Microsoft
Security Intelligence Report

July–December 2006

An in-depth perspective of software vulnerabilities, malicious code threats, and potentially unwanted software, focusing on the second half of 2006

Microsoft®

Microsoft Security Intelligence Report

Authors

Vinny Gullotto
Microsoft Security Research & Response

Jeff Jones
Trustworthy Computing

Mary Landesman
Microsoft Security Research & Response

Ziv Mador
Microsoft Security Research & Response

George Stathakopoulos
Microsoft Security Response Center

Jeff Williams
Microsoft Security Research & Response

Contributors

Chuck Bassett
Microsoft Forefront Client Security

Dave Berkowitz
Trustworthy Computing

Subratam Biswas
Microsoft Security Research & Response

Daniel Bohm
Exchange Hosted Services (EHS)

Matthew Braverman
Microsoft Security Research & Response

Christopher Budd
Trustworthy Computing

Alexandru Carp
Microsoft Security Research & Response

Doug Cavit
Trustworthy Computing

Brendan Foley
Microsoft Security and Access Product Marketing

Jason Garms
Windows Engineering

Jason Geffner
Microsoft Security Research & Response

Kjersti Gunderson
Waggener Edstrom

Jim Hahn
Windows Client

Brett Harris
Microsoft Security Research & Response

Richard Harrison
Content Master

Rob Hensing
Microsoft Security Technology Unit

Yuhui Huang
Microsoft Security Research & Response

Aaron Hulett
Microsoft Security Research & Response

Jonathan Keller
Microsoft Security Research & Response

David Kennedy
Microsoft Legal and Corporate Affairs

Jimmy Kuo
Microsoft Security Research & Response

Mady Marinescu
Microsoft Security Research & Response

Charles McColgan
Exchange Hosted Services (EHS)

Mark Miller
Trustworthy Computing

Michael Mitchell
Microsoft Legal and Corporate Affairs

Gina Narkunas
Microsoft Online Services Group

Adam Overton
Microsoft Security Research & Response

Tim Rains
Trustworthy Computing

Bo Rohlfsen
Windows Live OneCare

Stephen Toulouse
Trustworthy Computing

Pat Winkler
Microsoft Security Research & Response

Jaime Wong
Microsoft Security Research & Response

Table of Contents

About This Report

Scope

The last Security Intelligence Report published by Microsoft® focused on data and trends observed in the first half of 2006 specific to malicious software or potentially unwanted software. That report can be found at http://go.microsoft.com/?linkid=6543860.

We continue to focus on malicious software data and trends in this report, but we have also expanded the scope of the report to include data and trends for software vulnerabilities.

Note On November 30, 2006, Windows Vista™ was made available to business customers with volume license agreements. Windows Vista became generally available on January 30, 2007. Although this report does make reference to Windows Vista, a full analysis of relevant data from Windows Vista will be included in a future version of this report.

Reporting Period

This Security Intelligence Report contains data and trends observed over the past several years, but focuses on the second half of 2006 [2H06]. The nomenclature used throughout the report to refer to different reporting periods is *n*HYY, where *n*H refers to either the first (1) or second (2) half of the year, and YY denotes the year. For example, 1H06 represents the period covering the first half of 2006 (January 1 through June 30), while 2H05 represents the period covering the second half of 2005 (July 1 through December 31).

Data Sources

Software Vulnerabilities

The efforts to identify and fix vulnerabilities lacked a common naming mechanism until a consortium led by The Mitre Corporation began publishing the Common Vulnerabilities and Exposure (CVE) list, which drives a common naming mechanism that can be leveraged by multiple vulnerability databases and security products. The CVE naming conventions provide the most comprehensive list of vulnerabilities worldwide, across software products of all types. This report uses the CVE naming conventions when identifying individual vulnerabilities.

The analysis in this report uses a set of data that has been created by compiling, customizing, and cross-checking several sources of data available on the Internet:

- **Common Vulnerabilities and Exposures Web site (http://cve.mitre.org).** A large portion of the data analyzed originates from the CVE list maintained at this site, which is currently sponsored by the United States Department of Homeland Security (DHS). The naming mechanisms and external references to sources for additional information were particularly valuable.
- **National Vulnerability Database (NVD) Web site (http://nvd.nist.gov/).** This database superset of the CVE list, which provides additional objective information concerning vulnerabilities, was the source used to determine severity ratings and to exploit complexity assessment. The NVD is also sponsored by the United States DHS, and their data is downloadable in an XML format at http://nvd.nist.gov/download.cfm.
- **Security Web sites.** The following sites, as well as many others, were utilized for detailed verification and validation of vulnerability specifics:
  - http://www.securityfocus.com
  - http://www.securityfocus.com/archive/1 (Bugtraq mailing list)
  - http://www.secunia.com
  - http://www.securitytracker.com
- **Vendor Web sites and support sites.** The following sites, as well as others, were utilized for confirmation and validation of vulnerability details:
  - https://rhn.redhat.com/errata
  - http://support.novell.com/linux/psdb
  - http://sunsolve.sun.com
  - http://www.microsoft.com/technet/security/current.aspx
  - http://www.ubuntu.com/usn

By leveraging these sources, as well as many others, Microsoft has compiled a database of disclosure dates for vulnerabilities that can be used to determine the year, month, and day that each vulnerability was disclosed publicly and broadly for the first time.

Note that, in this report, “disclosure” is used to mean broad and public disclosure, and not any sort of private disclosure or disclosure to a limited number of people.

Malicious Software and Potentially Unwanted Software

Data from several customer-focused Microsoft security products and services, representing a total user base of several hundred million computers, was used to compile the trends and information provided in this report. Although most of the products mentioned in this report are aimed at individual users, this information is also applicable to business users. Figure 1 shows the five main data sources used in this report to compile data on the prevalence of malicious and potentially unwanted software.

The Windows® Malicious Software Removal Tool (MSRT) and Windows Defender are used as the main sources of information for this report. The two programs currently have the largest user bases of customer-focused Microsoft security products and services, and therefore provide the highest volume of malicious and potentially unwanted software prevalence data[1]. Windows Defender has more than 18 million active customers, where an active customer is defined as a computer retrieving new signatures at least once per week. The MSRT has been available since January 2005 and has a user base of more than 310 million unique computers. During 2H06, the tool was executed 1.8 billion times, bringing the total number of executions to 5.5 billion since January 2005.

Appendix A includes more information about the tools and services used as data sources for this report. It also includes information about additional business-focused Microsoft antimalware offerings, including Microsoft Forefront™ Security for Exchange Server and Microsoft Forefront Client Security.

Figure 1. *Data sources*

Product Name	Main Customer Segment		Malicious Software		Spyware and Potentially Unwanted Software		Available at No Additional Charge	Main Distribution Methods
	Consumers	Business	Scan and Remove	Real-time Protection	Scan and Remove	Real-time Protection		
Windows Malicious Software Removal Tool	●		Prevalent Malware Families				●	WU / AU, Download Center
Windows Defender	●				●	●	●	Download Center Windows Vista
Windows Live OneCare Safety Scanner	●		●		●		●	Web
Windows Live OneCare	●		●	●	●	●		Web / Store Purchase
Microsoft Exchange Hosted Filtering		●	●	●				Web

[1] Neither the MSRT nor Windows Defender intentionally collects personally identifiable information (PII). The Windows Defender privacy policy states that Windows Defender may unintentionally compile reports that contain personal information from file paths and partial memory dumps from users who have joined SpyNet as Advanced members. For more information on the type of data these products collect, see the Windows Defender privacy policy at http://www.microsoft.com/athome/security/spyware/software/privacypolicy.mspx and the MSRT online documentation at http://support.microsoft.com/kb/890830.

Executive Foreword

Five years ago, Microsoft made a commitment to dramatically shift the company's mission and strategy by infusing Trustworthy Computing (TwC) into everything we do—focusing on making our products and services more secure and reliable, protecting our customers' privacy, and being more transparent and responsive in our business practices.

Our first step was to increase the quality of our products. We put a lot of effort into understanding what "security assurance" truly means and applying this learning to our products. This resulted in one of our most important innovations—the Security Development Life Cycle (SDL). The SDL provides concrete, actionable steps that each member involved in the software development effort can use to understand, target, and measure the security of their product. The SDL and other engineering practices have greatly increased the security quality of our products, and as part of our commitment to the overall software ecosystem, we have started the process of sharing these tools with partners and the research community in general.

However, due to the complexity of contemporary software and ongoing vulnerability research, we must focus not only on finding and fixing specific security issues, but also on building in-depth defense mechanisms to improve our product resiliency. The Address Space Layout Randomization (ASLR) feature and Data Execution Prevention (NX) improvements that we built into Windows Vista are examples of such mechanisms, as they do not address specific coding issues, but do help make it more difficult to write automated attacks by making each Windows machine look different to an attacker.

We also continue to invest in security science to address classes of issues and raise the bar for creating exploits.

Our experience over the last five years has also taught us many things about how we share information. First and foremost, we have learned that transparency is the key to enabling our customers to respond to security issues in a proportionate and deliberate way. Transparency is also critical in our participation in the security research community, as it demonstrates our commitment to the shared goal of keeping customers truly protected. During this time, we've been proud to be part of the emerging security community, participating as a member, creating strong partnerships, and sharing our knowledge and continued innovation.

As part of our mission to provide transparency, this Security Intelligence Report contains our analysis of new security vulnerabilities disclosed during the 2006 calendar year. We also compare some trending information for vulnerabilities over the past several years, but with a particular focus on trends that might be emerging over the past 12 to 24 months. Our goal is to enable our customers to make the right decisions for their needs, based on accurate and trustworthy data.

As long as threats to our customers exist, we will stay vigilant and respond with our customers' best interests at heart. We will continue to improve our development processes, our products and services, our industry partnerships, and our response processes, in order to continue to meet our TwC vision.

Sincerely,

George Stathakopoulos
General Manager of Product Security
Microsoft Corporation

Executive Summary

This report provides an in-depth perspective of the software vulnerability, malicious software, and potentially unwanted software landscapes. The lists below summarize the key points from each section of the report.

Note On November 30, 2006, Microsoft Windows Vista was made available to business customers with volume license agreements. Windows Vista became generally available on January 30, 2007. Although this report does make reference to Windows Vista, a full analysis of relevant data from Windows Vista will be included in a future version of this report.

Software Vulnerabilities Highlights

- Disclosed vulnerabilities for 2006 rose 41 percent over the previous year, continuing an upward trend in new vulnerability disclosures. More vulnerabilities were disclosed in the second half of 2006 than in any single year from 2000 to 2004.
- December was the month with the most disclosures, with the week between Christmas and New Year's Day contributing the second-highest number of disclosures for the year.
- Over 90 percent of vulnerability disclosures occurred during the work week (between Monday and Friday). The most popular day of the week for new vulnerability disclosures was Tuesday.
- A much larger percentage of vulnerabilities were "complex to exploit" than in previous years, supporting the observation that the security researcher industry is maturing and utilizing better tools and techniques to find more complex issues.
- Application vulnerabilities continued to grow relative to operating system vulnerabilities as a percentage of all disclosures during 2006, supporting the observation that security vulnerability researchers may be focusing more on applications than in the past.

Malicious Software Highlights

- The number of malicious software variants remained steady throughout the second half of 2006; backdoor Trojans remained the most active type of malicious software, and bots remained the most active within that group. When viewed in terms of prevalence, however, bots and other backdoor Trojans continued to decline from 2H05 throughout 2H06. In computers in which the MSRT detected malicious software during that period, the rate decreased from 68 percent in 2H05 to 50 percent in 1H06 and to 43 percent in 2H06.
- The second half of 2006 also ushered in an increase in Trojan downloaders and droppers. One new and particularly active family was Win32/Stration, a family of Trojan downloaders and mass mailers that first gained momentum in September 2006.
- Over 3,700 distinct malicious WMF files that exploited the MS06-001 vulnerability were discovered during the second half of 2006. The continued prevalence of this kind of malicious file demonstrates that, despite the availability of a security update, attackers continually attempted to exploit this vulnerability. Most of the other exploits detected in Microsoft Office documents during this period were part of targeted attacks.
- During 2H06, the Trojan downloader's family Win32/Zlob became the most detected malware family by Microsoft Windows Live™ OneCare™, and is ranked number seven on the MSRT list.
- The likelihood of the MSRT finding malicious software on a Microsoft Windows XP computer without any service packs (SP) installed is 7.5 times higher than the likelihood of finding malicious software on a Windows XP SP2 computer. Additionally, the higher the level of service pack on a Windows computer, the less likely it is that the MSRT will find malicious software on that computer.
- MSRT has been an effective tool for removing malicious software from computers around the world. For 75 percent of those 12 families that are part of the tool, both in 1H06 and 2H06, the number of cleaned computers dropped by a range of 33 to 70 percent in 2H06 compared to 1H06.
- Exchange Hosted Services (EHS) blocked more infected mails in 2H06 compared to 1H06 (17-percent increase in the number of infected mails). During 2006, the number of scanned mails increased by 162 percent, which means that the percentage of infected mail actually went down.

Potentially Unwanted Software Highlights

- The standalone version of Windows Defender was released on October 23, 2006. This version of Windows Defender runs on Windows XP and Microsoft Windows Server™ 2003. Windows Defender is also a default component of the Windows Vista operating system.
- Detections by Windows Defender continue to increase. Adware remained the single largest category, based on volume, in 2H06 and was up 59.6 percent from 1H06, with a total of 16.7 million detections.
- The largest increases in detections were seen in the categories that represent the greatest impact to the privacy and security of the individual. For example, detections of remote control and monitoring software were up by 277 percent and 135 percent, respectively, from 1H06 to 2H06.
- The top 25 potentially unwanted software programs, ranked by the frequency the software is removed by Windows Defender, account for more than 56 percent of all removals in this period, in spite of there being thousands of families of potentially unwanted software that Windows Defender can detect and remove. This data tells us that a small number of parties are responsible for the majority of potentially unwanted software programs removed by Windows Defender customers.
- Overall, more than 38 million pieces of potentially unwanted software were detected by Windows Defender between July 1, 2006, and December 31, 2006.

Vulnerability Trends for 2006

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 security vulnerability researchers to run their code on the compromised system.

This section of the Microsoft Security Intelligence Report analyzes new vulnerabilities that were disclosed during the calendar year of 2006. It compares trending information for vulnerabilities starting from 2000, with a particular focus on trends that may be emerging over the past 12 to 24 months.

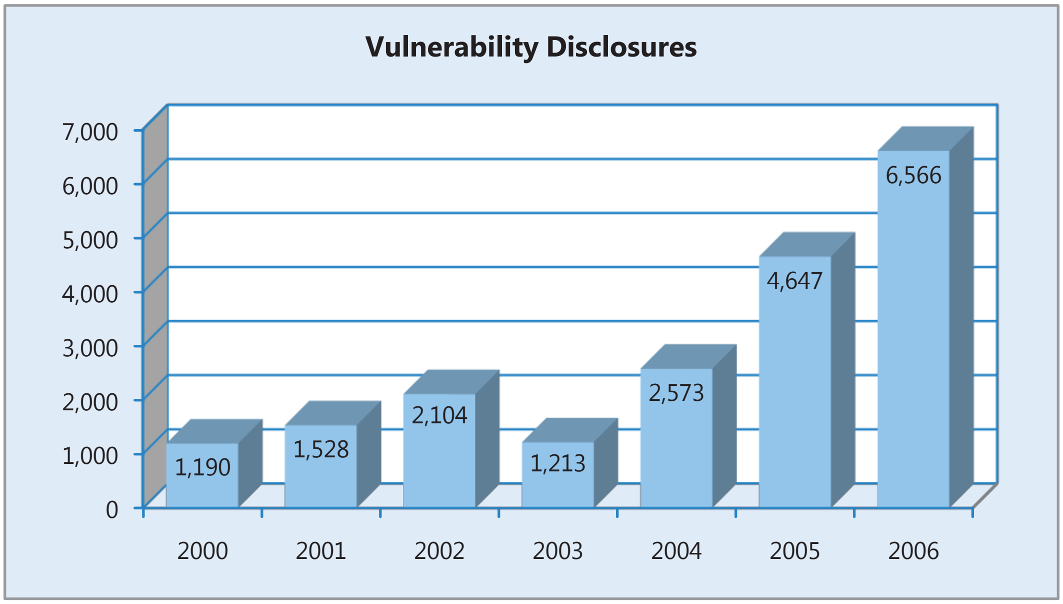
Note that, in this report, “disclosure” is used to mean broad and public disclosure, and not any sort of private disclosure or disclosure to a limited number of people.

Vulnerability Disclosures by Year

Reported vulnerabilities continue to rise in 2006. A total of 6,566 new vulnerabilities were disclosed to date, which is an increase of 41 percent from the previous year. In the last six months of 2006, the total number of vulnerabilities disclosed exceeded any full year's worth of vulnerability disclosures through 2004.

The annual vulnerability disclosures graphed in Figure 2 demonstrate a clear growth trend and illustrate the need for improved coding practices by software developers and for strong vulnerability management practices among IT departments.

Figure 2. *Annual vulnerability disclosures*



Vulnerability Disclosures by Month

With 642 disclosures in 2006, December remains the month with the most disclosures, as it has for the last five of seven years. The month of May comes in a close second with 627 disclosures. This affirms the average from 2000 to 2005, where December and May are historically the top two months for disclosures, as shown in Figure 3.

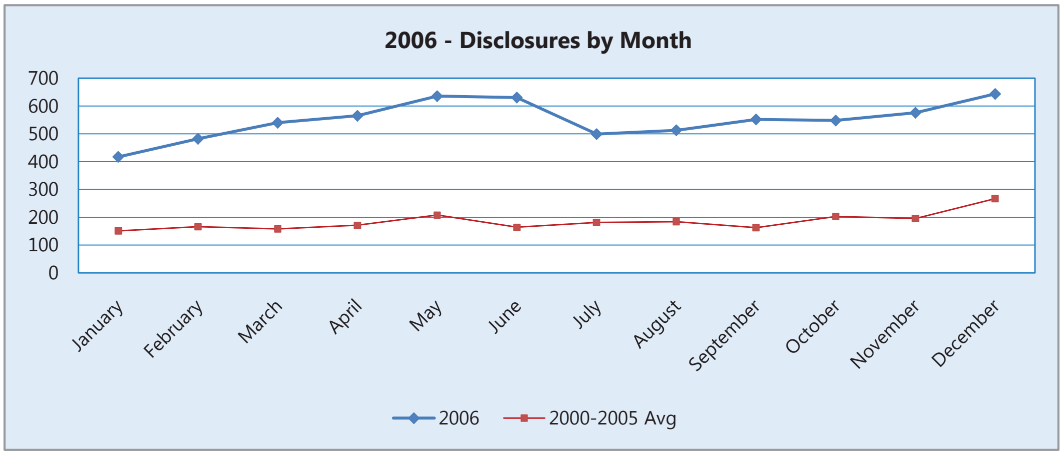


Figure 3. *Disclosures by month for 2006*

Observing monthly disclosures back to 2000, there appears to be a cyclical pattern that breaks disclosures into the first half of the year and the second half of the year. Disclosures in 2006 follow the same pattern of a steady increase from January to June, followed by a drop in July, and then a steady increase in disclosures through the end of the year.

Vulnerability Disclosures by Week

As shown in Figure 4, the weeks beginning on April 17, 2006, and December 25, 2006, vie closely for the week with the most disclosures.

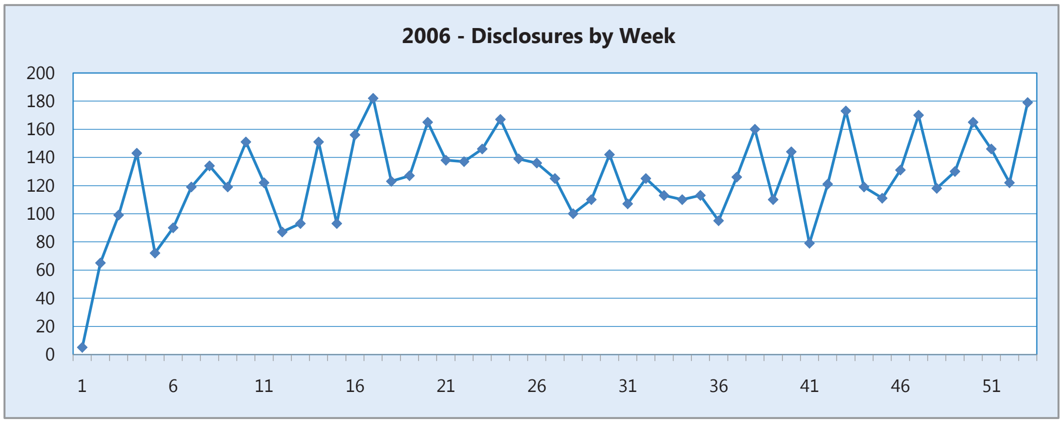
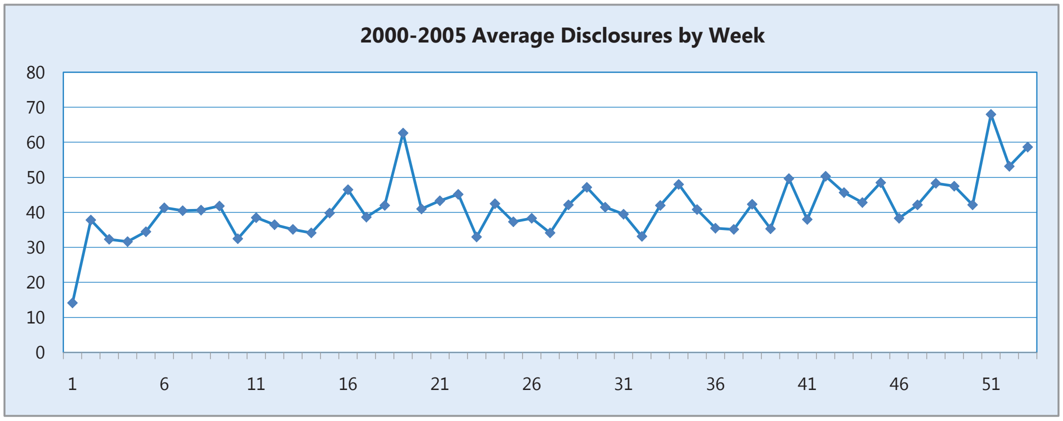


Figure 4. *Disclosures by week during 2006*

Looking at the weekly disclosures in Figure 4 and the average disclosures per week for 2000 through 2005 in Figure 5, the first week of the year consistently shows very few vulnerability disclosures.

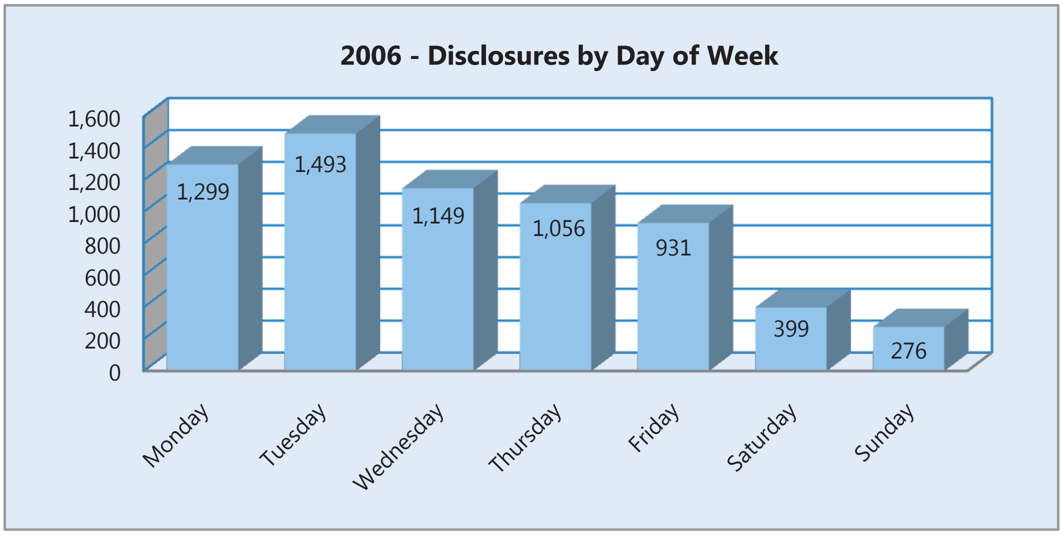
Figure 5. Average disclosures by week for 2000–2005



Vulnerability Disclosures by Day of the Week

A final calendar view of disclosures is by day of the week. As shown in Figure 6, Tuesday was the top day for new vulnerability disclosures in 2006. This is a departure from the recent averages for 2000 through 2005, in which Monday and Wednesday held top honors.

Figure 6. Disclosure by day of the week in 2006



In either case, however, the data indicates that public disclosures tend to happen during the work week, with 90 percent of all disclosures being published Monday through Friday, from 2000 through 2005. These figures are displayed in Figure 7.

With Tuesday identified as the most likely day for disclosures to happen, one must consider if this is a result of the so-called "Patch Tuesday," which is the day each month that Microsoft issues Security Bulletins. While this Microsoft policy clearly adds to the total Tuesday disclosures, the answer is no. There were 141 Tuesday disclosures for vulnerabilities affecting Microsoft products in 2006. If this amount is reduced out of the Tuesday disclosure count, Tuesday is still the top day for disclosures during 2006.

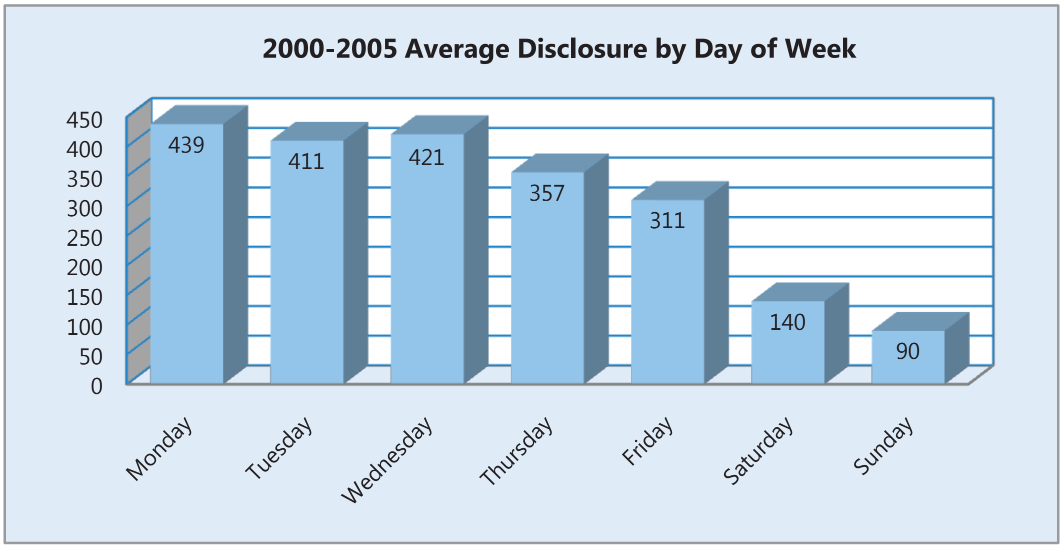


Figure 7. *Average disclosures by day of the week for 2000–2005*

Vulnerability Disclosures by Severity

The latest total vulnerability figures indicate that IT professionals and administrators have an ever-increasing volume of issues to handle, but it is also worth digging deeper to understand whether severity is increasing, as well. For purposes of severity analysis, this report uses the NVD severity ratings of High, Medium, and Low. Additional information about these rating is available at http://nvd.nist.gov/.

Figure 8 shows that while the growth of Low severity issues appears to be flattening, Medium and High severity vulnerabilities both experienced significant growth in recent periods.

Figure 8. *Vulnerabilities by severity*

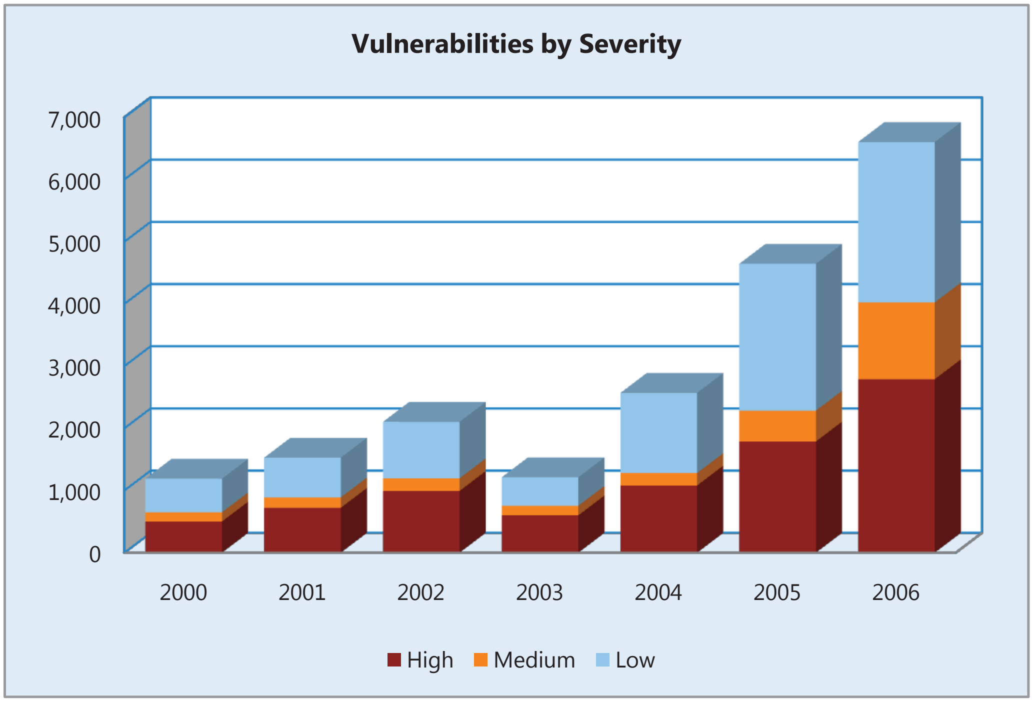
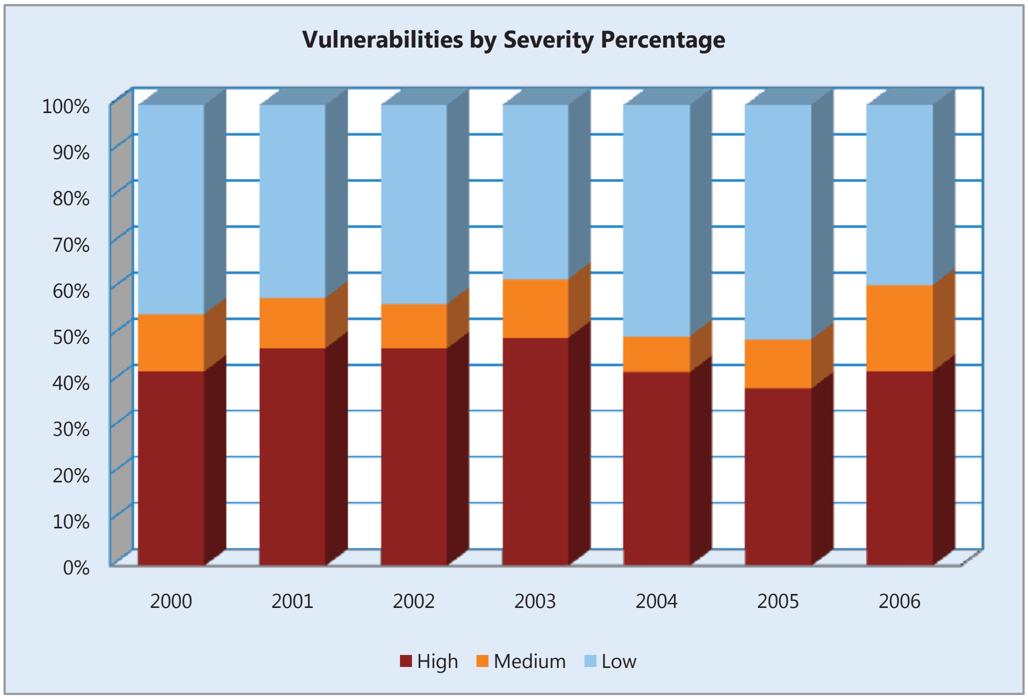


Figure 9 shows a slightly different view of severity. In charting the vulnerabilities by percentage, it appears that Medium severity issues are being identified and disclosed much more aggressively. For 2006, Low severity issues as a percentage decreased by nearly 10 percent from the previous year, while High severity issues remained flat relative to the total.

Figure 9. *Severities as a percentage of total vulnerabilities*



However, the absolute number of High severity vulnerabilities disclosed continues to increase. Given the higher-quality tools and maturing security research industry, it is likely that what we are observing in the Medium severity growth data is the improved ability to discover harder-to-find, lesser-impact vulnerabilities.

Complexity to Exploit

Another interesting way to characterize software vulnerabilities is by the level of complexity that a potential attack would require in order to exploit them. For purposes of complexity analysis, this report uses the NVD complexity ratings of Complex or Easy (to exploit). Additional information about these ratings is available at http://nvd.nist.gov/.

In the previous section, we observed that improvements in tools and techniques, and the maturing security vulnerability research industry, have resulted in increased disclosure of harder-to-find, lesser-impact vulnerabilities. This is reinforced by the complexity breakdown as shown in Figure 10. In previous periods, highly complex exploits were required for less than 5 percent of vulnerabilities disclosed. However, the trend has been upwards for the past few years, and in 2006, complex to exploit vulnerabilities jumped to more than 15 percent of the yearly total.

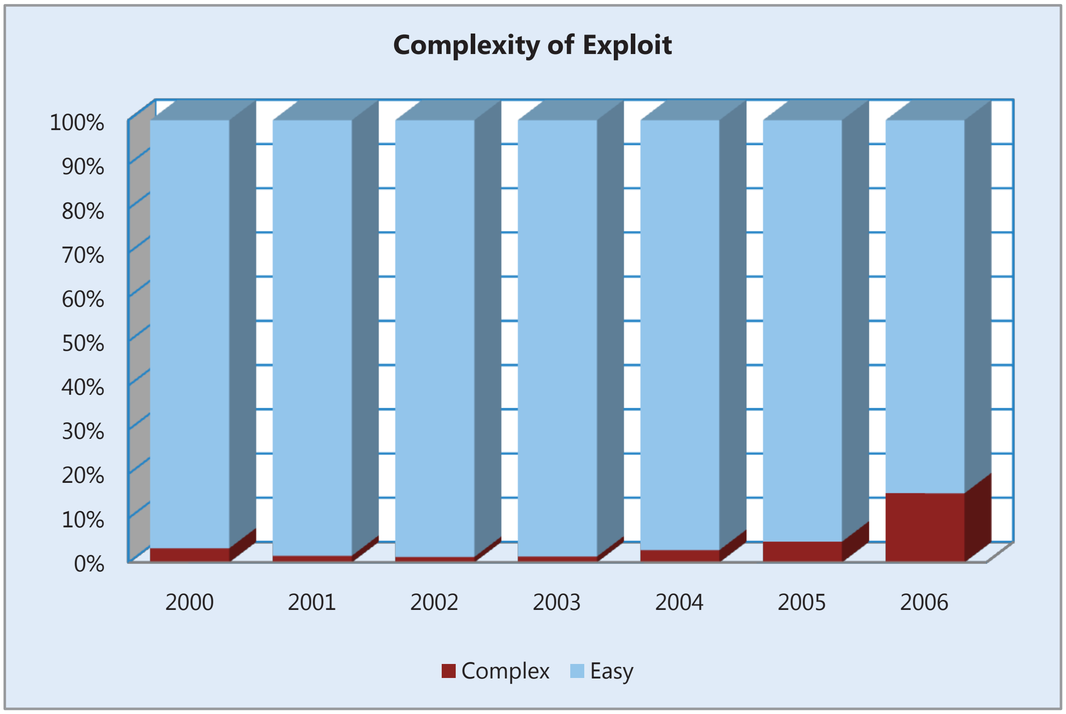
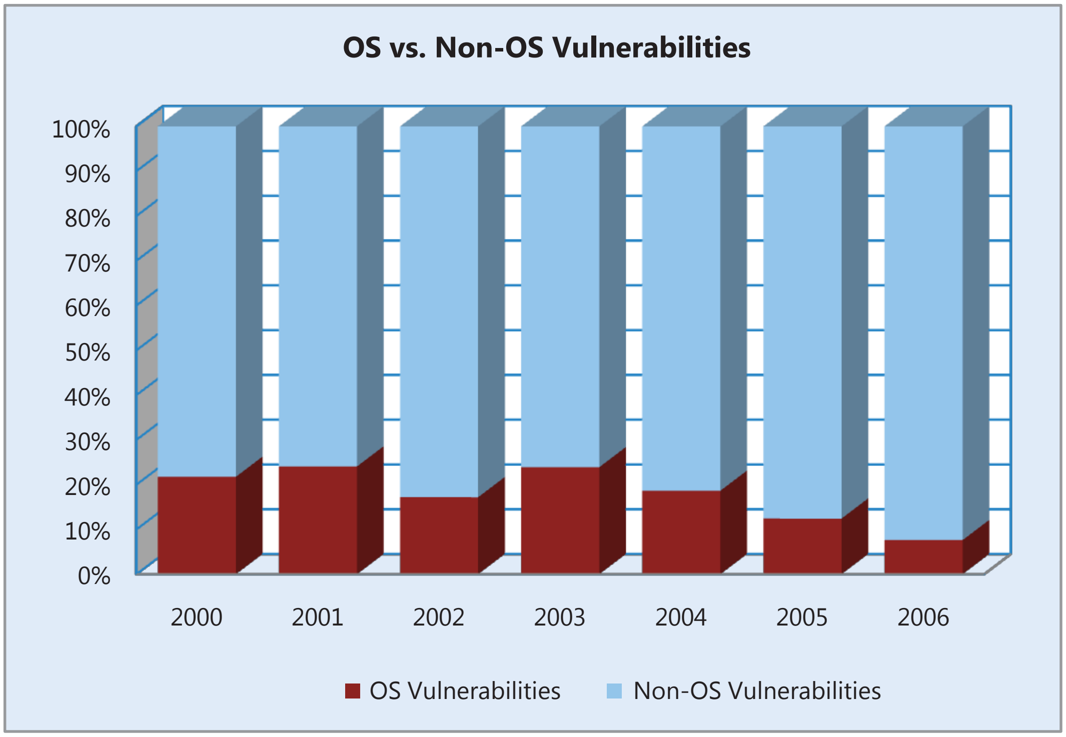


Figure 10. *Complexity of required exploit*

Operating System (OS) vs. Non-OS Disclosures

To break down vulnerabilities into OS and non-OS categories, all new vulnerabilities disclosed that affected Windows, Mac OS X, Unix, or the Linux kernel were grouped together into an **Operating System** (OS) category. The data was then used to calculate the percentage of total disclosed vulnerabilities that applied to operating systems. Figure 11 demonstrates that a decreasing percentage of vulnerabilities are from operating systems.

Figure 11. *OS versus non-OS vulnerability disclosures*



One possible interpretation of this trend is that security researchers are focusing more on applications as operating system security continues to improve. An alternate explanation could be that the number of new applications is growing far faster than the number of new operating systems and that the application proliferation is simply reflected in the vulnerability disclosure trend.

Summary and Conclusion

Disclosure of new vulnerabilities continues on a steady upward trend, with all categories of severity increasing over previous years. However, researchers appear to be finding many more “complex to attack” vulnerabilities than they did in the past. This suggests that the security research and testing industry is maturing, both in skill and in the level of tools they utilize, as evidenced by the increased use of fuzz testing techniques and other rigorous testing methods and devices.

Because applications continue on a three-year trend of contributing a higher percentage of vulnerabilities relative to the total number of disclosures, it is likely that applications are becoming a more attractive target to researchers, relative to operating systems. Both security vendors and IT professionals should adjust their risk-management processes appropriately.

Malicious Software

This section discusses the emergence of new malware variants and the prevalence of malicious software during 2H06. Notably, the emergence of new, potentially unwanted software variants is discussed in the “Potentially Unwanted Software” section.

Malicious Software Categories

This report refers to the categories of malicious software as shown in Figure 12.

***Figure 12.** Malicious software activity by category - 2006*

Category	Description
Backdoor Trojan	A type of Trojan that provides attackers with remote access to infected computers. Bots are a sub-category of backdoor Trojans, which often use Internet Relay Chat (IRC) as their main method of communication.
Exploit	Malicious code that takes advantage of software vulnerabilities to infect a computer.
IM worm	Malware that spreads through instant messaging (IM) applications, such as Windows Live Messenger and AOL Instant Messenger, typically by sending IM messages that include a link to an infected copy of itself.
Malware	Malicious software or potentially unwanted software installed without adequate user consent.
Mass-mailing worm	Malware that spreads by spontaneously sending copies of itself through e-mail.
P2P worm	Malware that copies itself to file shares that are associated with peer-to-peer (P2P) applications, such as KaZaA and Winny, to facilitate its spread over those networks.
Password stealer (PWS)/keylogger	A password stealer (PWS) is malware that is specifically used to transmit personal information, such as usernames and passwords. A PWS often works in conjunction with a keylogger, which sends key strokes and/or screen shots to an attacker.
Trojan	A generally self-contained program that does not self-replicate, but takes malicious action on the computer.
Trojan downloader/dropper	A form of Trojan that installs other malicious files to the infected system either by downloading them from a remote computer or by dropping them directly from a copy contained in its own code.
Virus	Malware that infects other files in the system, thus allowing the execution of the malware code and its propagation when those files are activated.

Although the category descriptions have been refined for this report, they are consistent with those defined in the 1H06 version of this document[1]. These category descriptions are also consistent with those found in the white paper *MSRT: Progress Made, Lessons Learned*[2].

These categories are not mutually exclusive—one malware variant or family might fit into several of the categories. For example, backdoor Trojans, password stealers, keyloggers, Trojan downloaders, and Trojan droppers are all different types of Trojans that have specific functionality, as implied from their names. The classification of families to malware types uses a rule where the most relevant type applies. Malware families that include Trojan functionality, but do not include any of the specific Trojan behaviors that are listed above, were classified using the general Trojan category.

Malicious Software Activity

There is some correlation between the metrics of malware *activity* and malware *prevalence*, though they are not tightly correlated. For example, Win32/Rbot is a malware family with both a large number of variants and a high number of detections, and these detections are distributed widely across the variants. Some other malware families have many variants, but they are less prevalent than families with significantly fewer variants.

Prevalence by Variants

The number of malware variants remained steady throughout the second half of 2006, with backdoor Trojans—in particular, bots—remaining the most active category. On average, the Microsoft Security Research & Response team analyzed more than 7,000 unique backdoor Trojan variants each month, and approximately 4,500 of those were variants of bots.

> ***"The number of password stealer and keylogger variants associated with the Win32/Banker and Win32/Bancos families generally decreased from 1H06 to 2H06."***

The number of password stealer and keylogger variants associated with the Win32/Banker and Win32/Bancos families generally decreased from 1H06 to 2H06. However, both families remain active in Brazil and other Portuguese-speaking countries. The Win32/Banker family was added to the Windows Malicious Software Removal Tool (MSRT) in August 2006, followed closely by the Win32/Bancos family in September 2006.

Conversely, the number of Trojan downloaders/droppers increased in the second half of 2006. One new and particularly active family was Win32/Stration, a family of Trojan

[1] The previous Microsoft Security Intelligence Report can be downloaded from the Microsoft Download Center (http://go.microsoft.com/?linkid=6543860.)

[2] This white paper can be downloaded from the Microsoft Download Center (http://go.microsoft.com/fwlink/?linkid=67998).

downloaders and mass-mailing worms that first gained momentum in September 2006. Win32/Stration uses many different variants of downloaders to get files from remote Web sites, which in many cases are new variants of the Win32/Stration e-mail worm. Nearly 5,000 unique Win32/Stration downloader variants were discovered in the fourth quarter of 2006 alone. Another notable downloader family was the Win32/Zlob family, which spawned nearly 2,900 variants in 2H06.

Along with increases in backdoor Trojans and Trojan downloaders/droppers, there were also increases in the activity of traditional Trojans and mass-mailing worms, as shown in Figure 13.

Figure 13. *Malicious software activity during 1H06 and 2H06*

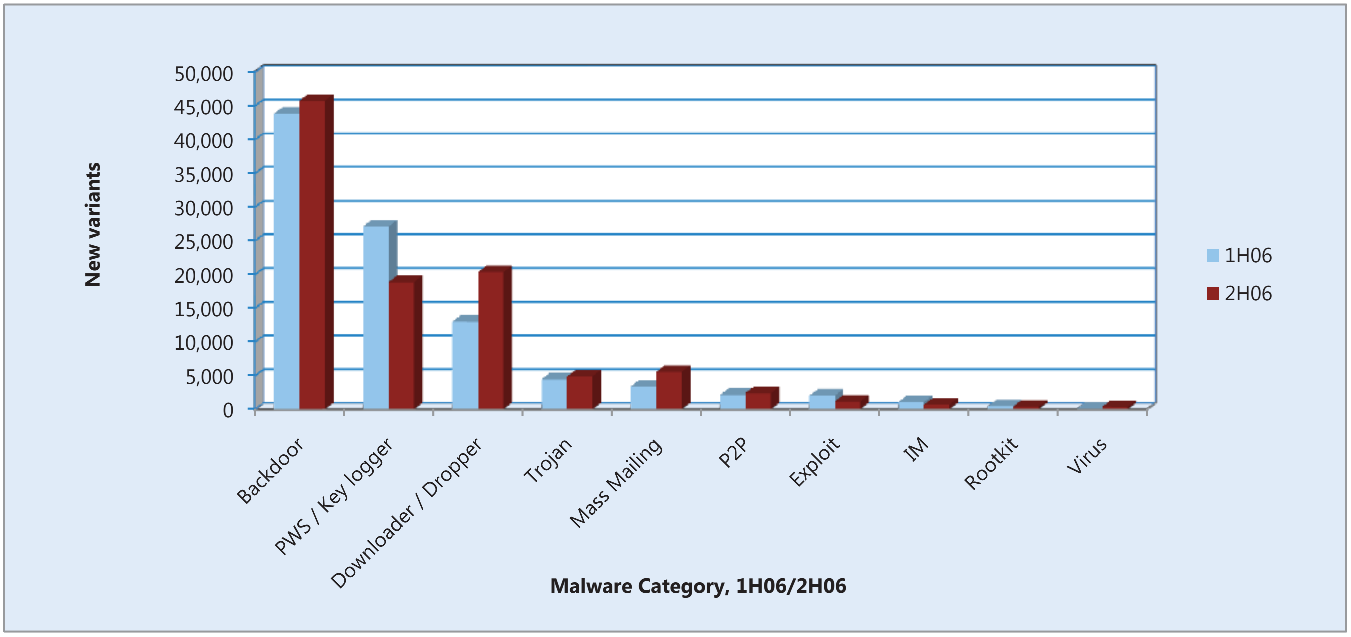


Figure 14. Top 25 most active malware families during 2H06

The most significant additions to the 2H06 25 most-active families list were the Win32/Stration mass-mailing worms and the Trojan downloaders family. Six of the top active families were bots. Many of the families appearing on the 2H06 report were carry-overs from the 1H06 report, signifying a continuing prevalence of these threats.

Rank	Malware Family	Mail	P2P	IM	Exploit	Backdoor	Rootkit	Virus	PWS / Key logger	Downloader / Dropper	Trojan	Number of variants (2H06)
1	Win32/Rbot					●						15,195
2	Win32/Banker								●			8,955
3	Win32/Hupigon					●			●	●		8,544
4	Win32/Stration	●								●		7,871
5	Win32/Sdbot					●						6,892
6	Win32/Small					●			●	●	●	3,115
7	Win32/Mmosteal								●			3,078
8	Win32/Zlob									●		2,873
9	Win32/Bancos								●			2,817
10	Win32/Gaobot					●						2,710
11	Win32/Tibs					●				●		2,483
12	Win32/Spybot		●			●						2,264
13	Win32/VB					●			●	●	●	2,167
14	Win32/Agent					●			●	●	●	1,803
15	Win32/Harnig									●	●	1,744
16	Win32/Lineage								●			1,676
17	Win32/Delf					●			●	●	●	1,589
18	Win32/Adload									●		1,021
19	Win32/Inservice									●		803
20	Win32/IRCbot					●						803
21	Win32/Sinowal								●			731
22	Win32/Mytob	●		●	●	●						727
23	Win32/Adialer										●	571
24	Win32/Bifrose					●						495
25	Win32/Startpage										●	433

Over 3,700 distinct malicious WMF files exploiting the MS06-001 vulnerability were discovered during the second half of 2006. This continued prevalence demonstrates that, despite the availability of a security update, attackers continue to attempt to exploit this particular vulnerability. Nevertheless, the effectiveness of these attacks was greatly reduced during 2H06.

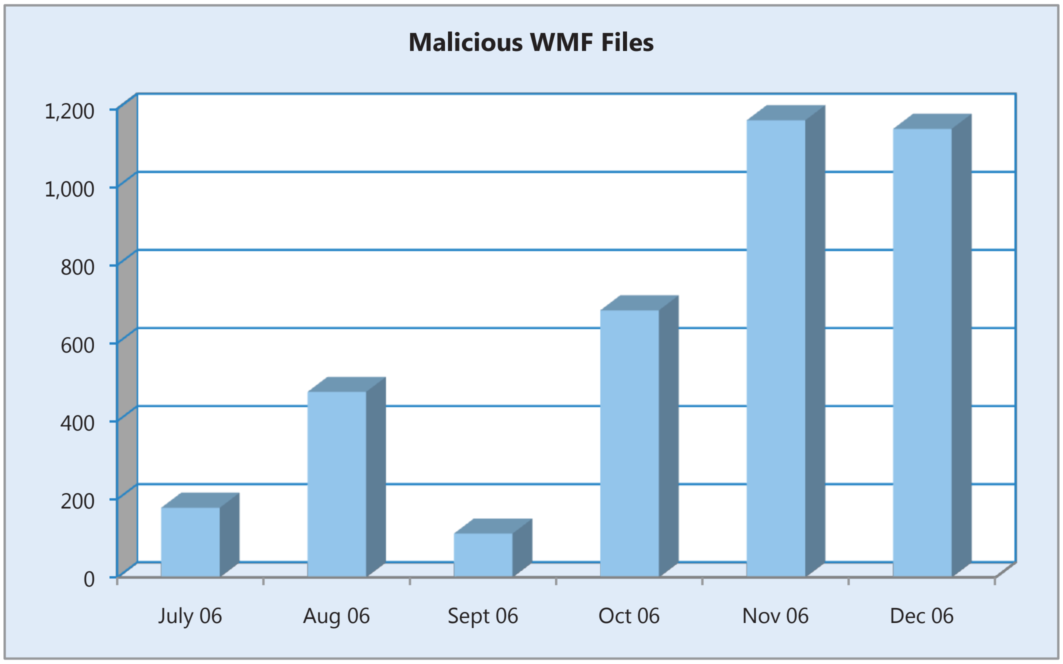


Figure 15. *New malicious WMF files during 2H06*

Additional exploits of Microsoft Office vulnerabilities have been recorded in 2H06. As before, most of the attacks were targeted, the detection numbers were very low and sometimes even zero, and in only a few cases were they detected on more than a handful of computers.

Figure 16 shows some examples of the additional generic exploit detections that were added to real-time protection during 2006.

Figure 16. *Examples of generic exploit detections added during 2006*

CVE ID	Security Update	Microsoft Generic Detection Name	Added On
CVE-2006-3649	MS06-047	Exploit:Win32/Ponaml.gen	Jun 06
CVE-2006-3059	MS06-037	Exploit:Win32/Exllobj.gen	Jun 06
CVE-2006-3590	MS06-048	Exploit:Win32/Chippto.gen	Jun 06
CVE-2006-3086	MS06-050	Exploit:Win32/Exllhlk.gen	Jul 06
CVE-2006-4868	MS06-055	Exploit:HTML/Levem	Aug 06
CVE-2006-3439	MS06-040	Exploit:Win32/MS06-040	Aug 06
CVE-2006-4534	MS06-060	Exploit:Win32/Wordfib.gen	Sep 06
CVE-2006-4777	MS06-067	Exploit:HTML/Daxctl	Sep 06
CVE-2006-3730	MS06-057	Exploit:JS/SetSlice	Oct 06
CVE-2006-0022	MS06-028	Exploit:Win32/Teppto.gen	Oct 06
CVE-2006-4704	MS06-073	Exploit:HTML/Meloits.A	Nov 06
CVE-2006-5745	MS06-071	Exploit:HTML/Xmlreq.A	Nov 06
CVE-2006-4691	MS06-070	Exploit:Python/MS06-070	Nov 06

Of the generic exploit detections that were added to exploits in other products, Exploit: JS/SetSlice, which addresses exploits of Windows vulnerability MS06-057, eventually became the fourth-most-detected malware by Windows Live OneCare.

Prevalence by Infection

The Microsoft Windows Malicious Software Removal Tool (MSRT) is designed to help identify and remove prevalent malware from customer computers and is available at no charge to licensed Windows users. Beginning in 2H05, the MSRT began measuring the number of unique computers cleaned. Since then, the MSRT has removed 31 million infections from 11.7 million computers worldwide. The number of executions has more than tripled since the first release of the tool and so has the number of disinfections. The moderate increase in the number of disinfections in 2H06 compared to 1H06 is the result of a combination of disinfections of active malware families that were added to the MSRT during 2H06, along with the decreasing prevalence of most of those families, which were already removed by the tool.

> ***“The Microsoft Windows Malicious Software Removal Tool (MSRT) is designed to help identify and remove prevalent malware from customer computers and is available at no charge to licensed Windows users.”***

The number of malware disinfections and computers cleaned by the MSRT are depicted in Figure 17.

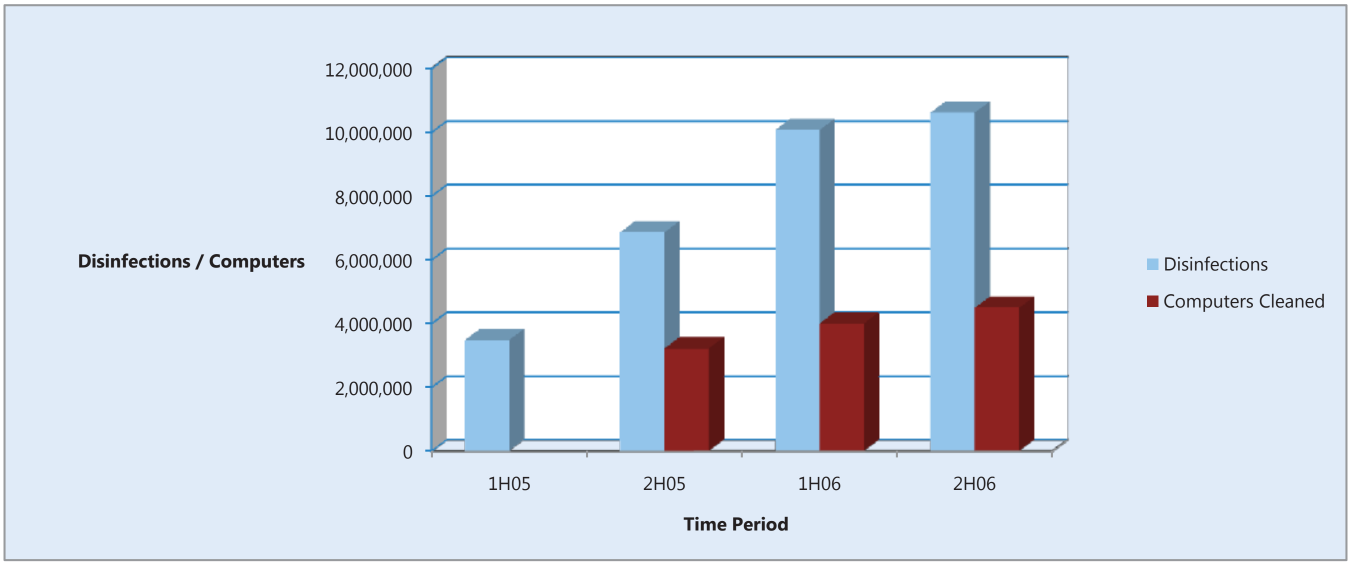


Figure 17. *Malware disinfections and computers cleaned by the MSRT*

Prevalence by Category

The Malicious Software Removal Tool

The MSRT is primarily released through Windows Update (WU), Microsoft Update (MU), and Automatic Updates (AU). A version of the tool is also available for download from the Microsoft Download Center. As of December 2006, the tool is capable of detecting and removing 82 different malware families. Notably, the tool does not target potentially unwanted software. The MSRT is also not a replacement for an up-to-date antivirus solution because of its lack of real-time protection and also because it uses only the portion of the Microsoft antivirus signature database that enables it to target prevalent malicious software.

Bots and Backdoor Trojans

Bots are used in botnets, which are groups of infected computers that are controlled by attackers, usually by using IRC channels. Bots remained the most active type of malware in 2H06, but in terms of prevalence, both bots and backdoor Trojans continued to decline throughout 2H06. Of computers in which the MSRT detected any malware during the period, detections of bots and backdoor Trojans declined from 68 percent in 2H05, to 50 percent in 1H06, to 43 percent in 2H06. Viewed as absolute numbers, the decrease appears more moderate—from 2.2 million backdoor Trojan detections in 2H05, to 2.0 million in 1H06, to 1.94 million detections in 2H06.

Trojan Downloaders and Droppers

The increase in the number of Trojan downloaders and droppers in 2H06 is not surprising. Malware often includes Trojan downloader and dropper components as part of the process it uses to infect a computer and take control over it. For example, the active Win32/Stration, Win32/Zlob, and Win32/Tibs malware families all include Trojan downloader or dropper components. Variants of Win32/Zlob were removed from 360,000 computers during 2H06.

Password Stealers and Keyloggers

In Brazil, the Win32/Banker and Win32/Bancos password stealers and keyloggers malware families rose to prominence in 2006. This malware, often sent in Portuguese and disguised as a greeting card e-mail message, mostly targets online banking users in Brazil. The MSRT removed this malware from 304,000 computers and 92,000 computers, respectively, during 2H06. Another prevalent family, Win32/Sinowal, was added to the MSRT in September 2006, and by the end of 2H06, the MSRT had disinfected 156,000 computers from this malware.

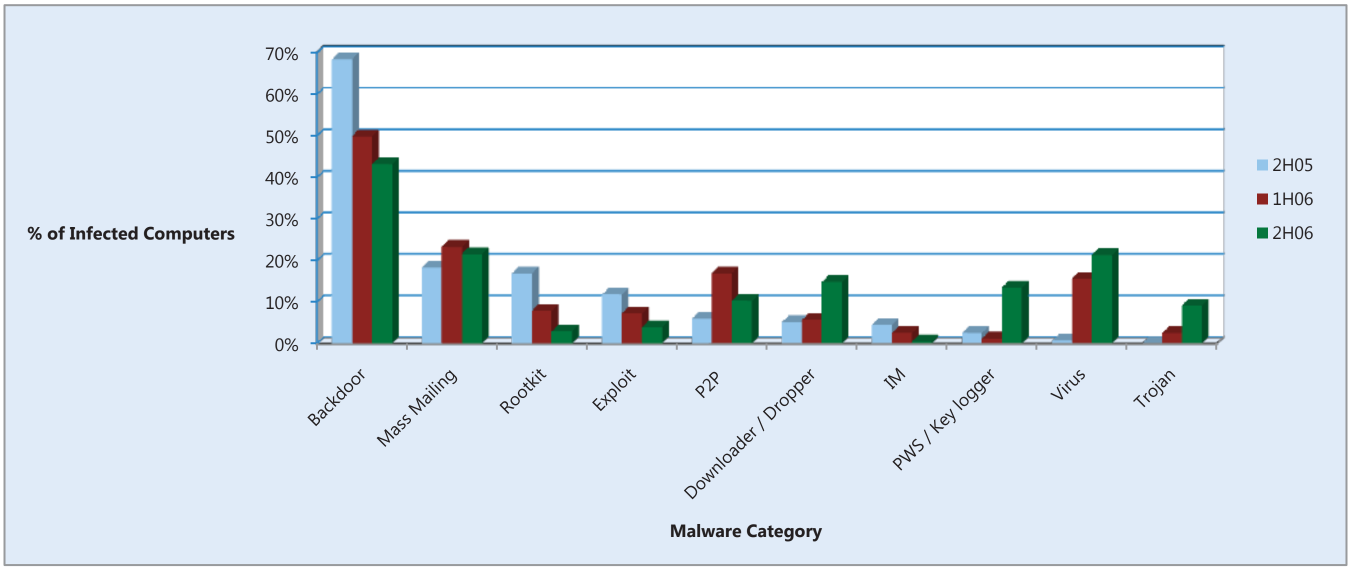
> ***"The significant numbers of mass-mailer worms detected demonstrates that e-mail remains an effective vector for spreading malware and infecting computers worldwide."***

Traditional Threats

Some file infectors are still active and prevalent even though they became active years ago. The MSRT removed Win32/Parite from 509,000 computers in 2H06. Win32/Jeefo, added in August 2006, accounted for disinfections of 384,000 computers in 2H06. Additionally, the significant numbers of mass-mailer worms detected demonstrates that e-mail remains an effective vector for spreading malware and infecting computers worldwide.

Figure 18 illustrates the categories of malicious software that were removed by the MSRT from infected computers in 2H05, 1H06, and 2H06. Malware categories are ordered by infection percentages by 2H05, 1H06, and 2H06, respectively. Note that these percentages correspond to infected computers, not to all computers scanned. For example, in 2H05, of the 3.2 million unique computers cleaned, approximately 2.2 million (or 68 percent) of these computers had some type of backdoor Trojan active on the system.

Figure 18. *Categories of malware removed by the MSRT during 2H05, 1H06, and 2H06*



Note that while Figure 18 shows a lower number of exploit detections by the MSRT during the second half of 2006, this number may be misleading, as there was actually an *increase* in the use of exploits during that period (as shown in the following section). The execution time of most of these exploits is short, and as a result, they are not included in the MSRT.

Windows Live OneCare

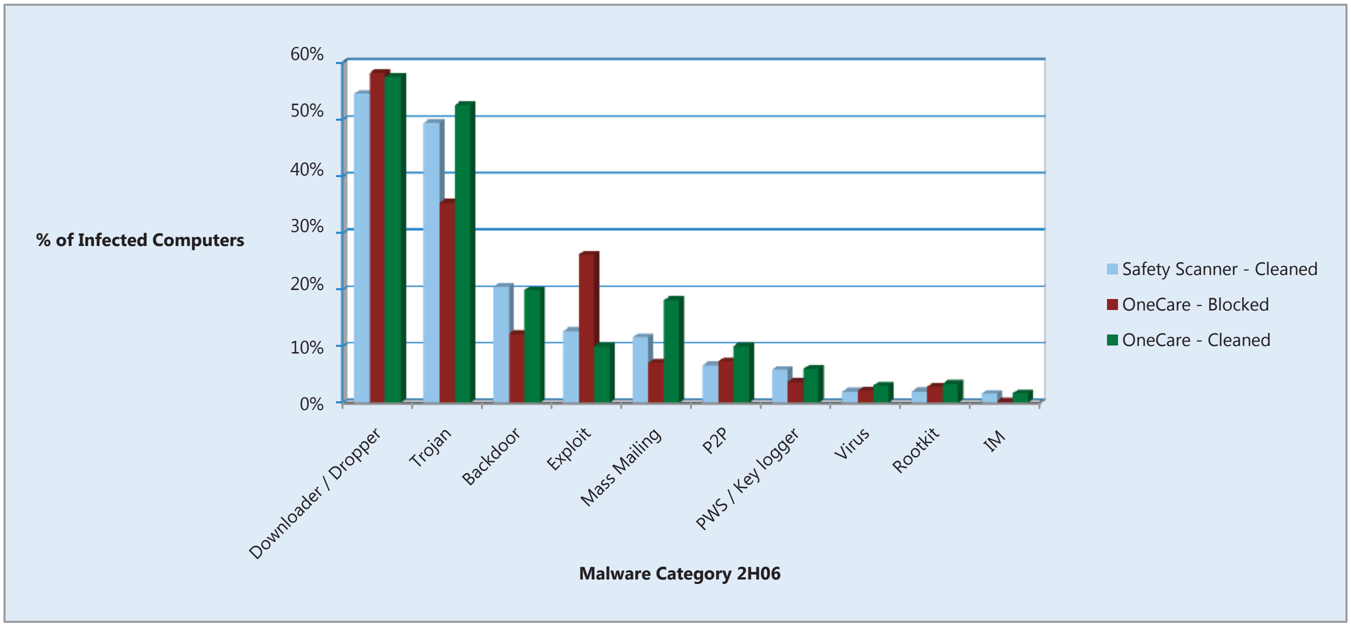
There were no significant changes in the type of malware that Windows Live OneCare and the Windows Live OneCare safety scanner detected in 2H06 compared to 1H06. Trojan downloaders and droppers remain the most common type of malware to be blocked and cleaned. The detection rate in Figure 19 is higher than the one shown in Figure 18 (MSRT) because the MSRT uses only a partial signature set. MSRT detects families that are resident in memory during its short scanning time and therefore does not include detection for many of the downloaders.

The high detection rate of exploits found by Windows Live OneCare is a result of the addition of a list of generic exploits detections during 2H06. For example, in October 2006, detection for Exploit:JS/SetSlice was added to Windows Live OneCare to block exploits of the vulnerability discussed in security update MS06-057. The safety scanner detected these exploits over 2,200 times during the second half of 2006. But while attackers continued to release large numbers of malicious WMF files (over 3,700 files detected in 2H06), the number of detections of WMF exploits by Windows Live OneCare in 2H06 actually decreased by 63 percent compared to the corresponding number in 1H06. This demonstrates that this attack technique was not as effective as in the previous period, likely due to increased deployment of the security update for this vulnerability (MS06-001), as well as improved detection by different antivirus programs.

Figure 19 shows the categories of malicious software removed by Windows Live OneCare safety scanner and Windows Live OneCare, using the same categories as shown in Figure 18 for the MSRT. The data for Windows Live OneCare is divided into two subsets, one showing malicious software that is blocked by the scanner's on-access/real-time mechanism, and the other showing malicious software that is found on the computer and then removed (cleaned). This makes it easier to compare the Windows Live OneCare data to the Windows Live OneCare safety scanner data because the Windows Live OneCare safety scanner does not block malicious software from infecting a computer.

Note that the percentage of all the types is higher than 100 percent because some of the malware families are multi-component and correspond to more than one malware type.

Figure 19. *Types of malware removed or blocked by the Windows Live OneCare safety scanner and Windows Live OneCare in 2H06*



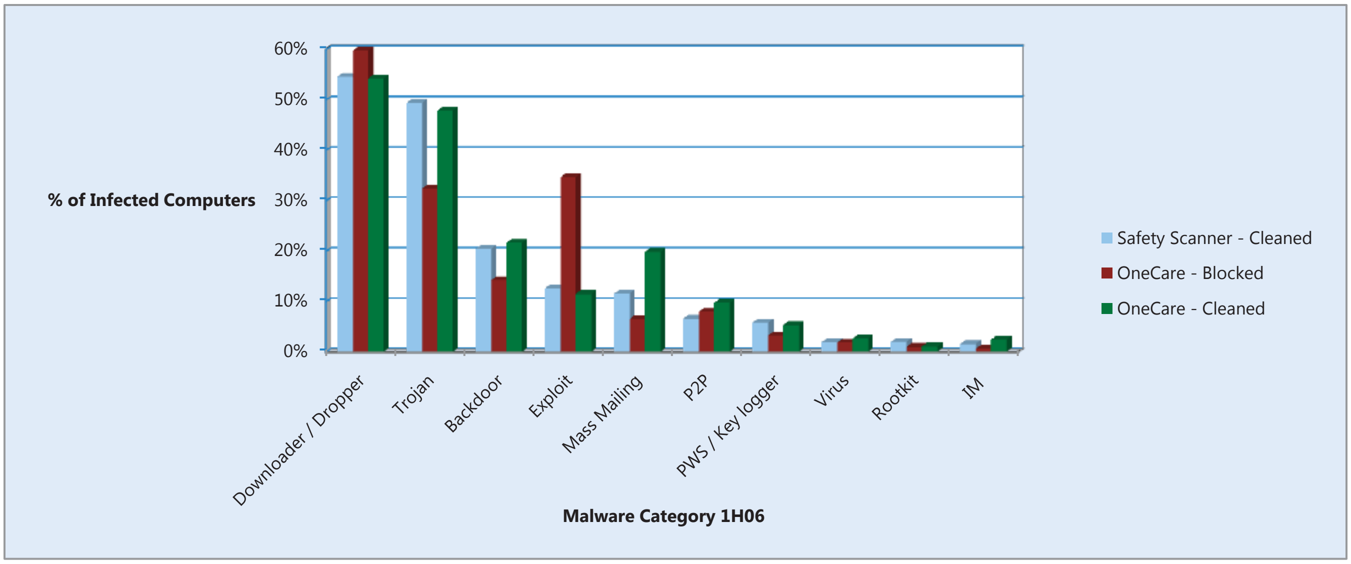


***Figure 20.** Types of malware removed or blocked by the Windows Live OneCare safety scanner and Windows Live OneCare in 1H06*

Prevalence by Family

With one exception, the prevalence of malware families included in the MSRT since the beginning of 1H06 has decreased in 2H06 compared to 1H06. This is in spite of a 12-percent increase in the number of MSRT executions between these two periods. For 9 of those 12 families, the number of cleaned computers dropped by a range of 33 to 70 percent. Additionally, the rank of most of the families included in Figure 21 fell during 2H06 compared to their rank in 1H06. Overall, this data demonstrates that the MSRT has been an effective tool for removing malware from computers around the world.

> ***"...The MSRT has been an effective tool for removing malware from computers around the world."***

Figure 21 lists the top 25 malicious software families removed by the MSRT during the second half of 2006. Figure 21 includes both the number of disinfections for each malware family and the number of unique computers cleaned, sorted by the latter. The number of disinfections for each family is greater than the number of unique computers cleaned because multiple variants might infect a single computer, or a computer might become re-infected.

Figure 21 also shows the percentage change in the number of computers cleaned for each malicious family since the previous six-month period (1H06). To ensure accuracy, rankings from the last period are included only for those families that were included in the tool since the beginning of the last six-month period, in January 2006.

Figure 21. *Top 25 malicious families cleaned by the MSRT during 2H06*

Rank	Malware Family	Disinfections	Computers Cleaned	Computers Cleaned Change Since 1H06	Rank from 1H06
1	Win32/Rbot	1,531,448	812,543	-33.19%	1
2	Win32/Hupigon	1,448,185	634,356	-	
3	Win32/Parite	1,189,599	508,886	-13.54%	2
4	Win32/Wukill	701,749	384,316	1.59%	4
5	Win32/Jeefo	946,929	384,235	-	
6	Win32/Alcan	598,537	362,474	-29.60%	3
7	Win32/Zlob	872,614	359,596	265.41%	10
8	Win32/Banker	579,904	304,343	-	
9	Win32/Brontok	460,672	282,042	-	
10	Win32/Sdbot	347,022	205,877	-41.40%	5
11	Win32/Sinowal	442,656	156,185	-	
12	Win32/Bancos	153,464	91,690	-	
13	Win32/IRCbot	127,664	82,002	29.83%	16
14	Win32/Tibs	193,178	75,613	-	
15	Win32/Netsky	94,015	57,882	-32.89%	13
16	Win32/Mywife	158,993	53,603	-54.89%	8
17	Win32/Chir	82,567	51,112	-	
18	WinNT/FURootkit	87,283	48,724	-68.27%	6
19	WinNT/F4IRootkit	60,793	40,848	-64.97%	9
20	Win32/Spybot	59,920	38,494	-45.01%	15
21	Win32/Bagle	79,812	37,639	-70.28%	7
22	Win32/Alemod	91,151	34,069	-	
23	Win32/Beenut	39,960	33,831	-	
24	Win32/Gaobot	70,184	33,702	-61.67%	12
25	Win32/Antinny	104,192	32,301	-54.78%	14

Some of the families that were added to the detection and cleaning capabilities of the MSRT turned out to be fairly prevalent. Over 8,500 variants of Win32/Hupigon were removed from 634,000 computers during 2H06. Equally prolific, the Win32/Jeefo, Win32/Alcan, Win32/Zlob, and Win32/Banker families were each removed from over 300,000 computers during the same period. Note that Win32/Banker and Win32/Jeefo were added to the MSRT in August 2006; therefore their average monthly removal numbers are even higher than the other two families, which were added to the MSRT during the first half of 2006.

Top Malicious Programs Cleaned

Figures 22, 23, and 24 list the top malicious software programs detected by Windows Live OneCare and the Windows Live OneCare safety scanner during 1H06 and 2H06, ranked by the number of unique computers on which each malware family was detected.

As previously discussed, the number of WMF exploits detected by Windows Live OneCare dropped by 63 percent between 1H06 and 2H06, while other exploit detections, such as JS/SetSlice, Win32/MS05-002, and HTML/AdoStream, were newly added to the list. This demonstrates the power of real-time protection combined with generic signatures.

Notably during 2H06, Win32/Zlob became the top-detected malware family by Windows Live OneCare and ranked number seven on the MSRT list. Nearly 2,900 variants of Win32/Zlob were detected during 2H06, and Win32/Small, Win32/VB, and Win32/Agent are simply large collections of Trojan downloaders and droppers with 3,100, 2,100, and 1,800 new variants, respectively.

OneCare - Blocked Rank	1H06 Malware Family	2H06 Malware Family
1	Win32/Wmfap	Win32/Zlob
2	Win32/Small	Win32/Wmfap
3	Win32/Agent	Win32/MS05-002
4	Win32/Wmfpfv	JS/SetSlice
5	Win32/VB	Win32/Wmfpfv
6	Java/Classloader	HTML/AdoStream
7	Win32/Alcan	Win32/Small
8	JS/Onload	Win32/VB
9	Win32/Rbot	Win32/Alcan
10	Win32/Istbar	Win32/Agent
11	Java/Bytverify	Win32/Rbot
12	Win32/Zlob	Java/Classloader
13	Win32/Renos	JS/Mult
14	JS/Drost	Win32/Istbar
15	Win32/P2Pworm	Java/Bytverify
16	JS/Mult	JS/Xfiledownloader
17	Win32/Swizzor	Win32/Tibs
18	Win32/Adialer	BAT/BWG
19	Tool:PornDialer	HTML/MhtRedir
20	VBS/Small	Win32/Sdbot
21	WinNT/Smallrk	VBS/Small
22	Win32/Lowzones	JS/Onload
23	Win32/Sdbot	Win32/Alureon
24	Win32/TSUpdate	Win32/Swizzor
25	HTML/Winload	Win32/Stration

Figure 22. *Top 25 malware families blocked by Windows Live OneCare in 1H06 and 2H06*

While there is some overlap in the malware blocked by Windows Live OneCare (on-access detection) and the malware that gets cleaned (on-demand access), there are also great dissimilarities. For example, the on-demand scan often finds malicious Java applets in the Internet Cache folder (reflected in Figure 23). While users surf the Web, they may access HTML pages that download or drop ZIP files with these JAVA applets included. During the on-demand scan, these HTML pages and applets get detected and cleaned. On the other hand, exploit detections happen more rarely during on-demand scans because these detections are effective in blocking the access to these files.

Figure 23. *Top 25 malware families cleaned by Windows Live OneCare in 1H06 and 2H06*

Cleaned by Windows Live OneCare Rank	1H06 Malware Family	2H06 Malware Family
1	Java/Classloader	Java/Classloader
2	Java/Bytverify	Win32/Zlob
3	Win32/Small	Java/Bytverify
4	Win32/Agent	Win32/Small
5	Java/OpenConnection	Win32/Agent
6	Java/OpenStream	Win32/Alcan
7	Win32/Istbar	Java/OpenConnection
8	Win32/Alcan	Java/OpenStream
9	Win32/VB	Win32/VB
10	Win32/Bagle	Win32/Bagle
11	Win32/Netsky	Win32/Netsky
12	Win32/Wmfap	Win32/Rbot
13	Win32/Rbot	Win32/Istbar
14	Win32/Sober	Win32/Wmfap
15	HTML/Bankfraud	Exploit:ContentMismatch
16	Win32/Lowzones	Win32/MS05-002
17	Win32/Zlob	Win32/Sober
18	Tool:PornDialer	Java/Beyond
19	Win32/Sdbot	Win32/Stration
20	Win32/TSUpdate	HTML/Bankfraud
21	Win32/Adialer	Win32/TSUpdate
22	Win32/Delf	Win32/Lowzones
23	Exploit:ContentMismatch	Win32/Sdbot
24	Exploit:LongName	Win32/Tibs
25	Win32/Swizzor	VBS/Small

Predictably, the type of malware found by Windows Live OneCare safety scanner is very similar to what is found during on-demand scans of Windows Live OneCare. Both methods involve scans of large portions of the computer's hard drive. The only major changes that reflect differences between the two are the drop in the rank of the

WMF exploit detection and the jump in the rank of the Win32/Zlob, both trends already discussed previously in this report.

Cleaned by Windows Live OneCare Safety Scanner	1H06	2H06
Rank	Malware Family	Malware Family
1	Win32/Small	Java/Classloader
2	Java/Classloader	Win32/Zlob
3	Win32/Agent	Win32/Small
4	Java/Bytverify	Java/Bytverify
5	Win32/Istbar	Java/OpenConnection
6	Java/OpenConnection	Win32/Agent
7	Win32/VB	Win32/Alcan
8	Java/OpenStream	Win32/Swizzor
9	Win32/Rbot	Win32/Netsky
10	Win32/Wmfap	Java/Openstream
11	Win32/Alcan	Win32/VB
12	Win32/Adialer	Win32/Rbot
13	Win32/Netsky	Win32/Bagle
14	Win32/Sdbot	Win32/Antinny
15	Win32/Bagle	Win32/Istbar
16	Win32/Dyfuca	Win32/Adialer
17	Win32/Delf	Win32/Stration
18	Win32/Sober	WinNT/Protmin
19	Win32/Swizzor	Win32/Wmfpfv
20	Win32/Startpage	Win32/Sdbot
21	Win32/TSUpdate	Win32/Wmfap
22	Win32/Adload	HTML/MhtRedir
23	HTML/MhtRedir	Win32/Lowzones
24	Win32/Zlob	Win32/Sober
25	Win32/Lowzones	Win32/Delf

Figure 24. *Top 25 malware families cleaned by Windows Live OneCare safety scanner in 1H06 and 2H06*

Prevalence by Operating System

The first two charts in Figure 25 show the percentages of prevalence of malicious software by operating system for 1H06 and 2H06. The major trends illustrated in these charts are similar to those observed in the previous report and reflect a combination of the following:

- Expected movement of customers to newer and more secure service packs
- Decrease in detections by the MSRT of malicious software that relies on replication of software vulnerabilities that have been resolved in Microsoft Windows XP SP2
- Increase in social engineering malware, as illustrated in Figure 18

During 2H06, 91.4 percent of the MSRT executions through Windows Update/ Automatic Update (WU/AU) were on computers running Windows XP SP2, compared to 1.1 percent for computers running Windows XP and 2.2 percent for computers running Windows XP SP1.

The chart data in Figure 25 has been normalized to accurately reflect executions on the specific operating system (OS). The normalization formula used is as follows:

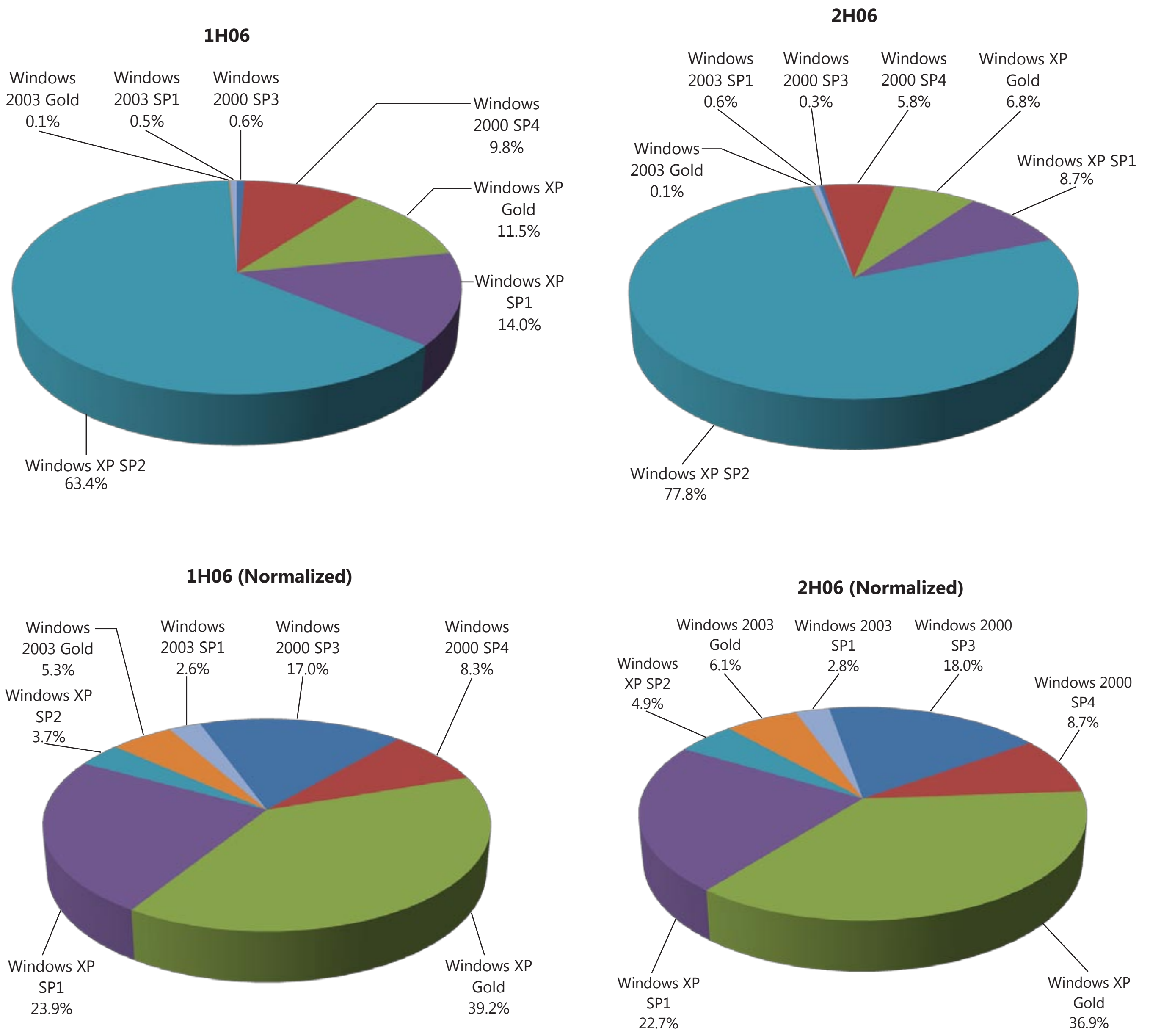
$$\text{Normalized disinfections}_{\text{OS}} = \text{Disinfections}_{\text{OS}} \,/\, \text{Execution percentage}_{\text{OS}}$$

Applying this formula to the figures for 1H06 and 2H06 yields the 1H06 (normalized) and 2H06 (normalized) charts in Figure 25, which depict percentages of computers cleaned by the MSRT by operating system.

The normalized charts help with understanding which operating system versions are more likely to be infected with malware. After normalization, the Windows XP SP2 infection rate in 2H06 was 4.9 percent, while the Windows XP Gold version (released with no service packs) infection rate was 36.9 percent. This means that the likelihood of the MSRT finding malware on a Windows XP Gold version computer is 7.5 times higher than the likelihood of the MSRT finding malware on a Windows XP SP2 computer, and in general, the higher the service pack level is, the less likely the MSRT is to find malware on a computer. This ratio between the infection rates of Windows XP and Windows XP SP2 is actually lower than it was in 1H06. This is due to the higher proportional detection of malware families that rely on social engineering, as social engineering can trick the user into installing malicious software regardless of security updating.

> *“...Social engineering can trick the user into installing malicious software regardless of security updating.”*

Figure 25. *Operating system versions of computers cleaned by the MSRT in 1H06 and 2H06*



Prevalence by Locale

The MSRT is available in 24 different languages. The data in Figure 26 compares the top 15 of those languages by operating system locale (or language) for computers that have been cleaned by the MSRT in 1H06 and 2H06. Therefore, note that locale is not necessarily indicative of geographical location. For example, installation of operating systems using the English (U.S.) locale is fairly popular in other countries around the world.

The first two charts in Figure 26 show that a high percentage of the computers cleaned have an English language operating system. This metric is deceptive because, as noted above, it can be expected that a large number of the computers on which the MSRT is run have an English language operating system installed. To take this into account, the computers cleaned can be normalized by the execution percentage of a locale, similar to the normalization of operating system use performed for Figure 25.

The normalization formula used is as follows:

$$\text{Normalized disinfections}_{\text{Locale}} = \text{Disinfections}_{\text{Locale}} \;/\; \text{Execution Percentage}_{\text{Locale}}$$

The result of this normalization is shown in the 1H06 (normalized) chart in Figure 26, in which the normalization process has distributed the disinfections more equally across most locales. In other words, when the values are normalized, the removal of all malware by the MSRT is spread across all Windows locales, including English.

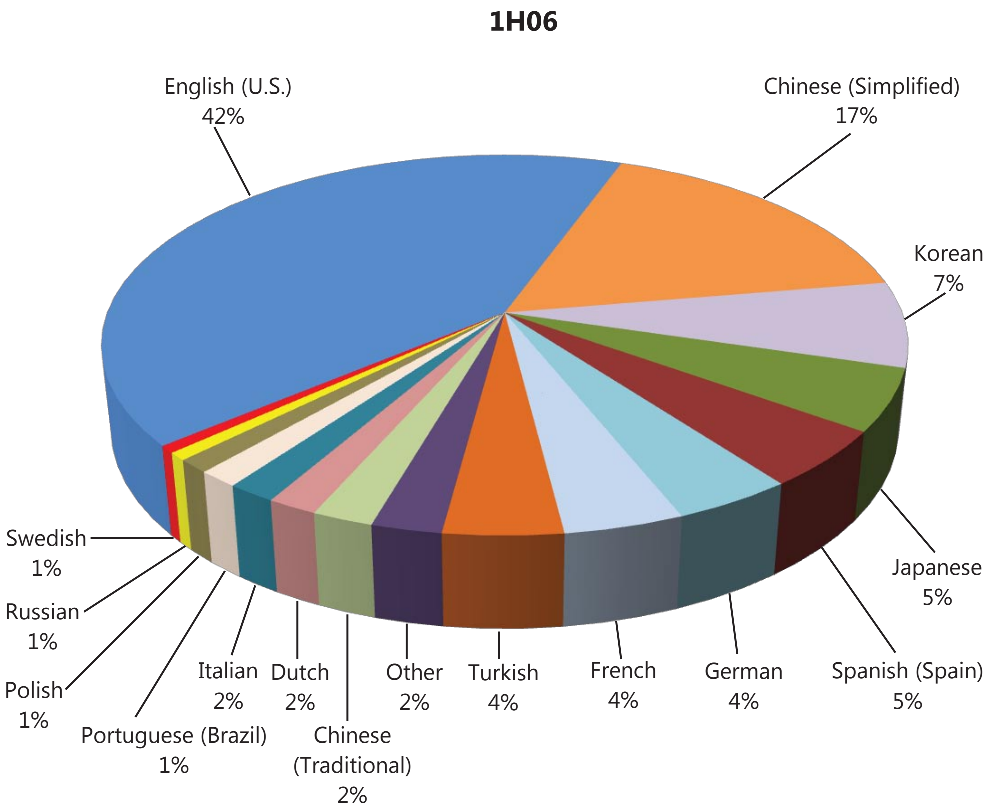
Data Highlights

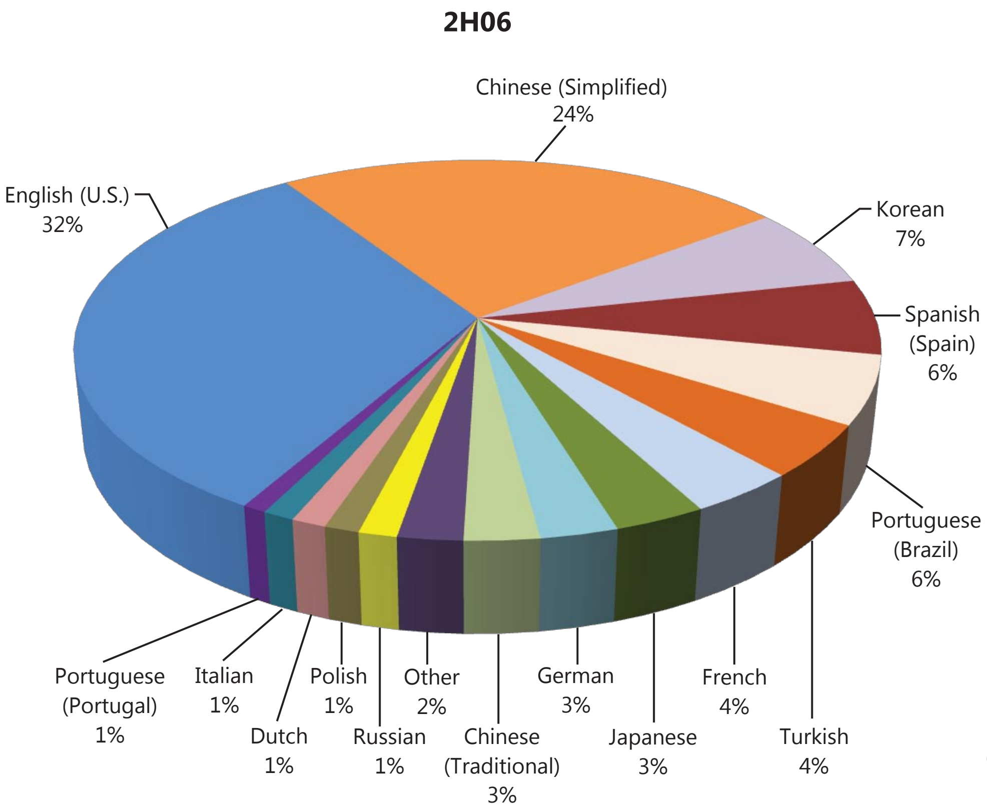
Using the normalized data, the Turkish version of Windows tends to be more consistently infected with the malware families than any other Windows locale. The two Portuguese versions of Windows were second and fourth in the number of MSRT detections among the different Windows locales. This is a result of the prevalence of password stealers and keyloggers associated with the Win32/Banker and Win32/Bancos families, which were added to the MSRT in August 2006 and September 2006. These two families predominantly use the Portuguese language to target users of Brazilian banks.

The MSRT also found proportionally more malware on the Chinese and Russian versions of Windows. This may be a result of the increased activity of malware authors in those countries or perhaps because of different levels of deployment of security products, such as antivirus products, in different regions around the world.

Other countries, such as Japan, became less infected with malware compared to the first half of the year. For example, the number of Japanese computers that were cleaned had decreased by 30 percent. This result can be attributed to the 55-percent decrease in the number of detections of the Win32/Antinny worm, which has spread almost exclusively in Japan.

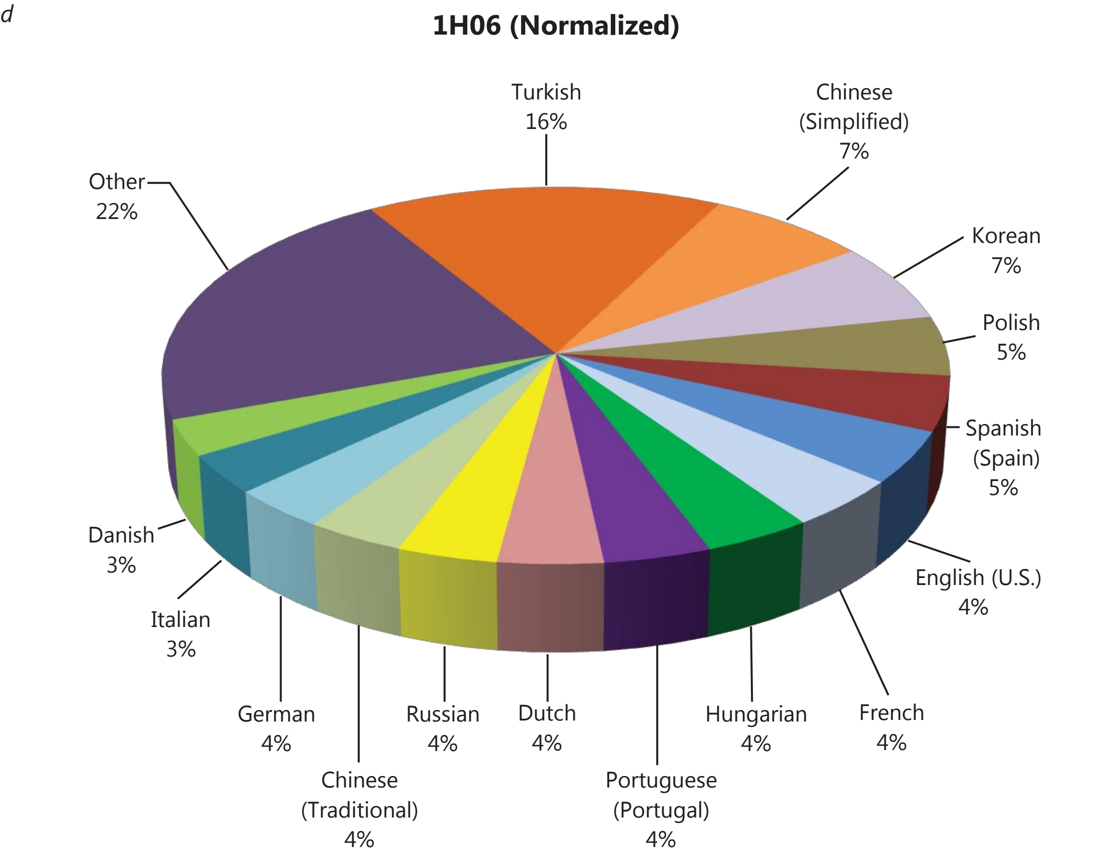
__Figure 26.__ Locales of computers cleaned by the MSRT

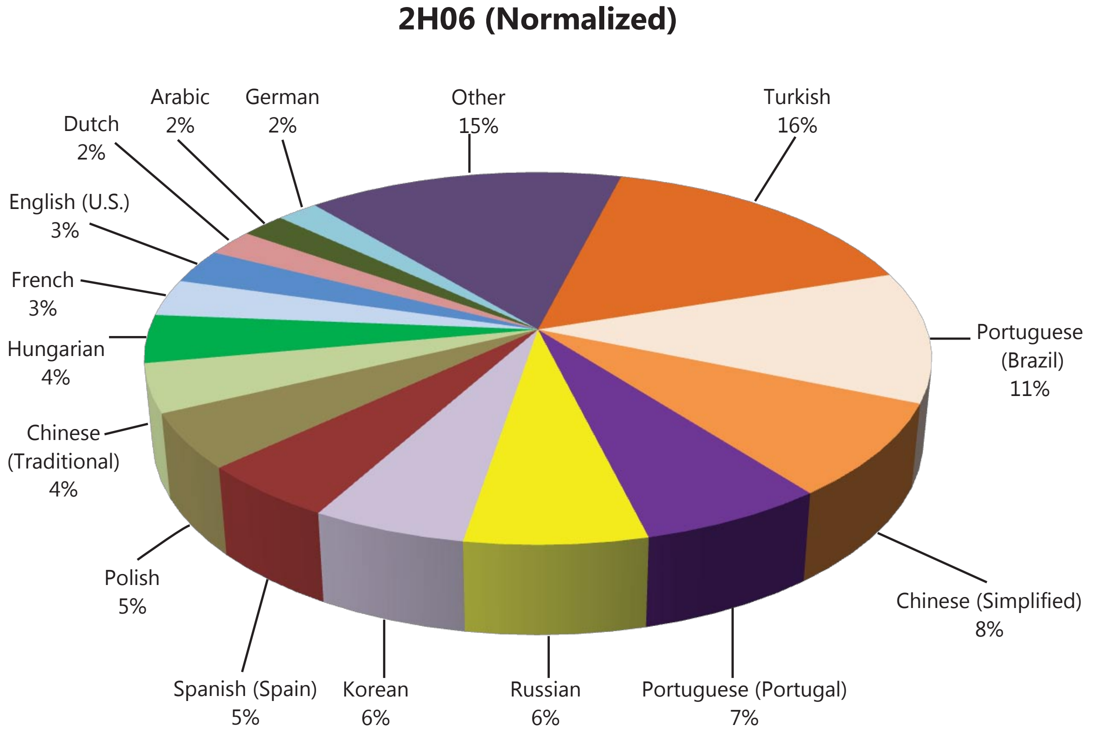




Continued on next page...

Figure 26. *Continued*





Infected Message Prevalence

The final set of malicious software prevalence data discussed in this section of the report relates to the number of infected messages caught by Microsoft Exchange Hosted Services (EHS) filtering during 2H06. EHS showed a 17-percent increase in infected e-mails blocked in 2H06 over 1H06, as shown in Figure 27.

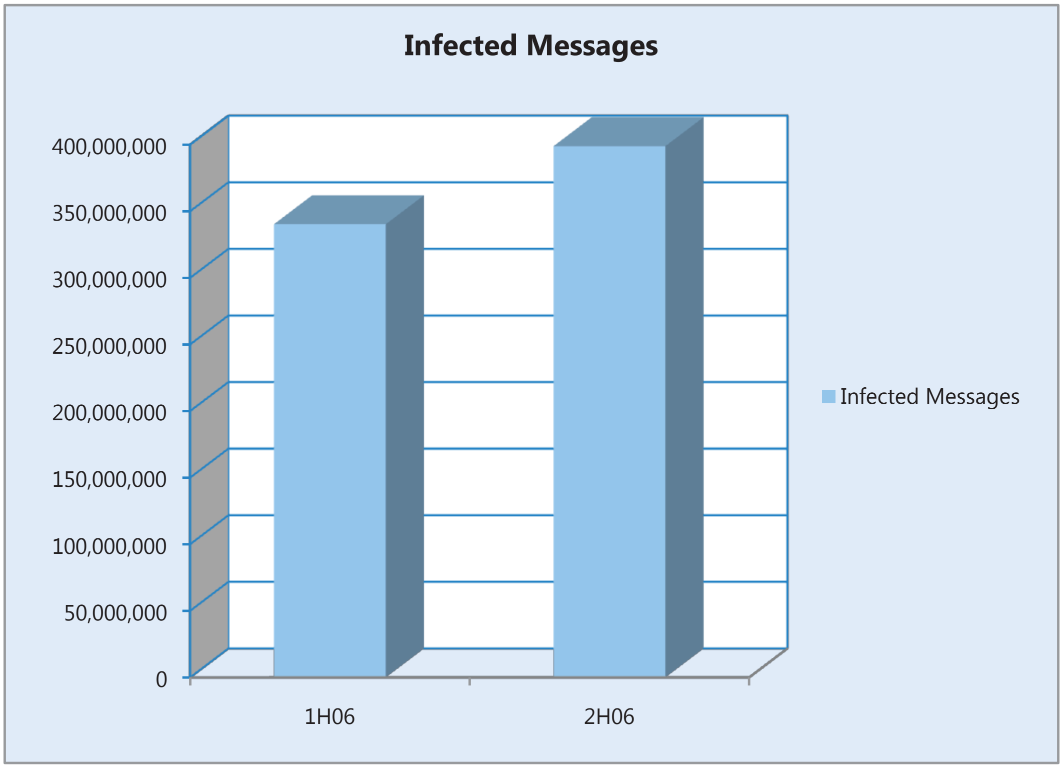
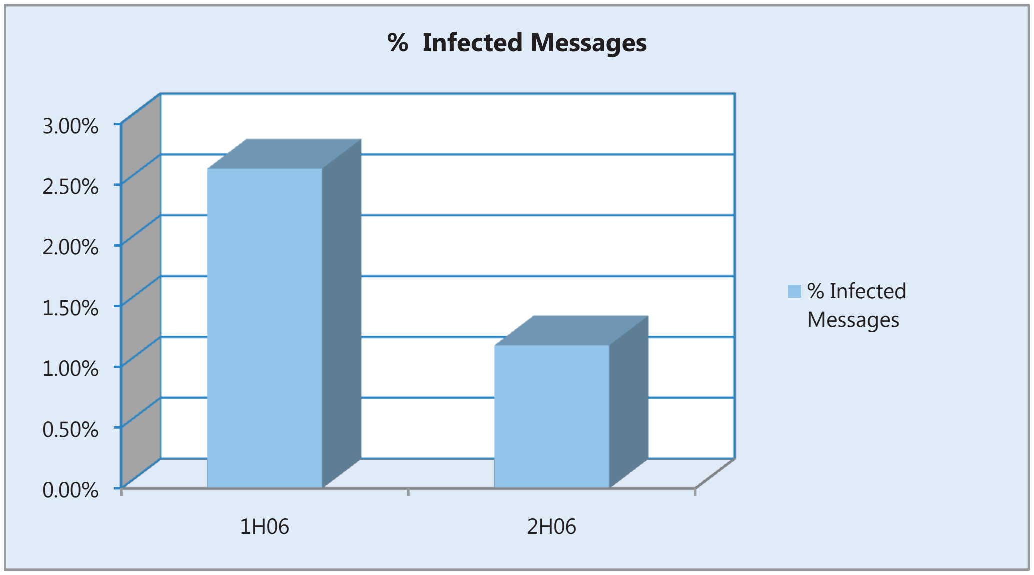


Figure 27. *Infected messages caught by Microsoft Exchange Hosted Services in 2006*

During 2006, the number of scanned mails increased by 162 percent, which means that the percentage of infected e-mail actually went down. Figure 28 shows the percentage of infected e-mail relative to the scanned traffic.

Figure 28. *Percentage of infected messages caught by Exchange Hosted Services during 2006*



This downward trend is further emphasized when looking at monthly data (Figure 29). January 2006 showed a 9.4-percent rate of infected e-mail (during the period that marked the end of the Win32/Sober.Z outbreak), so it was *not included* to allow easier observation of the trend. This trend is surprising given the several e-mail-based outbreaks in 2006 caused by malware families, such as Win32/Stration. The trend might be explained by the fact that EHS uses additional filtering phases before it applies its virus filtering. Also, this shows again that there is not always a clear correlation between the prevalence of infected e-mail and infected computers.

Figure 29. *Percentage of infected messages caught by Exchange Hosted Services between February 2006 and December 2006*

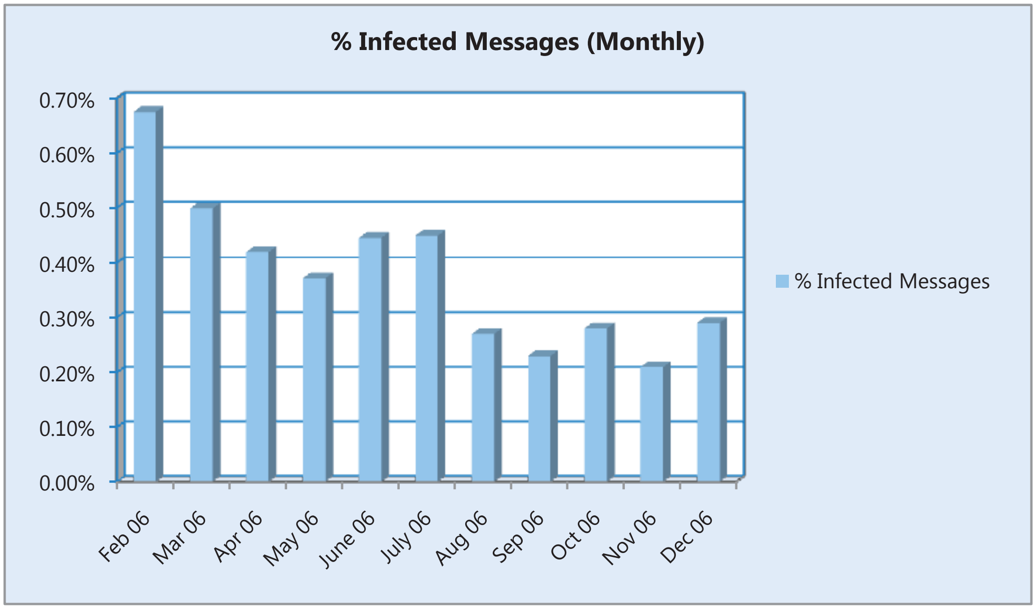


Figure 30 lists the outbreaks detected by EHS with over 1 million infected mails in one month per malware threat. The percentages were calculated by summing up the detection numbers for variants from the same malware family from the top 10 detections for every month and then calculating the percentage by dividing by the total number of infected mails during that month. As already discussed, the Win32/Sober worm sent an unusually high number of e-mail towards the end of 2H05 and January 2006, and then stopped. Additionally, years-old mass-mailer worms, such as Win32/Netsky, Win32/Mytob, and Win32/Bagle, still continue to spread by e-mail. However, along with these old families, year 2006 has also brought the new prolific mass mailers Win32/Tibs and Win32/Stration, both of which emerged during the last quarter of the year. Detections for phishing e-mail were also high, accounting for up to 30 percent of all infected e-mail detected by EHS.

Month	Malware Family	% Infected Mails for That Month
Jan	Win32/Sober	92.40%
	HTML.Bayfraud	1.50%
	Wn32/Netsky	0.80%
	Win32/Mytob	0.80%
	HTML.Iframe	0.70%
	Win32/Mywife	0.60%
Feb	Win32/Bagle	25.00%
	Win32/Mywife	12.50%
Mar	Win32/Mywife	15.30%
	Win32/Netsky	12.90%
Apr	Win32/Mywife	16.10%
May	Win32/Mywife	13.70%
	Win32/Netsky	13.70%
Jun	HTML.Fraud	37.70%
	Win32/Bagle	9.80%
Jul	HTML.Bankfraud	31.00%
	Win32/Bagle	14.60%
	Win32/Netsky	8.70%
Aug	HTML.Bankfraud	27.80%
	Win32/Bagle	15.90%
Sep	Win32/Bagle	18.90%
	HTML.Bankfraud	15.90%
Oct	Win32/Stration	22.20%
	HTML.Bankfraud	19.40%
	Win32/Bagle	10.20%
Nov	Win32/Stration	38.90%
Dec	Win32/Tibs	50.50%
	Win32/Stration	11.90%
	HTML.Bankfraud	8.60%

Figure 30. *Malware families that caused outbreaks with over 1 million infected mails per month*

Potentially Unwanted Software

This section describes the software detected and removed by the Microsoft Windows Defender component of Windows Vista, Windows XP, and Windows Server 2003 during the period between July 1, 2006, and December 31, 2006. It includes an analysis of the categories of potentially unwanted software removed by Microsoft Windows Defender and a separate discussion of rogue (false) security programs.

To understand this data, it is important to remember two things:

1. Windows Defender assigns each potentially unwanted software program an alert rating—Low, Medium, High, or Severe.
2. Each software program has also been assigned a default recommended action from the following list of possible actions:
    - **Ignore:** Users should ignore the alert for the current session.
    - **Ignore Always:** Users should ignore the alert from that point forward, even if the software is seen again.
    - **Prompt:** Users must make a decision about what to do with the software.
    - **Quarantine:** This option removes the software in such a way that it can be restored at a later point.
    - **Remove:** This option removes the software from the system. Software rated with an alert level of High or Severe is automatically removed during scheduled scans.

Users make choices about what to do about potentially unwanted software for different reasons, so it is important not to draw unwarranted conclusions about their intention. For instance, when users choose **Remove**, it usually indicates a clear, active choice that the individual does not want the software present on their computer, while choosing **Ignore Always** usually means that the person wants to keep the software.

Users choose **Ignore**, however, for a variety of reasons. For example, they might be confused by the choices, they might want to defer the action to a more convenient time, or they might want to spend more time evaluating the software before making a decision.

Windows Defender Arrives

During the second half of 2006, four significant milestones were achieved for Windows Defender:

1. The standalone version of Windows Defender moved out of the beta phase and into full general release on October 23, 2006.
2. Localized versions of Windows Defender in German and Japanese languages were also made available on October 23, 2006.
3. Windows Vista incorporated Windows Defender as a default component of the operating system that was released as part of the Windows Vista Beta program.
4. Windows Vista (with the Windows Vista version of Windows Defender) moved out of the beta phase and into release for the enterprise customer segment. The consumer release of Windows Vista also contains Windows Defender, but did not occur during the period covered by this report. Windows Vista will be discussed in more detail in a future report.

We identify these milestones because they have an impact on data presented in this report, and should be considered when attempting to make comparisons between periods, regions, or operating system versions.

Windows Defender is available, at no extra cost, to licensed users of Windows Vista, Windows XP, and Windows Server 2003. As a result, the client base of Windows Defender has increased in both size and geographic spread with each of these release milestones, as more language versions are released and as the product ended its beta period. As a corollary to the increase in distribution, an increase in available telemetry data has also occurred.

Software Detected by Windows Defender

Overall, more than 38 million pieces of potentially unwanted software were detected by Windows Defender between July 1, 2006, and December 31, 2006. Over 20 million of the detected software items were selected for removal, and Windows Defender customers chose to remove this potentially unwanted software an average of 53.3 percent of the time.

Figure 31 lists the top 25 programs detected by Windows Defender, ranked by percentile, according to the number of instances of removal at the time that the potentially unwanted software was identified.

Rank	Software Name	Category	% Remove	% Quarantine	% Ignore Always	% Ignore
1	TVMediaDisplay	Adware	98.7%	0.8%	0.0%	0.5%
2	BlockChecker	Adware	97.4%	0.9%	0.1%	1.6%
3	Monnet	Trojan Downloader	89.0%	0.2%	0.0%	10.8%
4	Look2Me	Spyware	88.0%	0.4%	0.0%	11.7%
5	Zlob *	Trojan Downloader	82.1%	1.0%	0.0%	16.9%
6	SurfSideKick	Adware	80.5%	0.5%	0.0%	19.0%
7	C2.Lop	Spyware	75.7%	1.4%	0.0%	22.9%
8	NewDotNet	Adware	73.6%	3.1%	0.1%	23.2%
9	Altnet P2P Networking	Potentially Unwanted Software	70.9%	0.8%	0.6%	27.7%
10	CMDService	Adware	59.6%	0.2%	0.0%	40.1%
11	180Solutions.WebInstaller *	Adware	49.5%	0.9%	0.2%	49.3%
12	WhenU.SaveNow	Adware	47.3%	1.3%	0.5%	51.0%
13	Altnet	Adware	45.7%	1.0%	0.4%	52.9%
14	CnsMin	Spyware	44.4%	1.8%	0.2%	53.7%
15	KaZaA	Software Bundler	41.1%	0.8%	5.1%	53.0%
16	PowerRegScheduler	Potentially Unwanted Software	40.2%	2.6%	1.2%	56.0%
17	Need2FindBar	Potentially Unwanted Software	37.9%	0.6%	0.2%	61.3%
18	SeekmoSearchAssistant *	Adware	34.2%	0.5%	0.2%	65.1%
19	RXToolbar*	Monitoring Software	32.6%	0.6%	0.1%	66.7%
20	BearShare	Software Bundler	30.0%	0.5%	17.7%	51.7%
21	Zango.SearchAssistant	Adware	28.8%	0.2%	0.1%	70.8%
22	Hotbar	Adware	27.7%	0.9%	0.3%	71.2%
23	RealVNC *	Remote Control Software	9.3%	0.5%	14.9%	75.2%
24	RServer *	Remote Control Software	7.4%	0.4%	29.6%	62.6%
25	Exploit:Win32/Wmfap *	Exploit	7.2%	56.1%	0.1%	36.7%

Figure 31. *Top 25 software programs detected by Windows Defender for 2H06 .* Note: *An entry marked with an asterisk (*) represents a new entry into the top 25.*

During this period, the top 25 software programs (selected by number of detections and subsequently ranked in Figure 31 by frequency of removals) account for more than 56 percent of all removals among thousands of families of potentially unwanted software that Windows Defender can detect and remove.

While many of the programs identified by Windows Defender are clearly unwanted by a majority of people (as illustrated by a high **% Remove** figure), some appear to have a value proposition that compels certain individuals to keep the programs. For example, the remote control software Real VNC receives a relatively high **% Ignore Always** rate of 14.9 percent from users, compared to the 0.0 percent figure received by the Look2Me spyware. This indicates that many users are aware of the nature of this remote control software and are still willing to accept it because of its perceived value, whereas they are not willing to accept identified spyware. Contrasting this, we can also see that nearly 10 percent of users choose to remove or quarantine the software, in all likelihood because they were not the person who installed the software.

> ***"The goal of Windows Defender is to provide individuals with visibility and control over what is running on their computers."***

Windows Defender allows individual users to make their own decisions about whether to keep or remove a piece of identified software. In some cases, an individual will choose to remove or quarantine the item. In others, an individual may choose to always ignore the notification. These active choices represent individual, personal decisions. The goal of Windows Defender is to provide individuals with visibility and control over what is running on their computers.

Because the data does not make it possible to infer an individual's intentions when he or she chose to remove or not remove a piece of software, we encourage you to consider the following questions:

1. Was the installation attempt intentional, an error, or the result of a covert software action?
2. Was the individual aware of the true nature of this software program and its behaviors prior to starting the installation?

We can make one final observation from the data behind Figure 31 that provides us with an insight into the motivation behind the creation of the potentially unwanted software. It is clear that the vast majority of these software programs are generating money, either directly or indirectly, for their developers. While the amounts involved are unknown, it can be assumed that there is enough potential profit to motivate both existing and new developers to create new and updated potentially unwanted software programs for the foreseeable future.

Categories of Potentially Unwanted Software

Windows Defender identifies potentially unwanted software based on specific behaviors. Software exhibiting those behaviors typically falls into one or more of the categories shown in Figure 32.

Figure 32. *Potentially unwanted software categories*

Category	Description
Adware	A program that displays advertisements. While some adware can be beneficial by subsidizing a program or service, other adware programs may display advertisements without adequate consent.
Backdoor	A program that listens on specific port(s) and waits for commands from an unauthorized individual.
Browser modifier	A program that changes browser settings, such as the home page, without adequate consent. Also includes browser hijackers.
Dialer	A program that uses the computer's modem to generate unauthorized telephone charges.
Exploit	Malicious software which attempts to exploit one or more vulnerabilities.
Joke program	Programs that are usually pretending to have a Trojan functionality (for example, pretending to delete files or format disks).
Monitoring software	A program that monitors activity, such as keystrokes, or captures screen images. It also includes network sniffing software. This usually applies to commercially available software.
Password stealer	Malicious software whose primary purpose is to steal passwords.
Potentially unwanted software	A program with potentially unwanted behavior that is brought to the user's attention for review. This behavior may impact the user's privacy, security, or computing experience.
Remote control software	A program that provides access to a computer from a remote location. These programs are often installed by the computer owner or administrator, and are only a risk if unexpected.
Settings modifier	A program that changes computer settings with or without user's knowledge.
Software bundler	A program that installs other potentially unwanted software, such as adware or spyware. The license agreement of the bundling program may require these other components in order to function.
Spyware	A program that collects information, such as the Web sites a user visits, without adequate consent. Installation may be without prominent notice or without user's knowledge.
Tool	This includes tools used by malware authors or hackers that can be legitimate depending on the context of its usage.
Trojan	A program which appears to be legitimate but is designed to have unwanted side effects on the computer on which the program is loaded.
Trojan downloader	A Trojan application whose primary purpose is the downloading of additional unwanted and/or malicious software.
Trojan dropper	A Trojan application which drops other components in a manner similar to an installer.

Microsoft Security Research & Response uses these categories to help identify and organize the potentially unwanted software that is included in the definition files used by Windows Defender.

Prevalence of Detection by Category

There are varying degrees of prevalence between each category. Figure 33 lists the top 10 categories during 2006, ranked by the total number of detections.

Rank	Category	Total 1H06	Total 2H06	% Change
1	Adware	10,471,061	16,709,368	+59.6%
2	Software bundler	2,084,164	3,740,722	+79.5%
3	Spyware	2,185,191	3,496,078	+60.0%
4	Remote control software	735,638	2,775,996	+277.4%
5	Trojan downloader	1,152,761	2,737,200	+137.4%
6	Potentially unwanted software	1,335,412	2,561,809	+91.8%
7	Browser modifier	747,266	1,359,098	+81.9%
8	Trojan	858,953	1,352,291	+57.4%
9	Settings modifier	911,026	1,130,677	+24.1%
10	Monitoring software	212,547	500,737	+135.6%

Figure 33. *Top 10 categories of potentially unwanted software*

You can see from these figures that the adware category is still, by far, the most prevalent category of potentially unwanted software in circulation today by volume. However, remote control software and monitoring software have both shown increased prevalence during this period. This is due, largely, to increased criminal use of this potentially unwanted software in order to commit theft of data or to control large numbers of computer systems—techniques perceived as more lucrative than those methods more commonly utilized in 1H06.

Additionally, the **% Change** column in Figure 33 illustrates that an increase in potentially unwanted software detection has been seen across all of the top ten categories. However, if you are planning to use these numbers for trending purposes, it is important to understand that they are affected by a variety of factors, specifically:

- The period covered in 1H06 was not a full half-year; Windows Defender Beta 2 was released on April 11, 2006, so the figures for 1H06 only cover from that date through June 30, 2006.
- The standalone version of Windows Defender moved out of beta during this period.
- The software detected by Windows Defender is continually increasing.

- The Microsoft Windows Vista Beta (with Windows Defender) was initially released only to testers. The final version of Windows Vista was made available to enterprise customers toward the end of this period.
- Windows Defender is now available in languages other than English (which was not the case in 1H06), and this has helped to increase the number of computers that are now running it.

While it is safe to say that potentially unwanted software is still a major problem for computer users worldwide, it would not be fair to use the **% Change** figure as a true representation of any increase in any particular category between the first and second halves of 2006. What is more notable is that the largest increases are seen in categories that represent the greatest impact to the privacy and security of the individual.

Geographic Data

Because of the different methods used by the purveyors of potentially unwanted software in different areas of the world, we see differences, in some cases significant differences, in the prevalence of a particular item when comparing between countries, regions, or by common language. These differences are a result of the methods by which the software in question is disseminated. For example, software that is distributed along with Web content often advertises itself on various Web sites. These Web sites, in turn, have a particular target demographic that frequents the site, resulting in a selection bias.

> *"Windows Defender is now available in languages other than English... and this has helped to increase the number of computers that are now running it."*

Local language can also play a part in the bias. For example, software that bundles with additional, potentially unwanted software may not be prevalent in a particular area because a local language version has not been developed or because there is a local language substitute that is more popular.

A final factor that can explain the prevalence of potentially unwanted software in a particular geographic region is that the distributors have specifically targeted that region, using local cultural or social motivators. For example, if a sporting event generates a high level of interest in a particular region, a social engineering attack can use this information to attempt to exploit individuals who are interested in that event. This type of attack will generate a spike in detection rates in that particular region.

The countries included in Figure 34 represent 94.1 percent of removals and 93.5 percent of detections recorded during 1H06 and 2H06. They are listed in order of the number of total detected items.

		1H 2006	2H 2006	%
Rank	Country	Detections	Detections	Change
1	United States	8,160,414	21,958,236	+169.1%
2	United Kingdom	1,210,678	3,521,976	+190.9%
3	Canada	503,536	1,424,370	+182.9%
4	Netherlands	300,449	1,149,623	+282.6%
5	Australia	299,817	860,404	+187.0%
6	France	228,545	742,464	+224.9%
7	Brazil	160,404	617,479	+285.0%
8	Germany	119,606	568,083	+375.0%
9	China	140,919	527,055	+274.0%
10	Spain	126,325	451,923	+257.7%
11	Belgium	106,832	428,608	+301.2%
12	Italy	91,044	422,369	+363.9%
13	Portugal	139,796	384,329	+174.9%
14	Turkey	101,004	332,041	+228.7%
15	Mexico	106,679	325,638	+205.3%
16	Denmark	71,028	276,232	+288.9%
17	Norway	82,837	258,998	+212.7%
18	Japan	52,622	256,760	+387.9%
19	Sweden	79,524	255,104	+320.8%
20	Poland	44,179	204,821	+363.6%
21	Hong Kong S.A.R.	45,346	155,325	+242.5%
22	Switzerland	43,451	138,343	+218.4%
23	Taiwan	37,256	133,943	+259.5%
24	Singapore	47,567	128,485	+170.1%
25	New Zealand	42,239	121,957	+188.7%

Figure 34. *Top 25 countries ranked by total number of detected items*

Again, the percentage increases in detections for the second half of 2006 are significantly higher than those reported in the January–June 2006 *Microsoft Security Intelligence Report*. The same factors that were responsible for this increase in the previous section of this report are responsible here as well—a longer detection period, Windows Defender moving out of beta, new software added to the definition files, the addition of the Windows Vista version of Windows Defender, and the increased customer install base.

However, even taking these factors into account, the data shows a worldwide, upward trend in detections of potentially unwanted software. This increase also shows that the developers of this software are still finding effective methods to distribute their software worldwide.

A Focus on Rogue Security Software

With the arrival of the always-on, broadband-connected home computer came a dramatic increase in new services and features that home users could access. Unfortunately, this also led to an explosion in malicious and potentially unwanted software attempting to obtain personal information from these same individuals. When combined with the myriad of new antispyware and antivirus products on the market combating this problem, and in an effort to get out from under the scrutiny of those same products, the developers of some potentially unwanted software changed tactics. They switched from overt, drive-by, and other non-consensual installation practices, to the use of social engineering designed to entice people into paying for "protection".

These products appear under a variety of names and produce a variety of results for the end user, ranging from limited or no detection capability, coupled with a fraudulent request to pay for a "full" version, to outright malicious behavior, such as installing malicious software without the user's consent in order to give the product something to detect. In many cases, the people behind such software would attempt to get the infected individual to pay them for removal of purported infections using fraud and social engineering.

These questionable products became known as rogue antivirus or antispyware software, which we are collectively referring to as *rogue security software*. Coupled with the massive increase in e-mail-based social engineering attacks, this rogue security software has served to erode the trust that users had in their computers.

Even with scanning and detection software that targets specific, objective behavioral criteria, it is still necessary to educate individual computer users so they do not fall prey to tactics of social engineering and fraud. We will only see significant relief from these rogue security software products when everyone who uses a computer understands how an e-mail, alert, or software program can be used to trick them.

Figure 35 provides a list of the most prevalent of these rogue programs, ordered by number of reported instances.

Figure 35. *Rogue security software*

Software Name	Alert Level	% Remove	% Quarantine	% Ignore	% Ignore Always
ClickSpring.PuritySCAN	High	79.3%	2.2%	18.4%	0.0%
SpySheriff	High	88.8%	0.8%	10.3%	0.1%
WinSoftware.WinAntiVirus	Medium	30.6%	14.2%	55.0%	0.2%
ClickSpring.PuritySCAN.Downloader	High	73.7%	0.7%	25.6%	0.0%
SpywareQuake	Medium	56.6%	3.6%	39.6%	0.1%
WinSoftware.WinAntiSpyware	Medium	37.6%	27.7%	31.3%	3.3%
TrustCleaner	High	89.2%	0.3%	10.4%	0.1%
SpyAxe	High	83.1%	1.6%	15.2%	0.2%
SpywareStrike	High	87.4%	1.8%	10.7%	0.2%
SpyFalcon	High	87.1%	2.1%	10.5%	0.3%
AntiSpywareSoldier	Severe	76.3%	0.1%	23.2%	0.4%
VirusBurst	High	89.3%	1.3%	9.2%	0.2%
Privacy Champion	Medium	42.4%	9.7%	47.9%	0.1%
WareOut	High	89.4%	6.3%	4.2%	0.1%
AntivirusGold	High	90.4%	0.5%	8.8%	0.3%
AlfaCleaner	High	92.5%	0.7%	6.8%	0.1%
PSGuard	High	89.4%	3.1%	7.4%	0.2%
WinHound	High	91.9%	3.5%	4.4%	0.2%

Rogue security software uses a number of different techniques to attempt to trick the user. To illustrate some of these techniques, the following section provides some examples of this rogue software, highlighting the techniques used to trick the individual into installing the software and obtain money from them.

It should be clear to the attentive reader that software in this group is very different from some of the other categories, such as adware and remote control software. One telling difference is the stark contrast in the **Ignore Always** category. As mentioned earlier, **Ignore Always** is a clear choice that users can make in Windows Defender that demonstrates their active intent to keep the software in question on their computer.

In Figure 35, when we compare the percentages in the **% Ignore Always** category with those same numbers in Figure 31, for software such as BearShare or KaZaA, we see significant differences in the frequency in which people actively seek to retain the software when it is brought to their attention. From this data we can infer that users, when faced with software from this group, do not actively choose to keep the software when prompted to take action on these products. The percentage of individuals who do choose **Ignore Always** are likely to have fallen for the social engineering aspects of the warnings or are related directly to those developing and distributing the software.

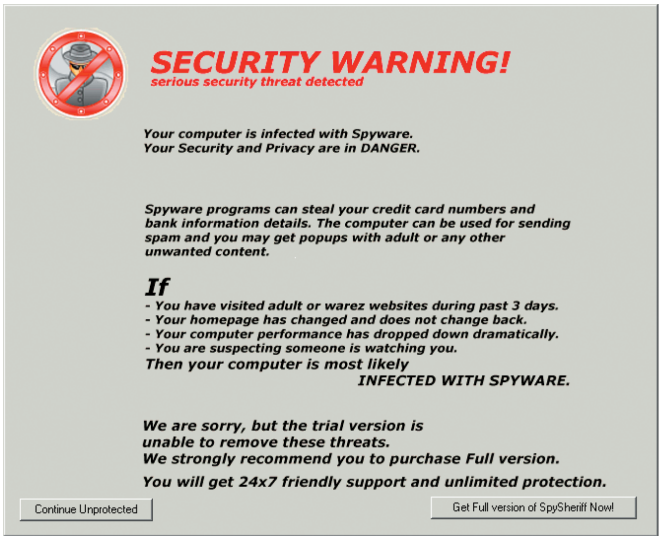
Changing Names

SpySheriff is the detection name used by Microsoft Security Research & Response for several related products, including the original SpySheriff, as well as the following:

- BraveSentry
- DiaRemover
- MalwareAlarm
- Mr. Antispy
- PestTrap
- PestWiper
- SpyTrooper
- SpyDemolisher
- SpyMarshall

Figure 36 illustrates two screen shots of warning messages used by different members of this family to attempt to get the computer user to pay for the product.

Figure 36. *Examples of false infection messages provided by SpySheriff and PestTrap*



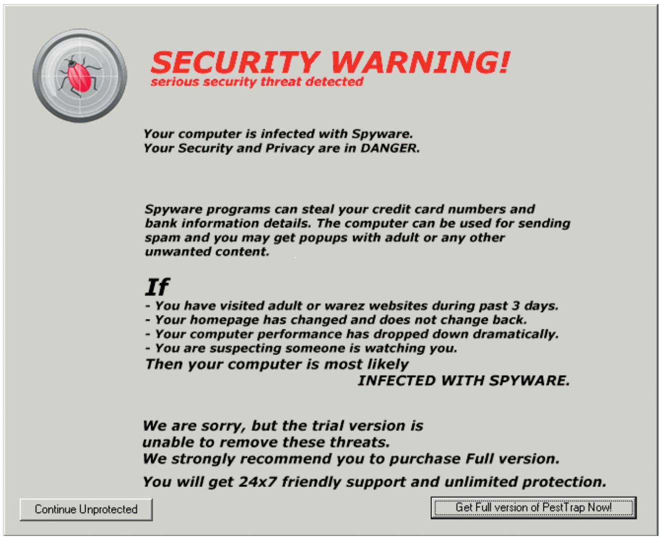
SECURITY WARNING!
serious security threat detected

Your computer is infected with Spyware.
Your Security and Privacy are in DANGER.

Spyware programs can steal your credit card numbers and bank information details. The computer can be used for sending spam and you may get popups with adult or any other unwanted content.

If
- You have visited adult or warez websites during past 3 days.
- Your homepage has changed and does not change back.
- Your computer performance has dropped down dramatically.
- You are suspecting someone is watching you.
Then your computer is most likely
INFECTED WITH SPYWARE.

We are sorry, but the trial version is unable to remove these threats.
We strongly recommend you to purchase Full version.
You will get 24x7 friendly support and unlimited protection.



SECURITY WARNING!
serious security threat detected

Your computer is infected with Spyware.
Your Security and Privacy are in DANGER.

Spyware programs can steal your credit card numbers and bank information details. The computer can be used for sending spam and you may get popups with adult or any other unwanted content.

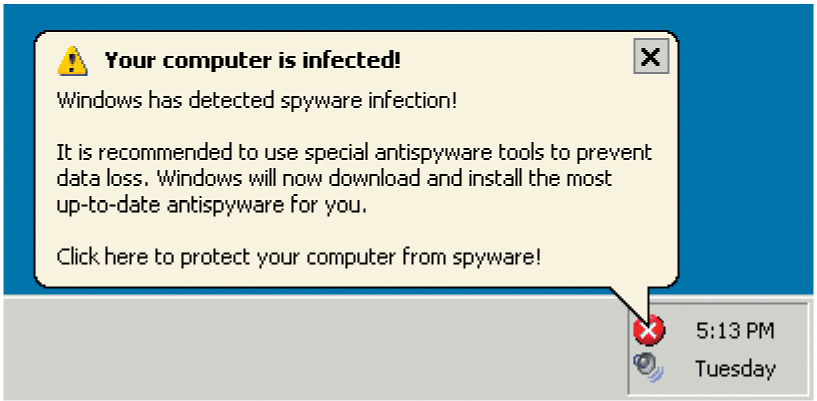
If
- You have visited adult or warez websites during past 3 days.
- Your homepage has changed and does not change back.
- Your computer performance has dropped down dramatically.
- You are suspecting someone is watching you.
Then your computer is most likely
INFECTED WITH SPYWARE.

We are sorry, but the trial version is unable to remove these threats.
We strongly recommend you to purchase Full version.
You will get 24x7 friendly support and unlimited protection.

As you can see, they are clearly based on the same original product and rely on the social engineering techniques of fear and the use of an authoritative voice.

Using Trojans

The SpySheriff family has used the Trojan downloader referred to as Win32/Renos to help trick individuals into installing SpySheriff rogue security software. Win32/Renos is delivered through malicious Web sites. If it is installed, it displays an infection alert that, when clicked, downloads the rogue security software. In some cases, the false Win32/Renos alert claims that Microsoft Windows is the source of this alert (see Figure 37).



Your computer is infected!

Windows has detected spyware infection!

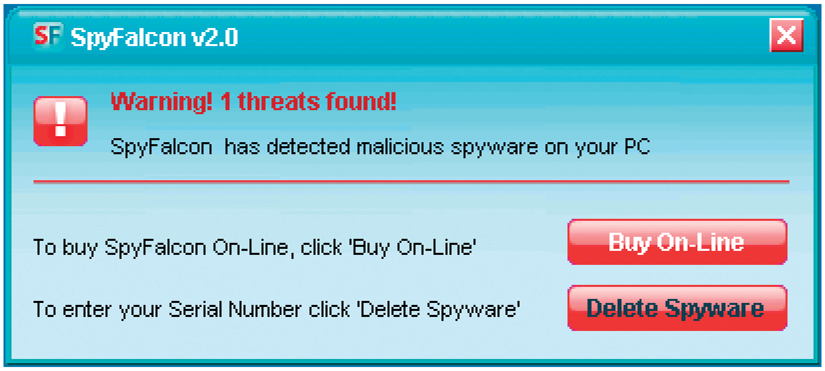
It is recommended to use special antispyware tools to prevent data loss. Windows will now download and install the most up-to-date antispyware for you.

Click here to protect your computer from spyware!

Figure 37. *Example of a false infection message provided by Win32/Renos*

SpyFalcon has been linked with both Win32/Renos and the Win32/Zlob families of Trojan programs. Variants of the Win32/Zlob family can modify Microsoft Internet Explorer settings, redirect the default Internet search page and home page, and attempt to download and execute malicious software, such as SpyFalcon, from the Internet.

Once SpyFalcon has been installed, either with or without user consent, it behaves similarly to SpySheriff in that it typically displays a dialog box prompting the user to purchase a version of the software in order to remove spyware that it purports to have found on the computer, as shown in Figure 38.



SF SpyFalcon v2.0

Warning! 1 threats found!

SpyFalcon has detected malicious spyware on your PC

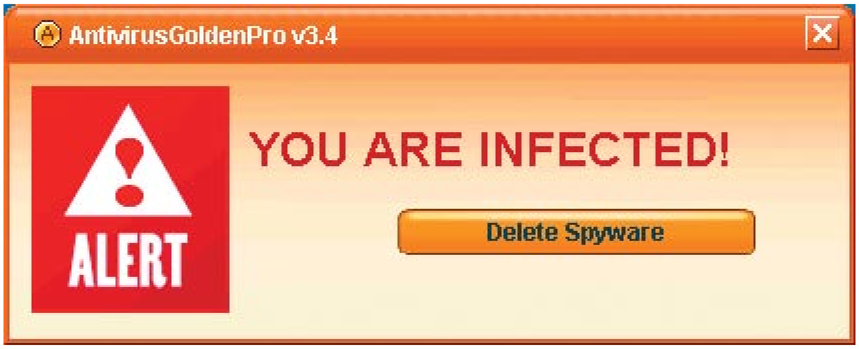
To buy SpyFalcon On-Line, click 'Buy On-Line'

To enter your Serial Number click 'Delete Spyware'

Figure 38. *Example of a false infection message provided by the SpyFalcon family of rogue security software*

Scare Tactics

The Antivirus Golden rogue security software (also known as *AntiVirus Gold*, *AVGold*, and *SpyAxe*) takes these warnings to a higher imperative. Figure 39 shows an example of the overt scare tactics used by this rogue security software to frighten an individual into paying money to the distributors.



YOU ARE INFECTED!

Figure 39. *Example of a false infection messages provided by AntiVirus Gold*

The Internet-connected world of the twenty-first century has led to an environment that is being exploited by distributors of malicious and potentially unwanted software to trick or scare people into handing over money for false or questionable services. Thanks to Windows Defender and other legitimate antispyware tools, it is becoming harder for distributors of this software to go undetected. However, even legitimate antispyware tools rely on the individual using the computer to understand the nature and source of the warnings before choosing their preferred course of action. Only with continued education and vigilance can we hope to squash the distribution and installation of these unwanted software programs.

Executive Afterword

First surging to prevalence in 2004, backdoor Trojans, password stealers, bots, Trojan downloaders, and droppers continue to be the dominant threats today. These are threats that do not self-replicate, thus the quantities we are seeing speaks to a high level of determination on the part of the attackers. It is the goal of these threats that explains this high level of determination—installing malicious code to steal personal, financial, or confidential information from the impacted user.

These Trojans are facilitated by an ever-expanding net of Internet interaction points. E-mail, once considered the most serious potential infection vector, is now just one of many. So-called "*Web 2.0" technologies*—forums, blog comments, instant messaging, peer-to-peer file sharing, and even online games and social networking sites—provide attackers with even greater opportunity to bypass protective measures and to interact with the user directly.

More and more frequently, this interaction occurs by first infecting and then exploiting the ‘trust relationship’ between shared users of these social interaction sites. Examples of this include injecting malicious links into forum postings and online interactions by equally innocent users.

Even spyware, adware, and potentially unwanted software can no longer be considered a category of threats distinct from the more traditional virus, worm, or Trojan. Increased criminal leveraging of these technologies and loosely policed affiliate programs create a lethal combination that poses a significant threat to users. An example is affiliate programs that surreptitiously sneak credential-stealing code in the Web sites of unsuspecting participants.

The nature of these attacks has evolved the meaning of ‘social engineering’ well beyond that of yesteryear’s e-mail worm. It is no longer a matter of simply avoiding executable file attachments or displaying a certain level of distrust where e-mail is concerned. Now, every avenue of social interaction is vulnerable to these types of attacks—with victims themselves unwittingly playing the role of malicious social engineer.

Protecting the user and preserving a rich Internet experience requires a holistic approach, providing specific protection at every level of interaction. As George touched on in the forward to this report, we must not simply focus on stopping these individual types of threats; additionally we must also focus on developing resilient technologies and initiatives that make these threats impractical for even the most determined criminal, regardless of form or vector.

Technology can also help enable users to respond appropriately to socially engineered attacks, but ultimately social interaction decisions remain in the hands of the user. Increased awareness and education play an important role in meeting this challenge and can help steer the appropriate decision. This commitment to helping the user make wise choices is ultimately an industry challenge that all should rise up to meet.

Certainly the stakes have never been higher than they are today. Malicious code is no longer a prank, and the impact is no longer relegated to the computer. The target is the user, and their finances, credit history, and even their very identity can be placed at risk. Our commitment is to ensure that we protect our customers to the best of our ability and to provide them with the tools necessary to protect themselves.

Sincerely,

Vinny Gullotto
General Manager of Microsoft Security Research & Response
Microsoft Corporation

Conclusion

Thank you for reviewing this second edition of the Microsoft Security Intelligence Report. Through the broad deployment of offerings, such as the Windows Malicious Software Removal Tool and Windows Defender, combined with the in-depth detection capabilities of offerings such as Windows Live OneCare, the Windows Live OneCare safety scanner, Microsoft Exchange Hosted Filtering, Microsoft Forefront for Exchange, and the upcoming Microsoft Forefront Client Security release, Microsoft is committed to providing customers and partners with relevant and accurate data. Future editions of this report will include data from additional sources, as required by the shifting landscape of security threats. To help protect against the threats outlined in this report, Microsoft highly recommends that all customers:

- Check for and apply software updates on an ongoing basis, including updates provided for third-party applications. Windows Vista, Windows XP, and Windows 2000 SP2 users can enable Automatic Updates to help ensure that computers stay up to date with critical operating system and application updates from Microsoft.
- Enable a firewall, such as the Windows Firewall in Microsoft Windows XP Service Pack 2 or the Windows Firewall in Windows Vista.
- Install and maintain an up-to-date antimalware program that provides protection from both malicious and potentially unwanted software. Microsoft offers Windows Live OneCare (currently available) for individuals and the upcoming Microsoft Forefront Client Security for businesses. Other antimalware products can be found at http://www.microsoft.com/athome/security/viruses/wsc/en-us/flist.mspx.

The following five specific suggestions are designed to help protect customers from the key malicious and potentially unwanted software trends. These suggestions are intended mainly for implementation within a corporate environment.

1. Implement the concept of least privilege within your organization. With least privilege, even if malicious or potentially unwanted software is executed within your environment, it is limited to performing non-administrative actions. For example, kernel mode rootkits, which use drivers to affect the operating system, cannot successfully install when run under least privilege.
2. Filter outgoing network traffic to help reduce the likelihood that an attacker could leverage a backdoor Trojan to retrieve sensitive or confidential information from your organization. The Windows Firewall in Windows Vista provides rules-based filtering for both incoming and outgoing traffic.

3. Use an application management system within your organization to help control the programs that end users can run. For example, IT administrators may wish to control the use of certain peer-to-peer (P2P) network software within their organizations because of the high rate of infected files found on these anonymous networks. If possible, the best strategy is to allow only a specific set of applications to run. An application management system can also help prevent users from running adware and other potentially unwanted software.

4. Educate your organization about malicious and potentially unwanted software. In relation to the trends described in this report, there are at least two levels of education:

    - All users should be educated about the danger of social engineering threats, particularly those involving technology-enabled attacks that exploit existing trust relationships. While e-mail is the most frequently discussed, all vectors should be addressed, including social networking sites, forums, instant messaging, and other online venues.

    - IT administrators should educate themselves about the trends and capabilities of malicious software. For example, as rootkit-enabled malware becomes more prevalent, administrators should familiarize themselves with the respective detection tools and techniques to help identify these threats.

5. Consider bolstering existing protection with tools that are available at no charge to help detect and remove some malicious and potentially unwanted software, especially if the cost of purchasing and maintaining an antimalware product is prohibitive to an organization. For example, the MSRT is available at no charge and can easily be scheduled to run each time a computer starts or a user logs on to the system. Note that these tools are not a replacement for up-to-date antimalware and antivirus software. For optimum performance, these tools should be used in combination with an up-to-date antimalware solution, as part of an in-depth strategy of defense against security threats.

Appendix A: Microsoft Antimalware Offerings

Microsoft provides the following antimalware offerings for individual users.

Windows Malicious Software Removal Tool

The Microsoft Windows Malicious Software Removal Tool (MSRT) is designed to help identify and remove specifically targeted, prevalent malware from customer computers, and is available at no charge to licensed Windows users. The main release mechanism of the MSRT is through Windows Update (WU)/Microsoft Update (MU)/Automatic Updates (AU). A version of the tool is also available for download from the Microsoft Download Center. As of December 2006, the tool is capable of detecting and removing 82 different malware families.

The tool does not target spyware or potentially unwanted software. Additionally, the MSRT is not a replacement for an up-to-date antivirus solution because the MSRT specifically targets only a small subset of malware that is determined to be particularly prevalent. Further, the MSRT includes no real-time protection and cannot be used for the prevention of malware.

The MSRT has been available since January 2005 and has a user base of more than 310 million unique computers. During 2H06, the tool was executed 1.8 billion times, which brings the total number of executions to 5.4 billion since January 2005.

A vast majority of the executions of the MSRT are through WU/AU. Because of the broad, automatic nature of this distribution, the customer profile of a typical MSRT user is likely to be varied, although it is assumed that most are home users or small business users because security issues of larger scale are usually handled individually in larger corporations. The MSRT acts a *complement* to other security software—users who execute the tool may or may not have active antimalware products installed on their computers.

For more information, please see http://www.microsoft.com/malwareremove.

Windows Defender

Microsoft acquired Giant Company Software, Inc. in December 2004. Sixteen days after the acquisition, Microsoft released the Microsoft AntiSpyware Beta 1 to help protect Windows customers from spyware and other potentially unwanted software, as a part of its larger initiatives in security and Trustworthy Computing. Following the release of the beta, the Microsoft Security Research & Response team began to enhance the technology, to better integrate it with other Microsoft technologies and platforms, and help ensure its scalability, so that the technology and its infrastructure could support hundreds of millions of users worldwide.

In April 2006, Microsoft released the English-language version of the antispyware product, which was re-named Windows Defender Beta 2, which provided improved capabilities for detection and removal to the more than 14 million beta users. This release also included improvements to the telemetry infrastructure. In May 2006, Microsoft expanded availability of the beta to two additional languages, Japanese and German. As Windows Defender continues to improve, has emerged from beta and adds support for more languages, the customer base has grown to more than 18 million.

> ***"With Windows Defender, Microsoft puts better control and visibility of what runs on a Windows computer into the hands of the computer user."***

The technology, processes, and infrastructure that support Windows Defender Beta 2 also support Windows Live OneCare, Windows Live OneCare safety scanner, and Microsoft Forefront Client Security.

Microsoft is committed to the fight against potentially unwanted software. With Windows Defender, Microsoft puts better control and visibility of what runs on a Windows computer into the hands of the computer user.

We also recognize that technology alone will not address the serious problem of spyware. In addition to our efforts to improve technology, we are working with:

- **Industry groups,** such as the Anti-Spyware Coalition, to better define the problem and the best practices for software development.
- **Legislators and law enforcement** to help ensure that there is a legal framework in which those parties who seek to undermine public trust in computing can be brought to justice.
- **Consumers** to improve the public's overall understanding of safer computing practices.

For more information, please see http://www.microsoft.com/windowsdefender.

Windows Live OneCare

Microsoft introduced Windows Live OneCare to help address the average consumer's challenge of keeping his or her computers protected and maintained in response to ever-changing Internet threats and technologies. Windows Live OneCare can help increase the user's ease of use and peace of mind through its comprehensive, automatic, and self-updating computer care service that continually manages vital computer security and performance maintenance tasks on behalf of the consumer. Offering a simple and hassle-free service to take care of their PCs, Windows Live OneCare helps to minimize customer confusion and raise confidence and peace of mind.

As a service, Windows Live OneCare will continually evolve and provide new features, enhancements, and other additions for its subscriber base. Currently, Windows Live OneCare offers the following feature areas:

- **Protection Plus.** Offers continuous, real-time antivirus monitoring united with antispyware technology and a managed, two-way firewall that helps protect against viruses, worms, Trojans, hackers, and other threats. In addition, Windows Live OneCare activates the Phishing Filter in Internet Explorer® 7 to help detect and block known sites for online ID scams and theft.
- **Performance Plus.** Regularly defragments the computer's hard disk, removes any unnecessary files that can clog the computer, and helps make sure that important security updates from Microsoft are installed efficiently and on time.
- **Backup and Restore.** Regularly copies important files and settings to CD, DVD, external hard disk, locally networked computers, and most USB-connected storage devices.
- **Help Center.** Provides unlimited online and phone support for subscribers.

The Windows Live OneCare subscription service was officially launched in June 2006, and it is now available in 17 markets worldwide. Customers can download the service directly from the Web at http://onecare.live.com or purchase a packaged version from participating retailers worldwide. Windows Live OneCare is a part of the Microsoft Windows Live™ strategy, designed to bring together and enhance the most relevant experiences for consumers across information, relationships, inspiration, and safety. Strongly integrated with security teams across Microsoft, Windows Live OneCare is part of the ongoing commitment of Microsoft to security and Trustworthy Computing, delivering solutions today to help protect customers and to take ongoing care of their PCs.

Windows Live OneCare Safety Scanner

To help support the Windows Live network and a healthier online ecosystem, the Windows Live OneCare safety scanner (found at http://onecare.live.com/scan) is a free, Web-based service that offers individuals quick, on-demand computer health and security scans. Unlike the MSRT, which is designed specifically to remove malware, the Windows Live OneCare safety scanner can address a variety of performance issues related to a user's machine. The full-service scan can check for viruses, spyware, and other potentially unwanted software, and help remove them. The Windows Live OneCare safety scanner can also test for open ports, help delete obsolete files, clean the registry, and run a disk defragmentation. Users can choose to run a complete scan or select one of three distinct scans: Protection, Clean-up, or Tune-up.

The Windows Live OneCare safety scanner is currently available at no charge in 44 markets worldwide. First released as a beta product in November 2005 under the name Windows Live Safety Center, the scanner has performed nearly 18 million scans since its debut. In addition to the Windows Live OneCare safety scanner, the related Web site offers consumer-friendly explanations about online threats and troubleshooting hints for everyday computer issues, including the need for active malware solutions. The Windows Live OneCare safety scanner is not intended as a replacement for always-on antivirus protection, such as Windows Live OneCare. Instead, it provides home users with a one-time computer clean-up and tune-up to help improve computer performance.

Microsoft provides the following antimalware products for business users.

Microsoft Exchange Hosted Filtering

Microsoft Exchange Hosted Filtering is a hosted e-mail security service that helps businesses quarantine or eliminate spam, viruses, and policy-violating e-mail from inbound and outbound e-mail streams. It is one of four enterprise-class services in the Microsoft Exchange Hosted Services (EHS) family, which also includes services for e-mail archiving, e-mail encryption, and e-mail continuity.

Exchange Hosted Filtering operates “in the cloud” (online-only) and is implemented with a simple mail exchange (MX) record configuration change. There is no need to change or modify the existing e-mail infrastructure, or even to install and maintain any new hardware or software. At the core of the Exchange Hosted Filtering service is a distributed network of secure data centers that are located at key sites along the Internet backbone and process more than 10 billion business e-mails a month for more than 5,000 enterprises worldwide.

Exchange Hosted Filtering performs four primary e-mail security functions:

- **Virus protection.** Exchange Hosted Filtering uses multiple antivirus engines that are integrated at the application programming interface level to continually provide critical virus definition updates. Performance is backed by a service level agreement (SLA) that ensures 100-percent blocking of known viruses.

- **Spam protection.** Powered by multiple filtering engines and an around-the-clock team of antispam experts, Exchange Hosted Filtering virtually eliminates spam from inboxes. Performance is backed by an SLA that ensures 95 percent of spam will be filtered and quarantined with no more than 1 in 250,000 messages being misclassified as spam. End users have the option to review quarantine spam e-mail either through a Web-based interface or an HTML e-mail containing a summary of the end users’ quarantined spam.

- **Disaster recovery.** In the event that a server or Internet connection is unavailable, Exchange Hosted Filtering helps to ensure that no e-mail is lost or bounced, by queuing inbound e-mail in a secure environment for up to five days.
- **Policy enforcement.** An intuitive policy rule writer helps e-mail administrators to enforce corporate e-mail use policy based on virtually any message attribute from originating IP to sender/recipient.

Exchange Hosted Filtering is backed by a comprehensive set of SLAs that cover the core aspects of the filtering service performance. The SLAs are:

- 99.999-percent network uptime
- E-mail delivery of under two minutes
- 100-percent detection of known viruses
- 95-percent spam capture
- 1:250,000 false positive ratio

To view the terms and conditions of these SLAs, please log on to the Exchange Hosted Services Admin Center at https://admin.global.frontbridge.com, or contact your Microsoft account representative if you do not have a logon account for the Admin Center.

Microsoft Forefront Client Security

Microsoft Forefront Client Security delivers unified protection from current and emerging malware to help protect business systems against a broad range of threats. Built on the same, highly successful Microsoft protection technology already used by millions of people worldwide, Forefront Client Security helps guard against viruses, spyware, and other current and emerging threats. By delivering simplified administration through central management, and providing critical visibility into threats and vulnerabilities, Forefront Client Security helps computer administrators protect their businesses with greater confidence and efficiency. Forefront Client Security integrates with existing infrastructure software, such as Active Directory®, and it complements other Microsoft security technologies for better protection and greater control.

Microsoft Forefront Client Security delivers:

- **Unified protection** from viruses, spyware, and other current and emerging threats, including:
  - A single solution for real-time spyware and virus protection.
  - Built-in protection technology used by millions of people worldwide.
  - Effective threat response.

- **Simplified administration** through central management, including the ability to:
  - Define one policy to manage all protection agent settings on one or more protected computers.
  - Deploy malware protection signatures and software quickly.
  - Integrate the technology with existing infrastructures.
- **Critical visibility and control** through insightful, prioritized security reports and a summary dashboard view to provide businesses with visibility and control over malware threats. Other features include the ability to:
  - View insightful reports.
  - Stay informed with state-assessment scans and security alerts.

Forefront Client Security is currently available as a public beta. The product is targeted for release to manufacturing (RTM) in the second quarter of 2007.

Learn more about Microsoft Forefront Client Security by visiting http://www.microsoft.com/forefront/clientsecurity/default.mspx.

Microsoft Forefront Security for Exchange Server

Microsoft Forefront Security for Exchange Server includes multiple scan engines from industry-leading security firms integrated into a single solution to help businesses protect their Exchange messaging environments from viruses, worms, and spam. It ships with and integrates multiple industry-leading antivirus engines to provide comprehensive, layered protection against the latest threats. Through deep integration with Exchange Server, scanning innovations and performance controls, Forefront Security for Exchange Server helps protect messaging environments while maintaining uptime and optimizing server performance. Forefront Security for Exchange Server also enables administrators to easily manage server configuration and operation, and automated scan engine signature updates and reporting, at the server and enterprise level.

> *“...Forefront Security for Exchange Server helps protect messaging environments while maintaining uptime and optimizing server performance.”*

Microsoft Forefront Security for Exchange Server delivers:

Comprehensive Protection

- Forefront Security for Exchange Server includes multiple scan engines from industry-leading security firms integrated in a single solution to help businesses protect their Exchange messaging environments from viruses, worms, and spam.

Optimized Performance

- Through deep integration with Exchange Server, scanning innovations and performance controls, Forefront Security for Exchange Server helps protect messaging environments while maintaining uptime and optimizing server performance.

Simplified Management

- Forefront Security for Exchange Server also enables administrators to easily manage configuration and operation through automated scan engine signature updates and reporting at the server and enterprise level.

For organizations that have not yet migrated to Exchange 2007, Forefront Security for Exchange Server provides downgrade rights to Antigen for Exchange, Antigen for SMTP Gateways and Antigen Spam Manager to protect Exchange 2003 and Exchange 2000 environments.

The 120-day trial of Microsoft Forefront Security for Exchange Server is available for download today at http://www.microsoft.com/forefront/serversecurity/exchange/download.mspx.

Microsoft Forefront Security for SharePoint

Microsoft Forefront Security for SharePoint manages and integrates industry-leading antivirus engines to provide comprehensive protection against the latest threats, helping ensure documents are safe before they are saved to or retrieved from the SharePoint document library. In addition, documents can be scanned for company-sensitive information, profanity, or other administrator-defined content policies. Through deep integration with Microsoft Office SharePoint Server and Microsoft Windows SharePoint Services, Forefront Security for SharePoint helps protect your collaboration environment while maintaining uptime and optimizing performance. Forefront Security for SharePoint also enables administrators to easily manage product configuration and operation, automated antivirus signature updates, and reporting at the server and enterprise level.

Like Microsoft Forefront Security for Exchange Server, Forefront Security for SharePoint provides multi-engine protection against the latest threats. Customers can use up to five engines per scanning operation to ensure that they have maximum protection for their document libraries for both internal and Internet-facing sites. All documents are scanned as they are uploaded to, and retrieved from SharePoint document libraries.

Microsoft Forefront Security for SharePoint delivers:

Comprehensive Protection

- Microsoft Forefront Security for SharePoint includes multiple scan engines from industry-leading security firms integrated in a single solution to help businesses protect their SharePoint collaboration environments from documents containing malicious code, confidential information, and inappropriate content.

Optimized Performance

- Through deep integration with Office SharePoint and Windows SharePoint Services, Forefront Security for SharePoint helps protect your collaboration environment while maintaining uptime and optimizing performance.

Simplified Management

- Forefront Security for SharePoint also enables administrators to easily manage product configuration and operation, automated antivirus signature updates and reporting at the server and enterprise level.

For organizations that have not yet migrated to Microsoft Office SharePoint Server 2007 or Windows SharePoint Services 3.0, Forefront Security for SharePoint provides downgrade rights to Antigen for SharePoint to protect SharePoint Portal Server 2003 and Windows SharePoint Services 2.0 environments.

Microsoft Forefront Security for SharePoint is currently shipping. The 120-day trial is available for download today from http://www.microsoft.com/forefront/serversecurity/sharepoint/download.mspx.

Appendix B: Windows Vista Security Features

Microsoft recommends that customers investigate and evaluate Windows Vista for personal and business use. Windows Vista provides many security enhancements designed to help protect a user from malicious and potentially unwanted software. These security enhancements include:

- **User Account Control (UAC).** UAC separates standard user privileges and activities from those that require administrator access, thereby reducing the surface area for attacks on the operating system, while still giving typical users most of the capabilities they need every day. Running as a standard user with restricted rights is designed to help decrease the impact of social-engineering attacks.
- **Kernel Patch Protection for x64 Windows.** Kernel Patch Protection improves reliability and security, and makes it more difficult for hackers to hide malware, such as rootkits, deep in the operating system where they can be difficult for antimalware technologies to remove. Kernel Patch Protection also helps prevent other software from making unauthorized or unsupported modifications to the operating system. Also, for Windows Vista on 64-bit systems, security at the kernel level has been greatly enhanced because it requires that all kernel-mode drivers be digitally signed.
- **Internet Explorer 7 with Protected Mode.** In Protected Mode, Internet Explorer 7 runs with reduced permissions to help prevent user or system files or settings from changing without the user's explicit permission. The new browser architecture also introduces a *broker process*, which helps enable existing applications to elevate out of Protected Mode in a more secure way. This additional defense helps verify that scripted actions or automatic processes are prevented from downloading data outside of low-rights directories, such as the Temporary Internet Files folder.
- **Windows Defender:** Microsoft has included its antispyware solution, Windows Defender, into Windows Vista. Windows Defender helps protect against and remove spyware, adware, keystroke loggers, control utilities, and other potentially unwanted software.
- **Address Space Layout Randomization (ASLR):** ASLR is another defense capability in Windows Vista that makes it harder for malicious code to exploit a system function. Whenever a Windows Vista computer is rebooted, ASLR randomly assigns executable images, such as DLLs and EXEs, to one of 256 possible locations in memory. This makes it harder for exploit code to locate executables in order to take advantage of functionality inside the executables.