPA, was the third most prevalent threat detected by Microsoft desktop security products worldwide in 2H09. Three others—Win32/Yektel, Win32/Fakespypro, and Win32/Winwebsec—ranked eleventh, fourteenth, and seventeenth, respectively.
- A full geographic breakdown of where Microsoft finds the most rogue security software and the top families of these threats in each region is available in the full *SIR*.
- Three new consumer-oriented videos have been posted on http://www.microsoft.com/protect that are designed to educate consumers about the increasing threat to their security and privacy from rogue security software.

The Threat Landscape at Home versus the Enterprise

The infection data produced by Microsoft desktop anti-malware products and tools includes information about whether the infected computer belongs to an Active Directory® Domain Services domain. Domains are used almost exclusively in enterprise environments, and computers that do not belong to a domain are more likely to be used at home or in other non-enterprise contexts. Comparing the threats that are encountered by domain computers and non-domain computers can provide insights into the different ways attackers target enterprise and home users and which threats are more likely to succeed in each environment.

Figure 9: Threat category breakdown for domain-joined and non-domain computers in 2H09



- Domain-joined computers were much more likely to encounter worms than non-domain computers, primarily because of the way worms propagate. Worms typically spread most effectively via unsecured file shares and removable storage volumes, both of which are often plentiful in enterprise environments and less common in homes.
  - Worms accounted for four of the top 10 families detected on domain-joined computers.
  - Win32/Conficker, which uses several methods of propagation that work more effectively within a typical enterprise network environment than over the public Internet, leads the list by a wide margin.
  - Similarly, Win32/Autorun, which targets removable drives, was more common in domain environments where such volumes are often used to exchange files.
- In contrast, the Adware and Miscellaneous Trojans categories are much more common on non-domain computers.

E-mail Threats

The data in this section is based on e-mail filtered by Microsoft Forefront Online Protection for Exchange (FOPE), which provides spam, phishing, and malware filtering services for thousands of enterprise customers.

Spam messages associated with advance-fee fraud (so-called “419 scams”) and gambling increased significantly in 2H09. Most other categories remained relatively stable in percentage terms.

- An advance-fee fraud is a common confidence trick in which the sender of a message claims to have a claim on a large sum of money but is unable to access it directly for some reason. Typically, the specified reason involves bureaucratic red tape or political corruption. The sender asks the prospective victim for a temporary loan that the sender will use to bribe officials or pay fees to get the full sum released. In exchange, the sender promises the target a share of the fortune, which amounts to a much larger sum than the original loan.
- These messages are often associated with Nigeria (“419” refers to the article of the Nigerian Criminal Code that deals with fraud) and other countries in western Africa, including Sierra Leone, the Côte d'Ivoire, and Burkina Faso.

Figure 10: Inbound messages blocked by FOPE content filters, by category, 2H08–2H09

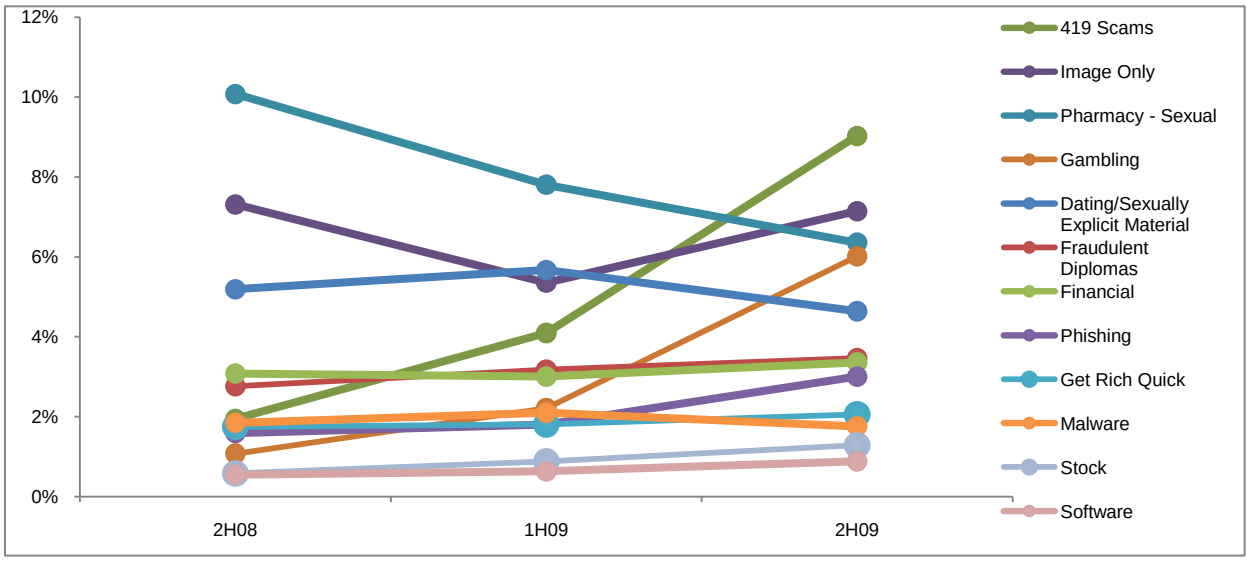
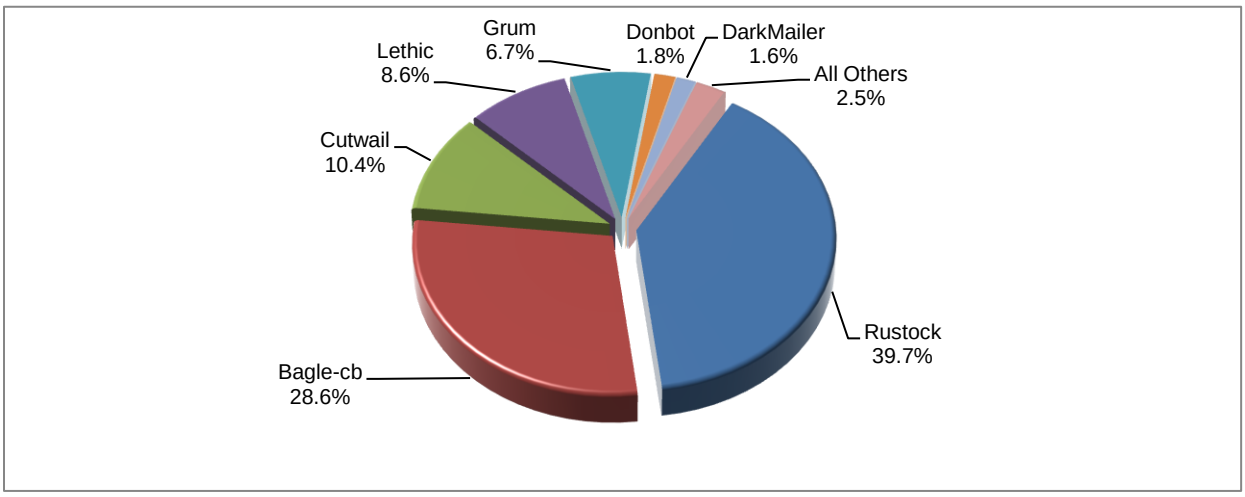


Figure 11: Top 5 locations that send the most spam, by percentage of all spam sent, in 2H09

	Country	Percent
1	United States	27.0%
2	Korea	6.9%
3	China	6.1%
4	Brazil	5.8%
5	Russia	2.9%

Botnets and spam networks of malware-infected computers that can be controlled remotely by an attacker are responsible for much or most of the spam that is sent today. To measure the impact that botnets have on the spam landscape, FOPE monitors spam messages sent from IP addresses that have been reported to be associated with known botnets.

Figure 12: A few botnets are responsible for sending almost all of the botnet spam observed in 2H09 (the full *SIR* includes more details)



Malicious Web Sites

As published in previous volumes of the SIR, social networking properties suffered the highest total volume of phishing impressions as well as the highest rate of phishing impressions per phishing site. Financial institutions received the lowest volume of phishing impressions per site though by far the highest total volume of distinct fraudulent sites. The following figure shows the percentage of phishing impressions recorded by Microsoft each month in 2H09 for each of the most frequently targeted types of institutions.

Figure 13: Left: Impressions for each type of phishing site each month in 2H09 Right: Active phishing sites tracked each month, by type of target, in 2H09

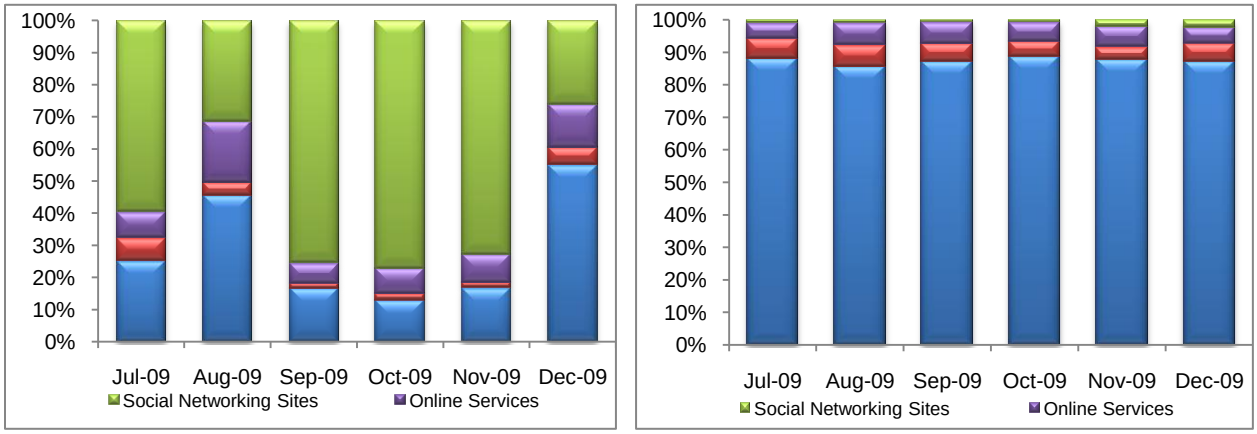
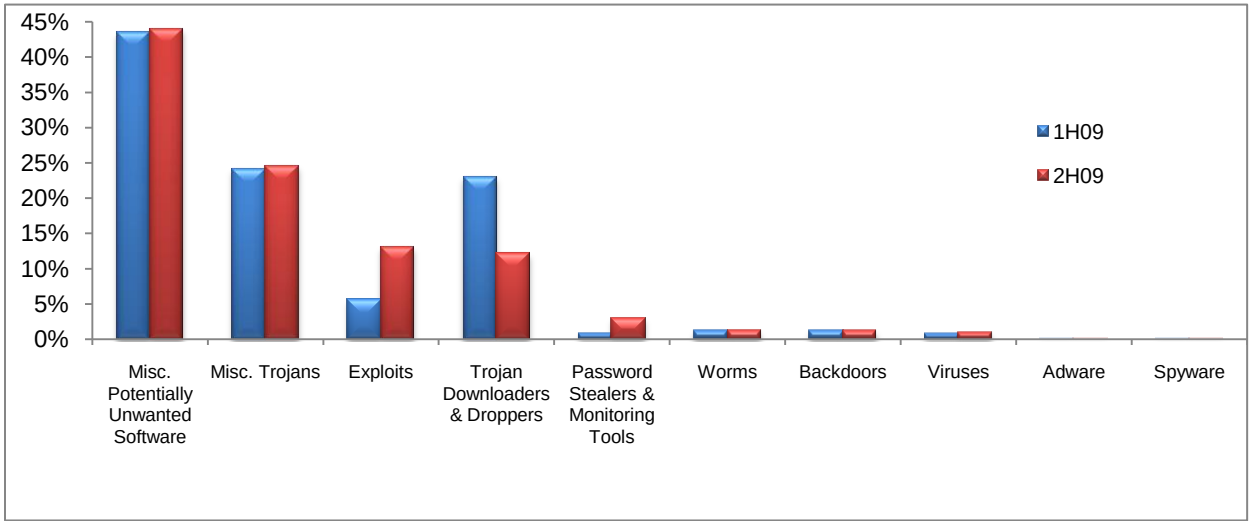


Figure 14: The category breakdown for threats hosted at URLs blocked by the SmartScreen Filter in 1H09 and 2H09



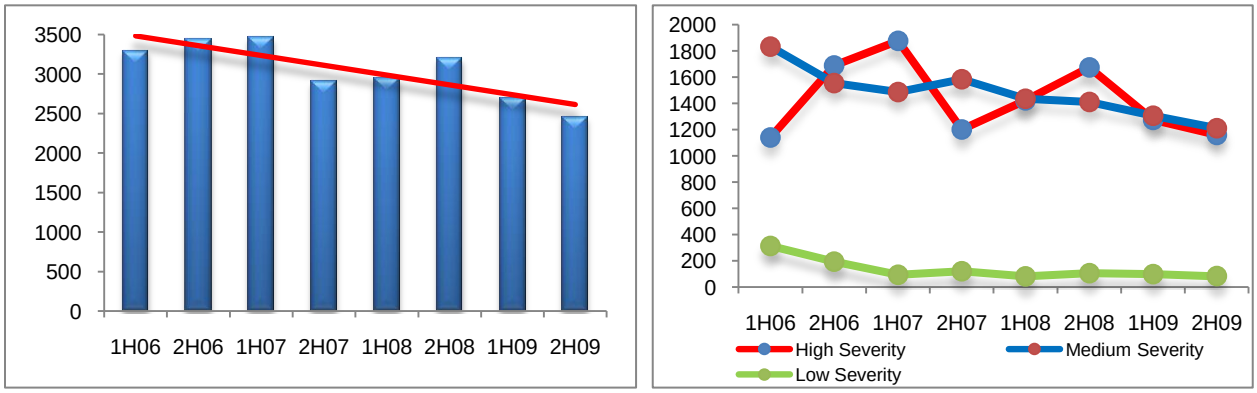
- The Miscellaneous Potentially Unwanted Software and Miscellaneous Trojans categories dominated the list in both periods.
- The Trojan Downloaders & Droppers category, which was nearly as prevalent as Miscellaneous Trojans in 1H09, fell by nearly 50 percent in the second half of the year, while Exploits more than doubled.

Key Findings from the Microsoft Security Response Center

Industry-Wide Vulnerability Disclosures

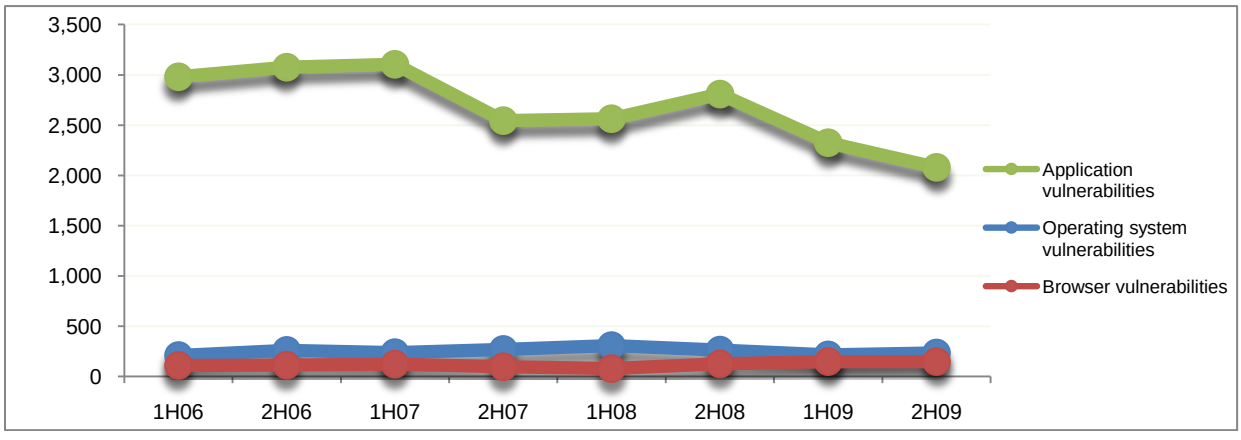
Vulnerabilities are weaknesses in software that allow an attacker to compromise the integrity, availability, or confidentiality of that software. Some of the worst vulnerabilities allow attackers to run arbitrary code on the compromised computer. A disclosure, as the term is used in this report, is the revelation of a software vulnerability to the public at large. It does not refer to any type of private disclosure or disclosure to a limited number of people.

Figure 15: Left: Industry-wide vulnerability disclosures by half-year, 1H06–2H09 | Right: Industry-wide vulnerability disclosures by severity, 1H06–2H09



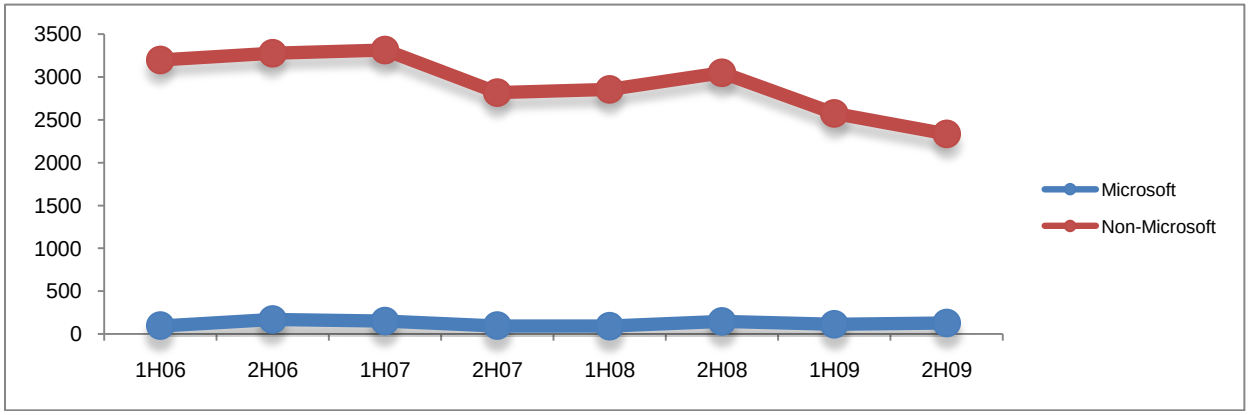
- Vulnerability disclosures in 2H09 were down 8.4 percent from the first half of the year, which continues an overall trend of moderate declines since 2006.
- Low severity vulnerabilities accounted for just 3.5 percent of overall vulnerabilities in 2H09, down from 4.1 percent in the first half of the year.
- High severity vulnerabilities disclosed in 2H09 were down 9.0 percent from the first half of the year, and 30.7 percent from 2H08.
    - The continued predominance of High severity and Medium severity vulnerability disclosures is likely caused at least in part to the tendency of both attackers and legitimate security researchers to prioritize searching for the most severe vulnerabilities.

Figure 16: Industry-wide operating system, browser, and application vulnerabilities, 1H06–2H09



- Application vulnerabilities continued to account for most vulnerabilities in 2H09, although the total number of application vulnerabilities was down significantly from 2H08 and 1H09.
- Operating system and browser vulnerabilities were both roughly stable, and each accounted for a small fraction of the total.

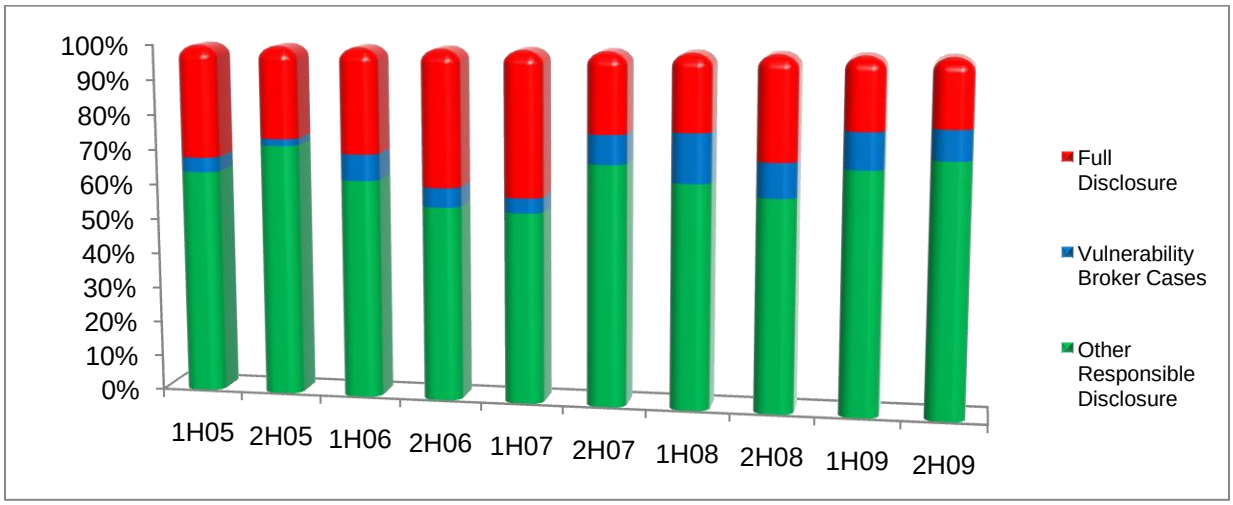
Figure 17: Vulnerability disclosures for Microsoft and non-Microsoft products, 1H06–2H09



- Vulnerability disclosures for Microsoft products increased to 127 in 2H09 from 113 in 1H09.
- Generally, trends for Microsoft vulnerability disclosures mirrored those for the entire industry, with peaks in 2H06-1H07 and again in 2H08.
- Over the past four years, Microsoft vulnerability disclosures have consistently accounted for 3 to 5 percent of all disclosures industry wide.

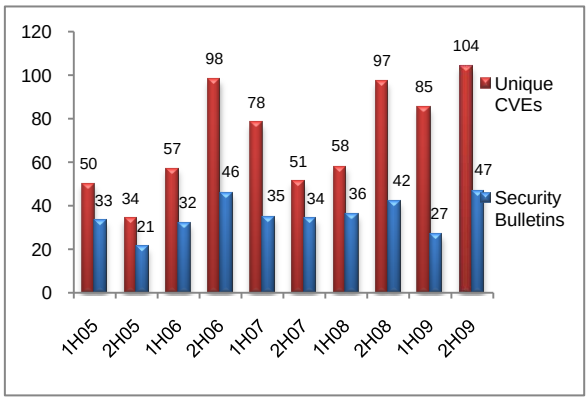
Responsible disclosure means disclosing vulnerabilities privately to an affected vendor so it can develop a comprehensive security update to address the vulnerabilities before the details become public knowledge.

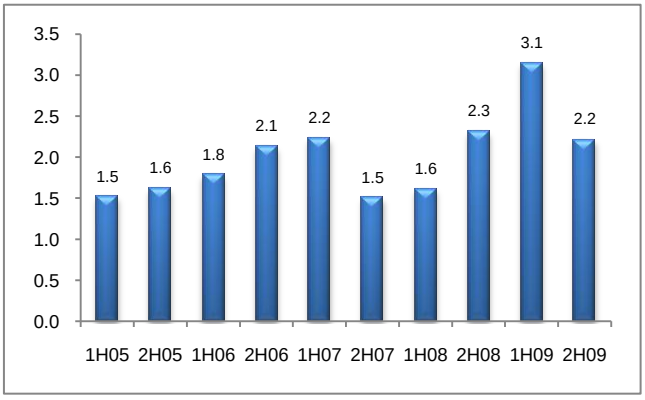
Figure 18: Responsible disclosures as a percentage of all disclosures involving Microsoft software, 1H05–2H09



- In 2H09, 80.7 percent of Microsoft vulnerability disclosures adhered to responsible disclosure practices, up from 79.5 percent in 1H09 and higher than in any previous tracked period.
- The percentage of disclosures submitted by vulnerability brokers declined slightly to 8.6 percent of all disclosures in 2H09, compared to 10.5 percent in the first half of the year.

Figure 19: Left: Security bulletins released and CVEs addressed by Microsoft by half-year, 1H05–2H09 | Right: Average number of CVEs addressed per security bulletin, 1H05–2H09

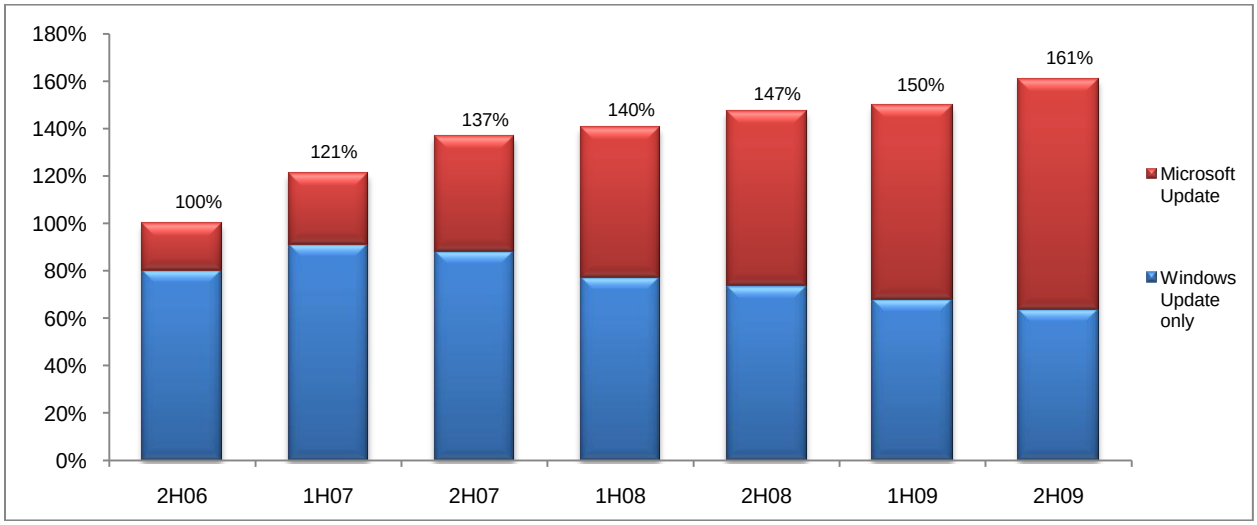




- In 2H09, Microsoft released 47 security bulletins that addressed 104 individual vulnerabilities that were identified on the Common Vulnerabilities and Exposures (CVE) list.
- Although the overall number of bulletins shipped increased from 27 in 1H09, the number of vulnerabilities addressed per bulletin decreased from 3.1 to 2.2

As the following figure shows, Microsoft Update adoption has increased significantly over the past several years. The number of computers using the more comprehensive service increased by more than 17 percent since 1H09.

Figure 20: Usage of Windows Update and Microsoft Update, 2H06–2H09, indexed to 2H06 total usage



- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft anti-malware products and the monthly release of the MSRT.
- **Microsoft Update** (http://update.microsoft.com/microsoftupdate) provides all of the updates offered through Windows Update and provides updates for other Microsoft software. Users can opt in to the service when installing software serviced through Microsoft Update or at the Microsoft Update Web site. Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

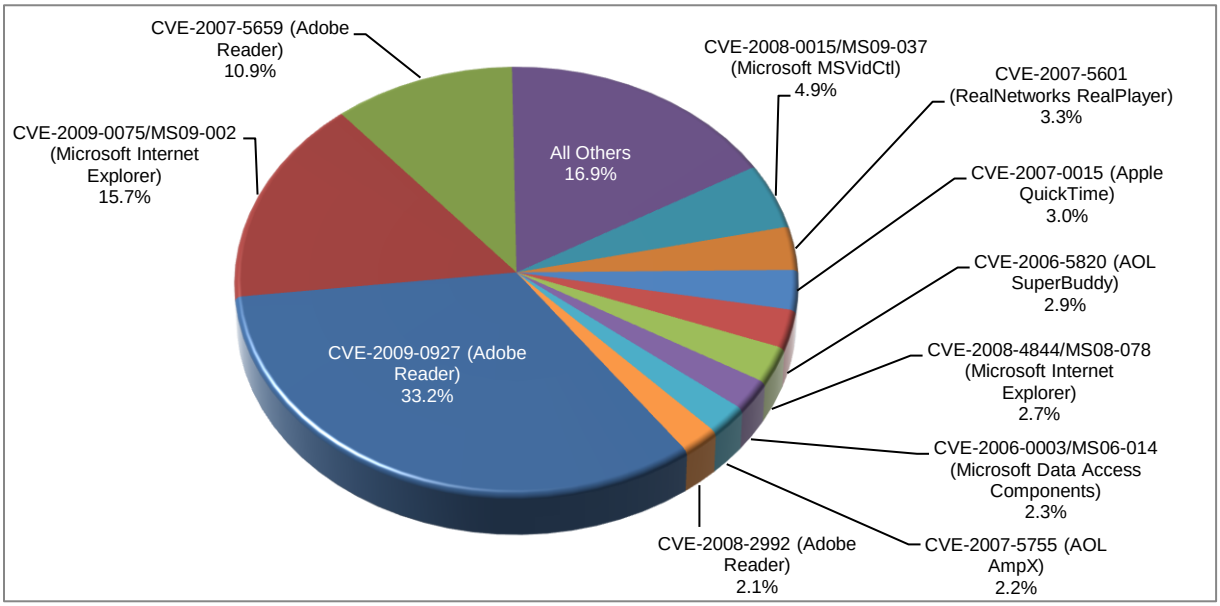
Key Findings from the Microsoft Security Engineering Center

Security Science: Exploit Trends

An *exploit* is malicious code that is designed to infect a computer without the user's consent and often without the user's knowledge. Exploits are often distributed through Web pages, although attackers also use a number of other distribution methods, such as e-mail and instant messaging (IM) services. Information about how attackers exploit browsers and add-ons can provide security researchers with a greater understanding of the risks that are caused by drive-by downloads and other browser–based attacks.

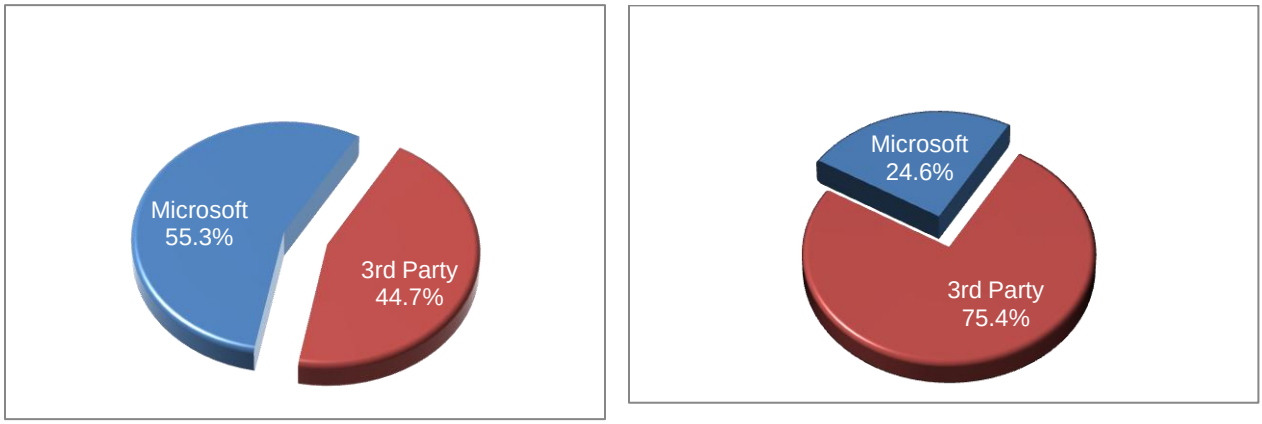
- In the past, exploit-kit makers tended to package four to six exploits together per kit to increase the chances of a successful attack.
  - This average dropped to 3.2 exploits per package in the first half of 2009 as attackers took advantage of a number of reliable and prevalent vulnerabilities in third-party components, which rendered large numbers of exploits unnecessary.
  - This trend continued into 2H09; the average number of exploits per package fell to 2.3.
  - However, some attackers still preferred to use large numbers of exploits—the largest exploit kit observed in 2H09 included 23 exploits.

Figure 21: Browser-based exploits encountered in 2H09, by percentage



- CVE-2007-0071, a Drive-by vulnerability in Adobe Flash Player that was the most commonly exploited browser vulnerability in 1H09, fell to twenty-third place in the second half of the year and accounted for just 0.4 percent of exploits.
  - Significant shifts such as these might be related to the tendency of exploit-kit creators to frequently replace older exploits with newer ones.
  - As the graph on the right in Figure 21 shows, the incidence of several of the most prevalent exploits varied significantly from month to month in 2H09.
- One listed vulnerability in Figure 21 received a patch in 2006
- All vulnerabilities covered in Figure 21 had security updates available prior to the SIR reporting period.

Figure 22:Left: Browser-based exploits that targeted Microsoft and third-party software on Windows XP–based computers in 2H09 | Right: Browser-based exploits that targeted Microsoft and third-party software on Windows Vista and Windows 7–based computers in 2H09



- Comparing exploits that target Microsoft software to third-party exploits (those that target vulnerabilities in software produced by other vendors) suggests that the vulnerability landscape of Windows Vista and Windows 7 is very different from that of Windows XP.
  - In Windows XP, Microsoft vulnerabilities account for 55.3 percent of all attacks in the studied sample.
  - In Windows Vista and Windows 7, the proportion of Microsoft vulnerabilities is significantly smaller, accounting for just 24.6 percent of attacks in the studied sample.
    - This is up from 15.5 percent in 1H09 (includes Windows Vista only) because of increased attacks on CVE-2009-0075/MS09-002, a vulnerability in Internet Explorer 7 that affects Windows Vista RTM and SP1 (but not Windows Vista SP2 or Windows 7). For which was addressed by Microsoft security update in January 2009.

Figures 23 and Figure 24 on the following page show the 10 vulnerabilities exploited most often in Windows XP (Figure 23) and in Windows Vista and Windows 7 (Figure 24).

Figure 23: The 10 browser-based vulnerabilities exploited most often on Windows XP–based, by percentage of all exploits, in 2H09

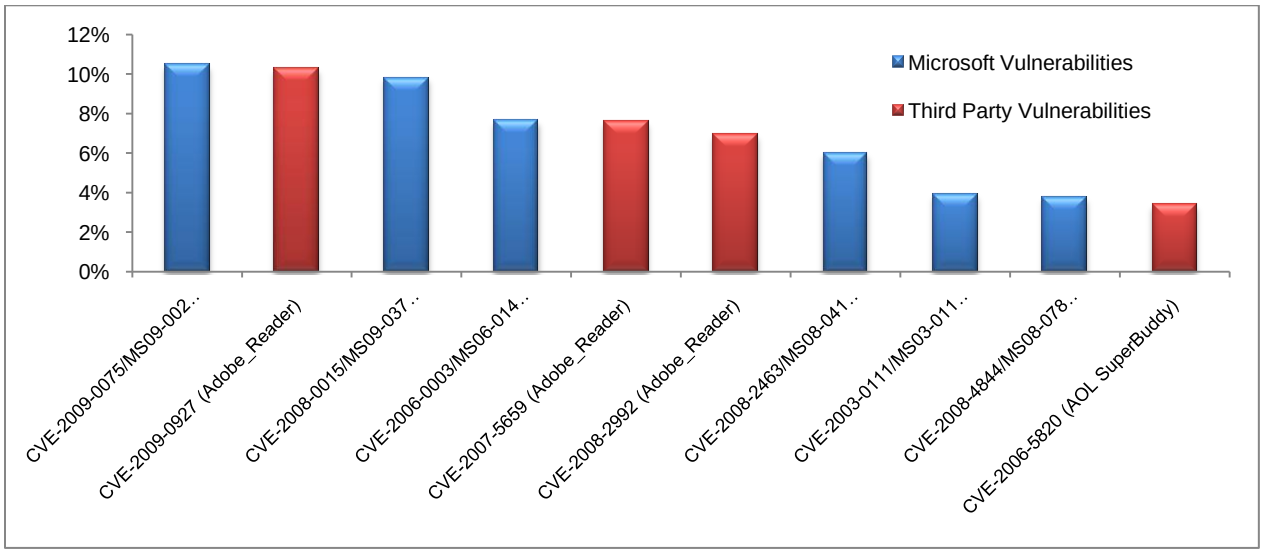
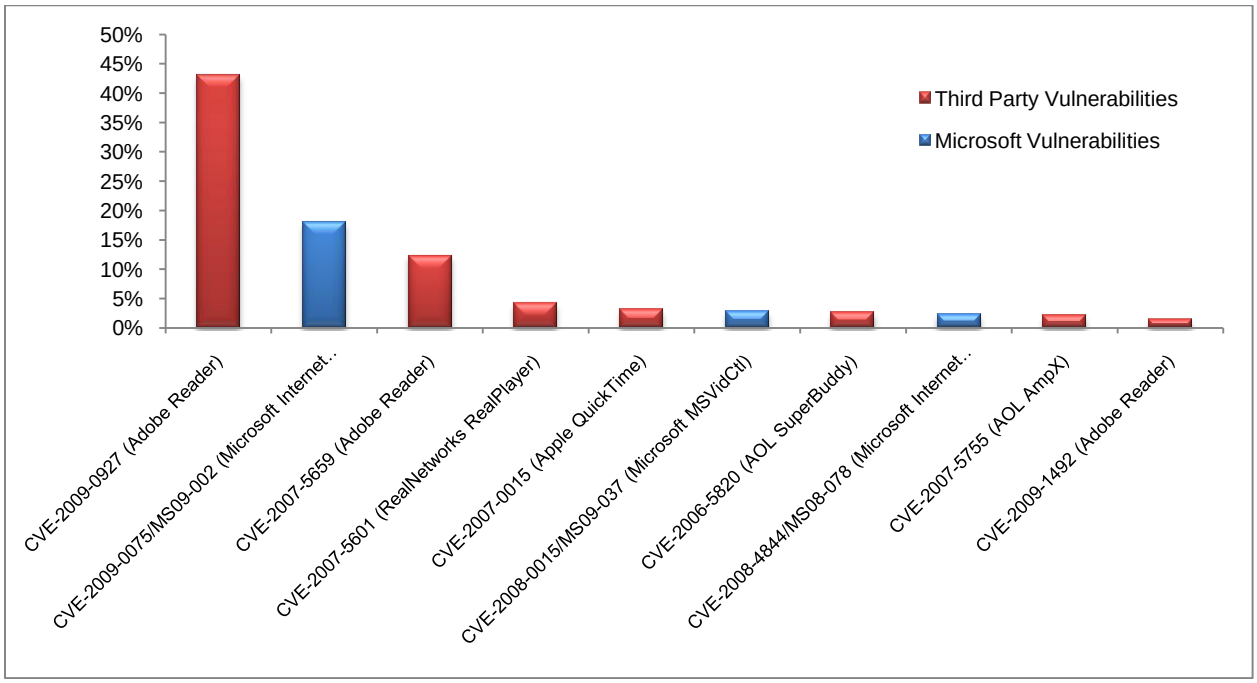


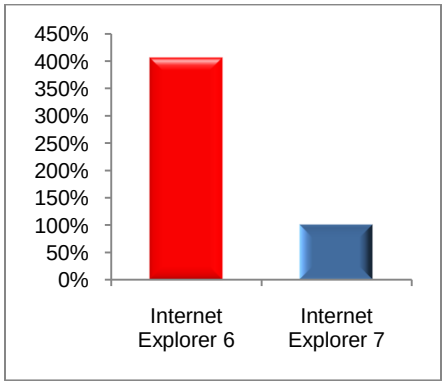
Figure 24: The 10 browser-based vulnerabilities exploited most often on Windows Vista and Windows 7–based, by percentage of all exploits, in 2H09



Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or when they post malicious code to a poorly secured Web form, like a comment field on a blog.

- An analysis of the specific vulnerabilities targeted by drive-by download sites indicates that most exploits used by such malicious sites target older browsers and are ineffective against newer ones. As the following figure illustrates, exploits that affect Internet Explorer 6 appeared on more than four times as many drive-by sites in 2H09 as did exploits that affect the newer Internet Explorer 7.

Figure 25: Drive-by download sites that targeted Internet Explorer 6 and Internet Explorer 7, indexed to the total for Internet Explorer 7, in 2H09

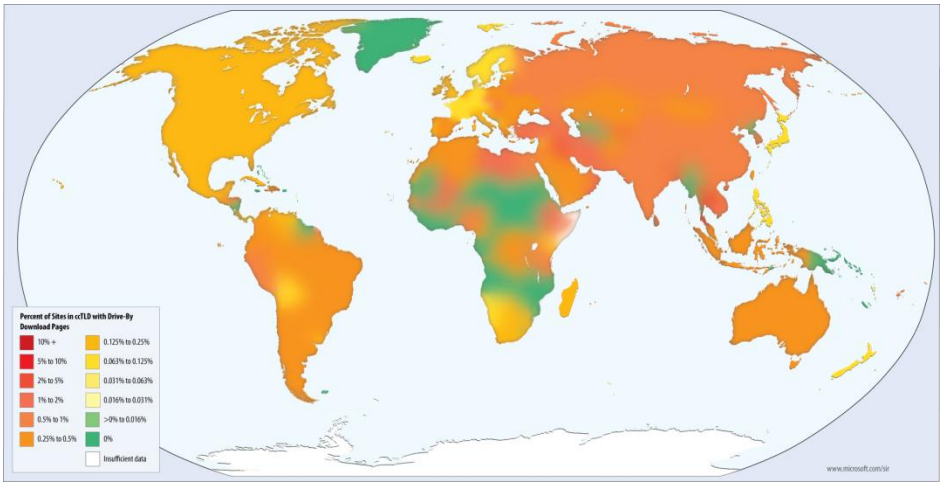


- As Bing indexes the Web, pages are assessed for malicious elements or malicious behavior.

- Bing detects a large number of drive-by download pages each month, with several hundred thousand sites that host active drive-by pages being tracked at any given time.
- Because the owners of compromised sites are usually victims themselves, the sites are not removed from the Bing index. Instead, clicking the link in the list of search results displays a prominent warning, saying that the page might contain malicious software.
  - In 2H09, about 0.3 percent of the search results pages served to users by Bing contained warnings about malicious sites.
- Overall, the number of affected Web sites tracked by Bing increased in 2H09, with 0.24 percent of all Web sites that host at least one malicious page, up from 0.16 percent in 1H09. This increase is probably due in part to a number of new, improved detection mechanisms that Bing deployed in the second half of 2009.

- Although Bing has detected drive-by download sites all over the world, the risk is not spread equally among Internet users worldwide. Users in some parts of the world are more at risk than in others. The following figure shows the portion of Web sites in each country-code top-level domain (ccTLD) that were found to host drive-by download pages in 2H09.
  - Drive-by download pages were discovered on more than 2.1 percent of the sites in the .th ccTLD (associated with Thailand) and almost 1 percent in the .cn ccTLD (China).

Figure26: [BingGeo_Heatmap] Percentage of Web sites in each country-code top-level domain (ccTLD) that hosted drive-by download pages in 2H09

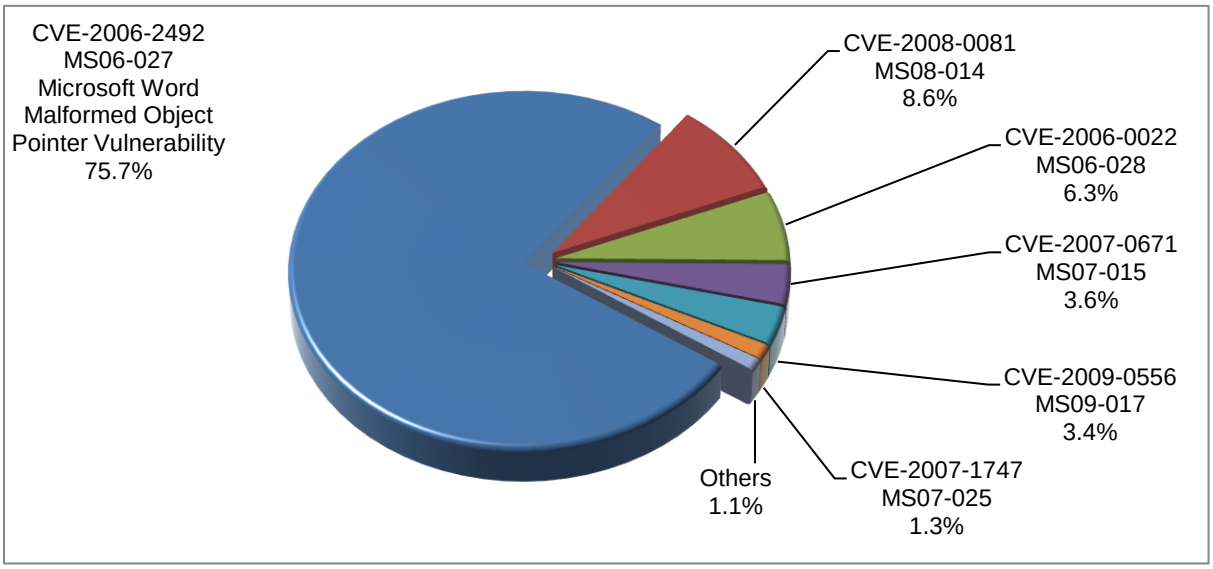


- By comparison, generic and sponsored top-level domains that do not serve particular countries/regions do not display the same level of variance that ccTLDs do.
  - The .biz TLD, which is intended for businesses, contains the highest percentage of sites that host drive-by download pages; 0.76 percent of all active .biz sites were found to contain such pages.
- Although drive-by download pages can be found in quantity in most generic, sponsored, and country-code TLDs, exploit servers are concentrated in a much smaller number of TLDs, led by .com (33.2 percent) and .cn (19.0 percent).
  - In 2H08, the most heavily used exploit server in the world had a reach of about 100,000 pages. This increased to more than 450,000 pages in 1H09, and to nearly 750,000 pages in 2H09.
    - Despite this increase, very few of the servers at the top of the list in 1H09 remain there in 2H09.
- Malware distribution networks tend to be moving targets, with servers that constantly appear and disappear in different locations.

Attackers increasingly use common file formats as transmission vectors for exploits (formats like .doc, .pdf, .ppt, and .xls for example). *Parser vulnerabilities* are a class of vulnerability in which the attacker creates a specially crafted document that takes advantage of an error in how the code processes or parses the file format. Many of

these formats are complex and designed for performance, and an attacker can create a file with a malformed section that exploits vulnerability in the program.

Figure27: Microsoft Office file format exploits encountered, by percentage, in 2H09



- Most of the vulnerabilities exploited in the data sample were several years old and all of them had security updates available to help protect against exploitation; a third of them were first identified in 2006.
- 75.7 percent of the attacks exploited a single vulnerability (CVE-2006-2492, the Malformed Object Pointer Vulnerability in Microsoft Office Word) for which a security fix had been available for more than three years by the end of 2009.
- Users who do not keep their Office program installations up to date with service packs and security updates are at increased risk of attack. Most attacks involved computers with severely out-of- date Office program installations.
  - More than half (56.2 percent) of the attacks affected Office program installations that had not been updated since 2003.
  - Most of these attacks involved 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.
  - It is not at all uncommon for victims of Office program exploit attacks to have Windows installations that are much more current. Almost two-thirds (62.7 percent) of the Office attacks observed in 2H09 affected computers that run versions of Windows that had been updated within the previous 12 months.
  - The median amount of time since the last operating system update for computers in the sample was about 8.5 months, compared to 6.1 years for the most recent Office program update—almost nine times as long.
    - This data helps illustrate the fact that users can keep Windows rigorously up to date and still face increased risk from exploits unless they also update their other programs regularly.

Security Breach Trends

Security Incidents that Led to Privacy Consequences

Over the last few years, laws have been passed in a number of jurisdictions around the world requiring that affected individuals be notified when an organization loses control of personally identifiable information (PII) with

which it has been entrusted. These mandatory notifications offer unique insights into how information security efforts need to address issues of negligence as well as technology4.

Figure28:Breach incidents that result from attacks and negligence, 1H08–2H09

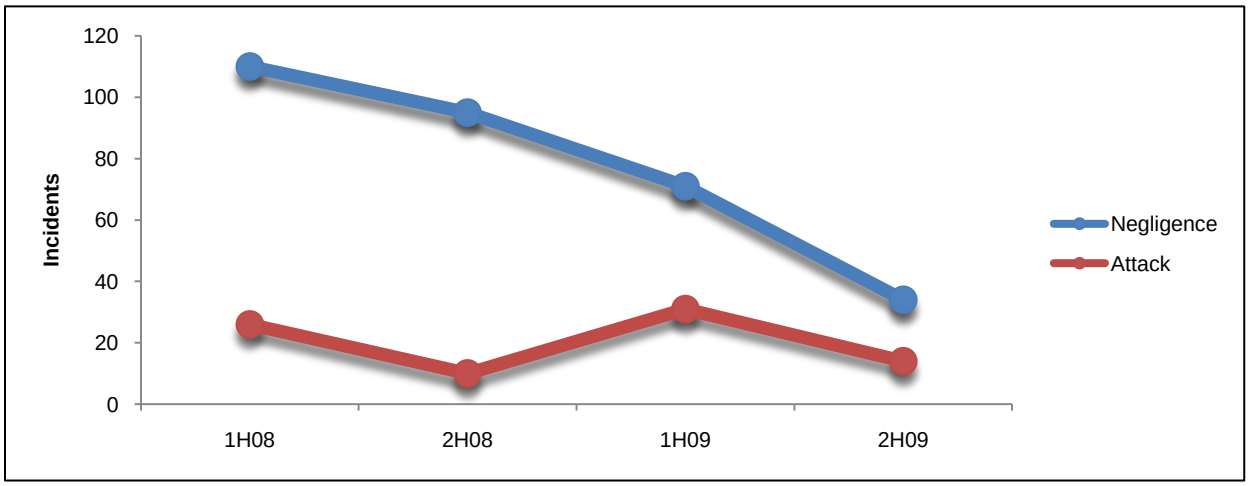
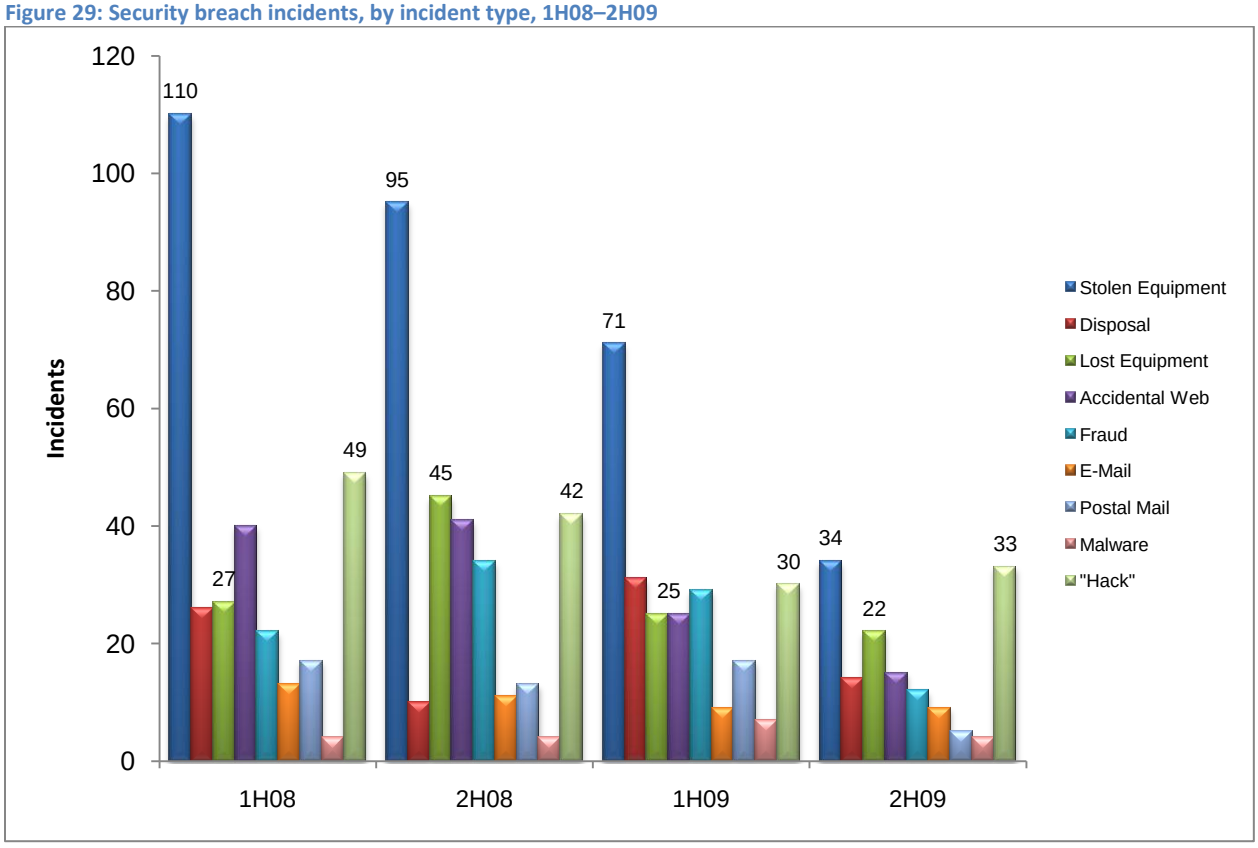


Figure 29: Security breach incidents, by incident type, 1H08–2H09



[4] Since 2005, volunteer security researchers have tracked worldwide reports of such data security breaches and recorded them in the Data Loss Database (DataLossDB) at http://datalossdb.org

- There is a clear downward trend in the absolute number of incidents in every single category except for malware attacks, which remains unchanged.
- Stolen equipment and media and accidental Web loss account for the largest declines.
- Improper disposal of business records accounts for quite a few incidents. Organizations can address this type of data breach relatively easily with effective policies regarding the destruction of paper and electronic records that contain sensitive information.
- Although many people link security breaches with malicious parties who seek and gain unlawful access to sensitive data, incidents that involve attacks (hacking, malware, and fraud) have been significantly outnumbered in recent years by incidents that involve negligence (lost, stolen, or missing equipment; accidental disclosure; or improper disposal).
- Incidents that involve negligence have declined steeply over the past two years, from 110 in 1H08 to just 34 in 2H09.
    - Organizations might be taking more steps to secure sensitive equipment, such as security checks at facility gates or programs to educate employees about secure practices.
    - Adoption of strong encryption solutions such as Windows BitLocker® Drive Encryption might also affect the decline. Disclosure laws in many jurisdictions do not require notification when encrypted data is lost or stolen because it is much more difficult for the thief or finder to extract than unencrypted data.

Mitigation Strategies

How Microsoft IT Manages Risk at Microsoft

Microsoft IT is responsible for day-to-day operations and security for the global network at Microsoft. In this new section of the SIR, Microsoft IT shares many of the specific mitigation strategies they use to manage risk in this highly complex environment, and provides practical guidance that IT and security professionals can use to help secure their own environments. Topics discussed include various ways to help protect an organization's network infrastructure as well as how to promote awareness and safe computing behavior within the organization.

Microsoft has also produced extensive guidance for IT professionals to help manage the process of assessing, prioritizing and deploying security updates for Microsoft products. The Microsoft Security Update Guide is available as a free download from www.microsoft.com/securityupdateguide.

The full *SIR* also contains mitigation strategies and best practice information to help organizations mitigate many of the security risks that are identified in the *SIR*.

The full *SIR* can be downloaded from www.microsoft.com/sir.

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