

Microsoft Security Intelligence Report



January-June 2006

*An in-depth perspective of trends in the malicious and
potentially unwanted software landscape in the first half of 2006*

Microsoft®



Microsoft Security Intelligence Report

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2006 Microsoft Corporation. All rights reserved.

Microsoft, the Microsoft logo, ActiveX, Internet Explorer, OneCare, the Security Shield logo, Win32, Windows, Windows Live, Windows Live OneCare, Windows NT, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.



Authors

Matthew Braverman

Microsoft Security Technology Unit

Jeff Williams

Microsoft Security Technology Unit

Ziv Mador

Microsoft Security Technology Unit

Contributors

Dave Berkowitz

Microsoft Security Technology Unit

Christopher Budd

Microsoft Security Technology Unit

Alexandru Carp

Microsoft Security Technology Unit

Mike Chan

Microsoft Windows Client

Jeremiah Glodoveza

Microsoft Exchange Hosted Services

Kristin Johnsen

Microsoft Security Technology Unit

Jeff Jones

Microsoft Security Technology Unit

Mary Landesman

Microsoft Security Technology Unit

Tony Lee

Microsoft Security Technology Unit

Lena Lin

Microsoft Security Technology Unit

Mark Miller

Microsoft Security Technology Unit

Michael Mitchell

Microsoft Legal and Corporate Affairs

Gina Narkunas

Microsoft Online Service Group

Adam Overton

Microsoft Security Technology Unit

Adrien Robinson

Microsoft Security Technology Unit

Shira Sagiv

Microsoft Security Technology Unit

Dave Sarjantson

Microsoft Security, Access and Solutions Division

Scott Stanzel

Microsoft Security Technology Unit

Jaime Wong

Microsoft Security Technology Unit

Table of Contents

Executive Summary	1
Overview of H106 Trends	1
Data Sources	3
Malicious Software	5
Malicious Software Categories	5
Malicious Software Activity	6
Infection Prevalence	9
Infected Message Prevalence	21
Potentially Unwanted Software	22
Software Removed by Windows Defender	23
Software Removed by the Windows Live OneCare Safety Scanner	25
Geographical Differences	25
A Focus on Adware	28
Conclusion	33
Appendix A: Security Enhancements in Windows Vista	35
Appendix B: Microsoft Antimalware Offerings	36
Windows Malicious Software Removal Tool	36
Windows Defender	36
Windows Live OneCare	37
Windows Live OneCare Safety Scanner	38
Microsoft Exchange Hosted Filtering	39
Microsoft Forefront Client Security	40
Microsoft Forefront Security for Exchange Server	41
Microsoft Antigen for Exchange	43

Executive Summary

Microsoft Corporation has made a significant investment over the past few years researching and combating malicious and potentially unwanted software, and in developing technology to help customers mitigate the security risk that it creates. As part of this investment, Microsoft created a dedicated antimalware team that is responsible for researching malicious software (or “malware”) and potentially unwanted software. In addition, this team is responsible for the release and maintenance of the Microsoft® Windows Malicious Software Removal Tool (MSRT) and Windows Defender.

This report focuses on the first half of the 2006 calendar year (from January to June) [H106] and expands upon a white paper Microsoft released in June 2006 entitled *MSRT: Progress Made, Lessons Learned* (<http://go.microsoft.com/fwlink/?linkid=67998>). Compared to the MSRT paper, this report includes more recent results based on a significantly expanded set of data sources. Using data derived from several hundred million Windows users, this report provides an in-depth perspective of trends in the malicious and potentially unwanted software landscape.

Overview of H106 Trends

Interested parties, especially security professionals, are encouraged to familiarize themselves with the contents of this entire document. For those readers interested in the key trends in malicious and potentially unwanted software during the first half of 2006, this section will summarize the most important points.

- Backdoor Trojans and bots continue to comprise a significant percentage of the malicious software detected by Microsoft antimalware offerings and therefore serve as a top threat to consumers and businesses alike.
- Attackers, with financial gain in mind, are clearly concentrating a significant amount of development focus on this category of malware. With more than 43,000 new variants found in the first half of 2006, backdoor Trojans and bots are the most active category of malware.
- Of the 4 million computers cleaned by the MSRT, approximately 2 million of the computers (or about 50 percent of those with malware present) contained at least one backdoor Trojan. While this is a high percentage, it is a decrease from the second half of 2005. During that period, the MSRT data showed that, of the computers with malware present, 68 percent contained a backdoor Trojan.

- Despite increased industry interest in Windows rootkits in 2005, there has actually been a 50 percent reduction in this kind of attack against computers running Microsoft Windows during the past six months—as indicated by the MSRT—a potential trend that will bear watching. The reduction in rootkit attacks may be related to the increasing availability of antirootkit tools and educational materials made available as of 2006. These tools have helped to decrease the number of large-scale rootkit attacks in favor of more specialized techniques related to stealth. While these techniques may never progress beyond proof of concept, undoubtedly some will appear as part of targeted attacks against high-value entities.
- Social engineering continues to be a popular means of spreading malware, especially when sent over e-mail and peer-to-peer (P2P) networks. For example, in the case of both the MSRT and Microsoft Windows Live™ OneCare, approximately 20 percent of computers cleaned were infected with a mass mailing worm. For the MSRT, this represents a slight increase from the previous six-month period, mainly due to the appearance of the Win32/Mywife.E mass mailing worm.
- Data collected by the MSRT suggests that computers that use certain languages are more likely to be infected with malicious software than others. For example, when the disinfection figures from an operating system language are normalized with the appropriate number of tool executions of that same language, we find that 16 percent of computers cleaned by the MSRT are from Turkish language computers. Differences here may be due both to malware activity and to the usage of up-to-date antimalware software in a specific country.
- The top 10 adware programs, treated as a group, are removed nearly 54 percent of the time by users when presented with a choice by Windows Defender. This suggests that, even where there is a value proposition stated to users, many are unwilling to take advantage of the value proposition in exchange for ad display.

“Social engineering continues to be a popular means of spreading malware, especially when sent over e-mail and peer-to-peer (P2P) networks.”

While the threat landscape continues to evolve, users can take steps to protect themselves. For Microsoft’s detailed recommendations on these trends, please refer to the “Conclusion” section at the end of this report.

Data Sources

Data from several customer-focused Microsoft antimalware 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 are aimed at individual users, the information provided is also applicable to business users.

Figure 1 shows the five main data sources used to compile the data regarding malicious and potentially unwanted software prevalence included in this report.

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	Businesses	Scan and Remove	Real-Time Protection	Scan and Remove	Real-Time Protection		
Windows Malicious Software Removal Tool	•		Partial				•	WU/AU, Download Center
Windows Defender	•				•	•	•	Download Center
Windows Live OneCare Safety Scanner	•		•		•		•	Web
Windows Live OneCare	•		•	•	•	•		Web / store purchase
Microsoft Exchange Hosted Filtering		•	•					Web / store purchase

Because they can be downloaded at no additional charge, the Windows Malicious Software Removal Tool (MSRT) and Windows Defender currently have the largest user bases. As a result, these products provide the highest volume of malicious and potentially unwanted software prevalence data and will be used as the main sources of information for this report.¹

Windows Defender, in beta 2 at the writing of this report, has more than 14 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 290 million unique computers. During H106, the tool was executed 1.6 billion times, bringing the total number of executions since January 2005 to 3.6 billion.

¹ Neither of these products 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 an Advanced member. 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.msp> and the MSRT's online documentation at <http://support.microsoft.com/kb/890830>.

To address the overall computer “health” issues (including malware prevention) facing consumers, Microsoft has launched two new services: Windows Live OneCare (launched in June 2006 in the United States only) and the accompanying Windows Live OneCare safety scanner (launched in August 2006 in 44 international markets). Windows Live OneCare is the consumer-facing service that provides continuous, real-time malware protection for its subscribers. Windows Live OneCare safety scanner is a free, Web-based service offering quick, on-demand computer health and security scans. As of the writing of this report, the Windows Live OneCare safety scanner has performed nearly 7 million scans, detected almost 3 million instances of malware or spyware, and cleaned more than 575,000 infected computers since its public beta availability in August 2006.

The Appendix includes more information about the tools and services used as data sources for this report. It also includes information about three additional business-focused Microsoft antimalware offerings: Microsoft Antigen for Exchange, Microsoft

Forefront Security for Exchange Server, and Microsoft Forefront Client Security. Microsoft Antigen for Exchange is available to customers now. Forefront Security for Exchange Server is expected to be generally available by late 2006 or early 2007. Forefront Client Security will be available as a public beta in Q4 2006 and will be released in the first half of 2007.

Most of the data used in this report was derived by measuring cleaned or blocked infections on customer computers, as reported by the products listed in Figure 1. The only exception to this method is for the data reported by Microsoft Exchange Hosted Filtering, which measures the number of e-mail messages sent by attackers. Both of these methods are valid threat measurement

tools and, as described later in this report, for a specific threat there may be similarities in the results derived from these methods. However, tracking actual infections on user computers is the most accurate method of determining the prevalence of malware infections because it indicates whether malicious software was successful in actually infecting a computer.

“The Windows Live OneCare safety scanner has performed nearly 7 million scans, detected almost 3 million instances of malware or spyware, and cleaned more than 575,000 infected computers since its public beta availability in August 2006.”

Malicious Software

This section discusses the emergence of new malware variants and malicious software prevalence during H106. The emergence of new spyware and potentially unwanted software variants is not covered in this report. The prevalence of potentially unwanted software is discussed in the “Potentially Unwanted Software” section.

Malicious Software Categories

This chart refers to the following categories of malicious software:

Category	Description
Mass mailing worm	Malware that spreads using electronic mail.
P2P worm	Malware that spreads through peer-to-peer network (P2P) applications, such as KaZaA and Winny.
Instant messaging (IM) worm	Malware that spreads using instant messaging applications such as Windows Live Messenger and AOL Instant Messenger.
Exploit malware	Malware that uses exploits of software vulnerabilities as its primary infection mechanism.
Trojan	Malware that seems to be harmless but contains hidden code to harm the user's system and serve the attacker.
Backdoor Trojan	A form of Trojan that can enable an attacker to control an infected computer and access confidential information. Bots are a sub-category of backdoor Trojans that use Internet Relay Chat (IRC) as their main method of communication.
Trojan downloader / dropper	A form of Trojan that copies other files to the system either by downloading them from a remote computer or by dropping them directly.
Virus	Malware that infects other files in the system, enabling the execution of its code and its propagation when those files are activated.
Password stealer (PWS) / key logger	Malware that is used specifically to transmit personal information such as passwords or key strokes to an attacker.

These categories are consistent with those defined in the white paper *MSRT: Progress Made, Lessons Learned*.¹ These categories are not mutually exclusive; one malware variant or family might fit into several of the categories.

¹This white paper can be downloaded from the Microsoft Download Center (<http://go.microsoft.com/fwlink/?linkid=67998>).

Backdoor Trojans, password stealers, key loggers, 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

While malware activity does not directly relate to malware prevalence, there is some correlation between these two metrics. 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.

Figure 2 shows the total number of variants in the first half of 2006 (H106), for each of the malware categories defined in the previous section. These numbers include variants from hundreds of different malware families. The activity metrics are measured in terms of new variants, not files. In cases where the malware’s functionality changes minimally or does not change at all, such as in file infector viruses, one malware variant can be mapped to multiple files. Thus, tracking variant activity is a more accurate form of measuring trends. To illustrate the difference between counting files and variants, in January 2006, Microsoft received 5,706 unique files that were classified as Win32/Rbot, and those were mapped to 3,320 distinct variants.

Figure 2. Malicious software activity during H106

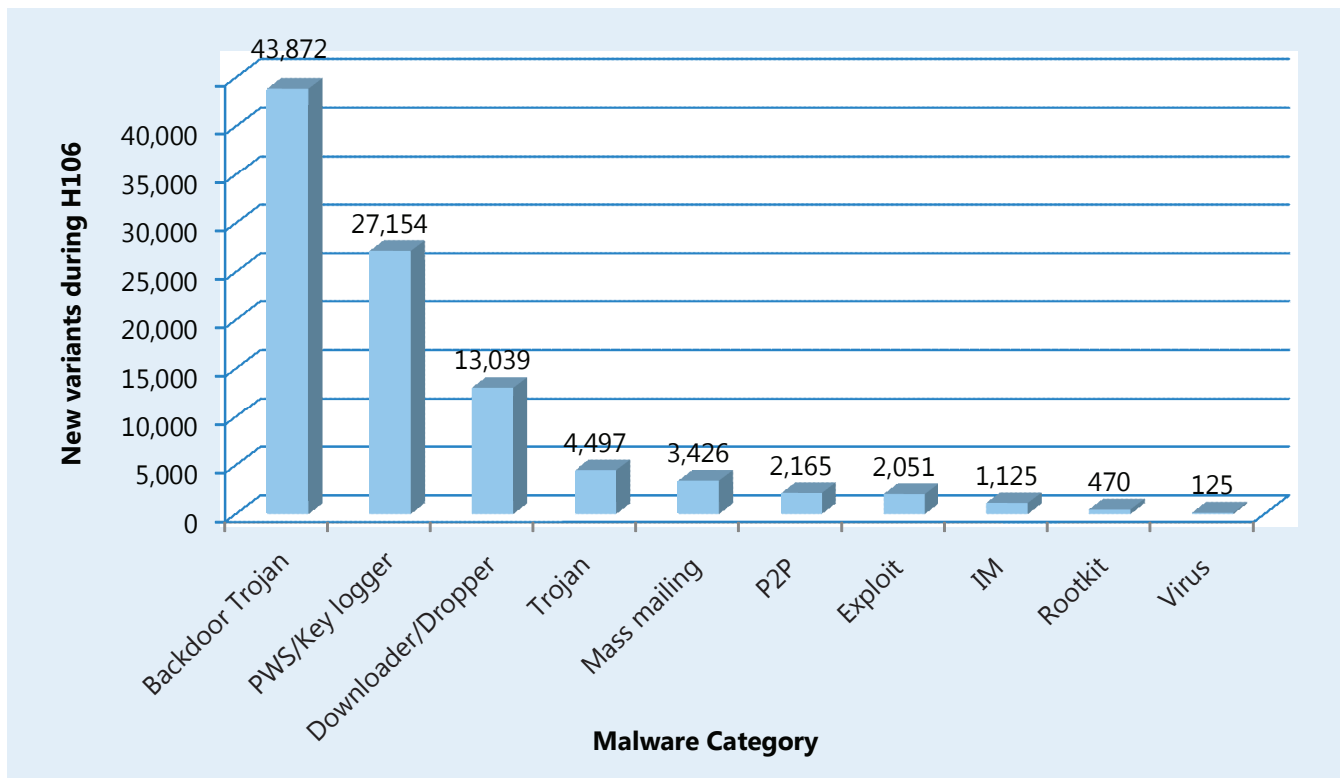


Figure 2 highlights the following:

- **Backdoor Trojans:** H106 has yielded a significant number of new backdoor Trojans. A large number of those belong to bots families, such as Win32/Rbot and Win32/Sdbot. This trend is consistent with anecdotal industry knowledge; owners of bot networks are continually creating and delivering new variants of their bots to maintain their bot networks, and to evade detection by antimalware products. Win32/Hupigon is another active backdoor family, with several thousand new variants appearing during this period.
- **Password stealers and key loggers:** These comprise the second-largest malware category, in terms of number of variants. Although this type of malware exists worldwide, the Microsoft antimalware team has seen a high number of variants coming from Brazil. Several thousand new variants from the Win32/Banker and Win32/Bancos families were discovered during H106, which mainly use Portuguese for their user interface. This malware is used to steal bank account information such as passwords.
- **Downloaders and droppers:** These comprise the third-largest category. These are tools used by the attackers to copy files to the victim's system that are necessary to complete the attack and control that system. Downloaders and droppers are also often used to distribute spyware and adware. Because of this, the presence of downloaders and droppers as part of malicious attacks is not a surprise.
- **Worms:** The different types of worm families have a relatively low number of variants, although they remain prevalent. In fact, mass mailing worms continue to be an effective way to infect a significant number of computers around the world, as discussed in the "Infection Prevalence" section of this report.

Figure 3 (on the next page) lists the 25 malware families with the highest number of variants in H106. It also shows the categories to which these families belong and the total number of variants during that period. Note that there are no virus families in this list, and there is only one family that includes rootkit functionality (JS/Feeps).

Rank	Malware Family	Mail	P2P	IM	Exploit	Backdoor Trojan	Rootkit	Virus	PWS / Key logger	Downloader/ Dropper	Trojan	Number of variants (H106)
1	Win32/Rbot					X						16,736
2	Win32/Banker								X			15,782
3	Win32/Hupigon					X			X	X		8,646
4	Win32/Sdbot					X						5,408
5	Win32/Small					X			X	X	X	4,610
6	Win32/Bancos								X			4,320
7	Win32/Agent					X			X	X	X	2,790
8	Win32/Delf					X			X	X	X	1,937
9	Win32/Spybot		X			X						1,904
10	Win32/Gaobot					X						1,899
11	Win32/VB					X			X	X	X	1,610
12	Win32/Zlob									X		1,399
13	Win32/Bifrose					X						1,214
14	Win32/Centim									X		1,041
15	Win32/Mytob	X		X	X	X						946
16	Win32/IRCbot					X						853
17	Win32/Startpage										X	591
18	Win32/Adialer										X	581
19	Win32/Bagle	X				X				X		543
20	Win32/Inservice									X		388
21	Win32/Sinowal								X			355
22	Win32/Berbew					X			X			323
23	Win32/Wmfpgv				X					X		253
24	JS/Feebs	X					X			X		210
25	Win32/Adload									X		162

Figure 3. Top 25 active malware Families during H106

The figure shows that, of the four biggest families, two are large bot families: Win32/Rbot and Win32/Sdbot. As discussed earlier in this section, these are backdoor Trojans that use IRC channels to get commands from the attacker to control the infected computer. To complicate detection, the attacker that controls the bot network frequently updates infected computers with new variants. Note that even though Rbot often uses exploits as a mechanism to spread, it hasn't been classified as an exploit malware. This paper classifies a malware family as an exploit malware only if the exploit is the primary mechanism to infect a computer and/or execute its payload.

Win32/Hupigon is another family of backdoor Trojans that has a very high number of variants. This family also includes password stealing and key logging capabilities, as well as a stealth component to hide its presence. One explanation for the high number of Win32/Hupigon variants is that a kit allowing attackers to create new variants can be purchased online.

The Win32/Banker and Win32/Bancos families include basically the same functionality as Win32/Hupigon, and, as noted above, can capture bank account credentials.

New variants of malware that exploit the WMF vulnerability appear at the bottom of Figure 3. These exploits started appearing at the end of December 2005 and, in a short time, dozens of Web sites were hosting them. In most of these cases, the malicious WMF files serve as Trojan downloaders or Trojan droppers.

Microsoft released a generic detection for this exploit on December 27, 2005, with the name Exploit:Win32/Wmfap. Using this generic detection, Microsoft found 8,881 unique files in the wild. Even though the security update was released in early January, the Microsoft antimalware team has seen new malicious WMF files released throughout this year, particularly in H106. While many users have updated their computers, attackers are still likely targeting those who may have not yet done so. Microsoft also added explicit detection for 253 variants of these exploits (as indicated in Figure 3: Win32/Wmfpfv). These variants detect 1,389 malicious WMF files.

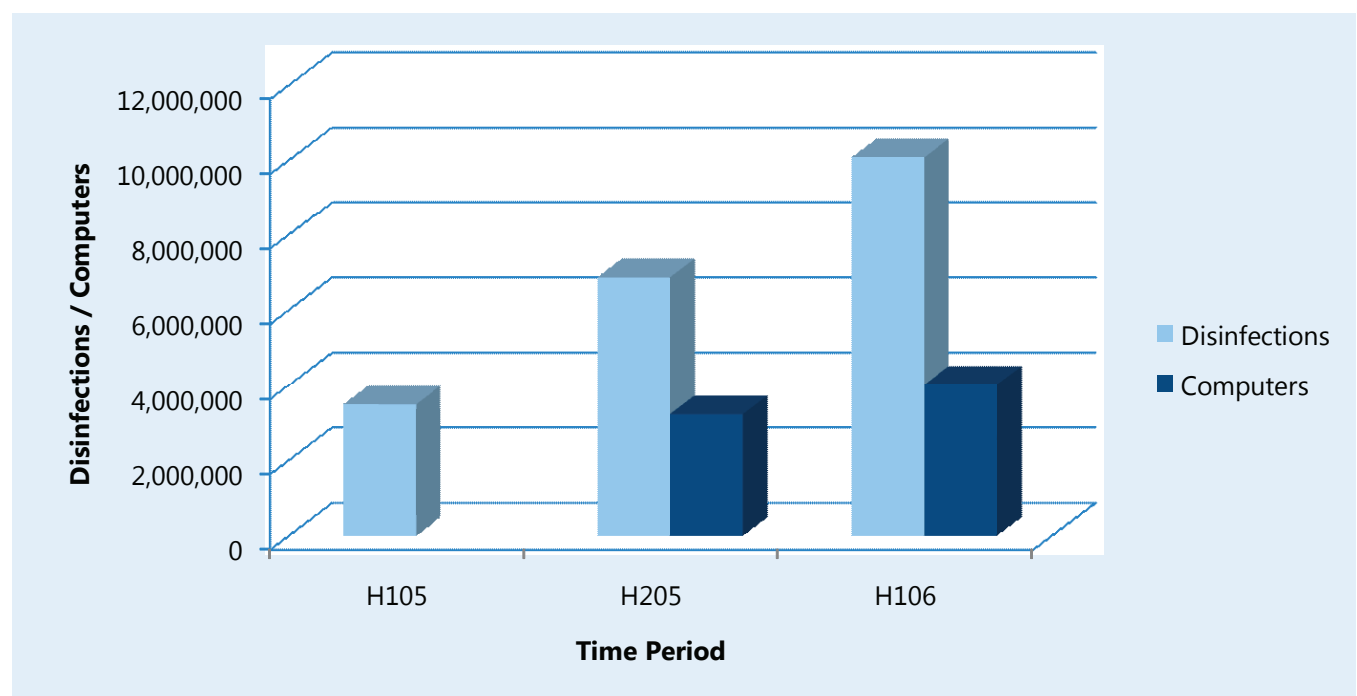
During H106 the Microsoft antimalware team has also seen exploits of non-patched vulnerabilities in Microsoft Office. However, unlike the WMF exploit, these Office exploits were mostly targeted attacks and limited in scope.

Infection Prevalence

This section provides information regarding the malicious software that was found on customer computers during the current report period (H106) and compares that information to trends from previous periods, where available. Data in this section is generated from users of the Windows Malicious Software Removal Tool (MSRT), Windows Live OneCare safety scanner, Windows Live OneCare, and Microsoft Exchange Hosted Filtering.

Figure 4 shows the disinfections and computers cleaned by the MSRT from the first half of 2005 (H105) through H106.

Figure 4. Disinfections and computers cleaned by the MSRT



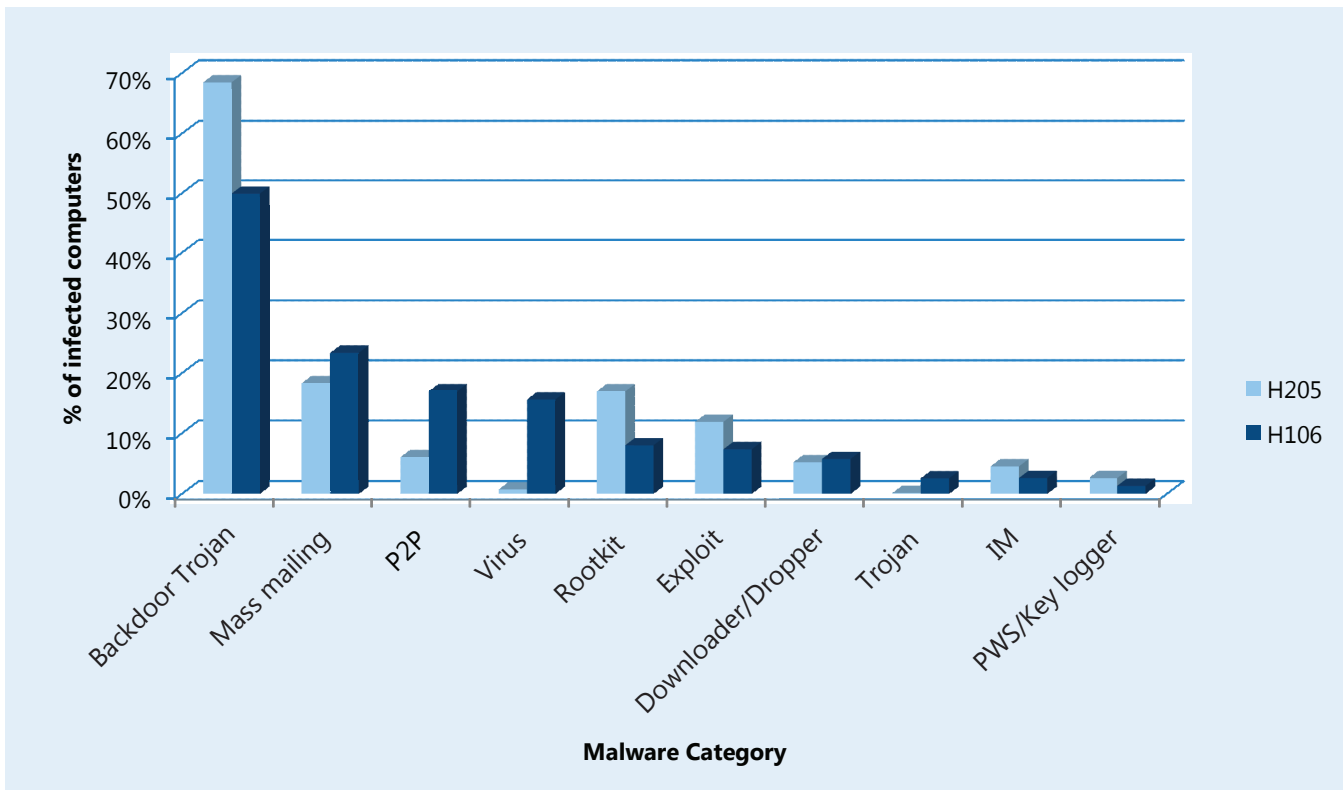
As shown in the chart, the MSRT removed approximately 10 million pieces of malicious software from nearly 4 million unique computers during the first half of 2006. In total, the MSRT has removed more than 20 million pieces of malicious software from more than 7 million unique computers. Most of the 4 million unique computers cleaned in H106 were computers not previously cleaned by the tool, although there were some computers which became re-infected with malicious software between H205 and H106. The increase in disinfections and computers cleaned with each successive period is due both to retroactive malicious software families being added to the MSRT and to new malware variants appearing in the wild.

Note that Microsoft did not begin to measure unique computers cleaned until H205, so this data is unavailable for H105.

Prevalence by Category

Figure 5 illustrates the categories of malicious software removed by the MSRT from infected computers. Both H205 and H106 are shown for comparative purposes. The malware categories are ordered by infection percentages for H106. Note that the percentages correspond to infected computers, not to all computers scanned. For example, in H205, 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 5. Categories of malware removed by the MSRT during H205 and H106



Some of the trends shown indicate a shift in the malware landscape. Other trends, however, result from retroactively adding families to the tool. For example, the percentage of viruses found increased from 0.74 percent to 15.71 percent, mainly due to the inclusion of the Win32/Parite virus detection to the tool. This virus, first discovered in October 2001, is still very active today, demonstrating that file-infecting viruses are still prevalent.

Backdoor Trojans, clearly representing a significant portion of the malware cleaned by the MSRT, were found on 68 percent of machines cleaned in H205 and 50 percent of computers cleaned in H106, demonstrating a decrease in this type of malicious software during H106. In particular, detections of some of the larger bot families, such as Win32/Sdbot and Win32/Gaobot, which compose a large portion of the backdoor Trojan detections, have significantly decreased during this time. This is true despite the fact that detection for thousands of new variants of these families has been added to the signature database during H106, as indicated in the “Malicious Software Activity” section.

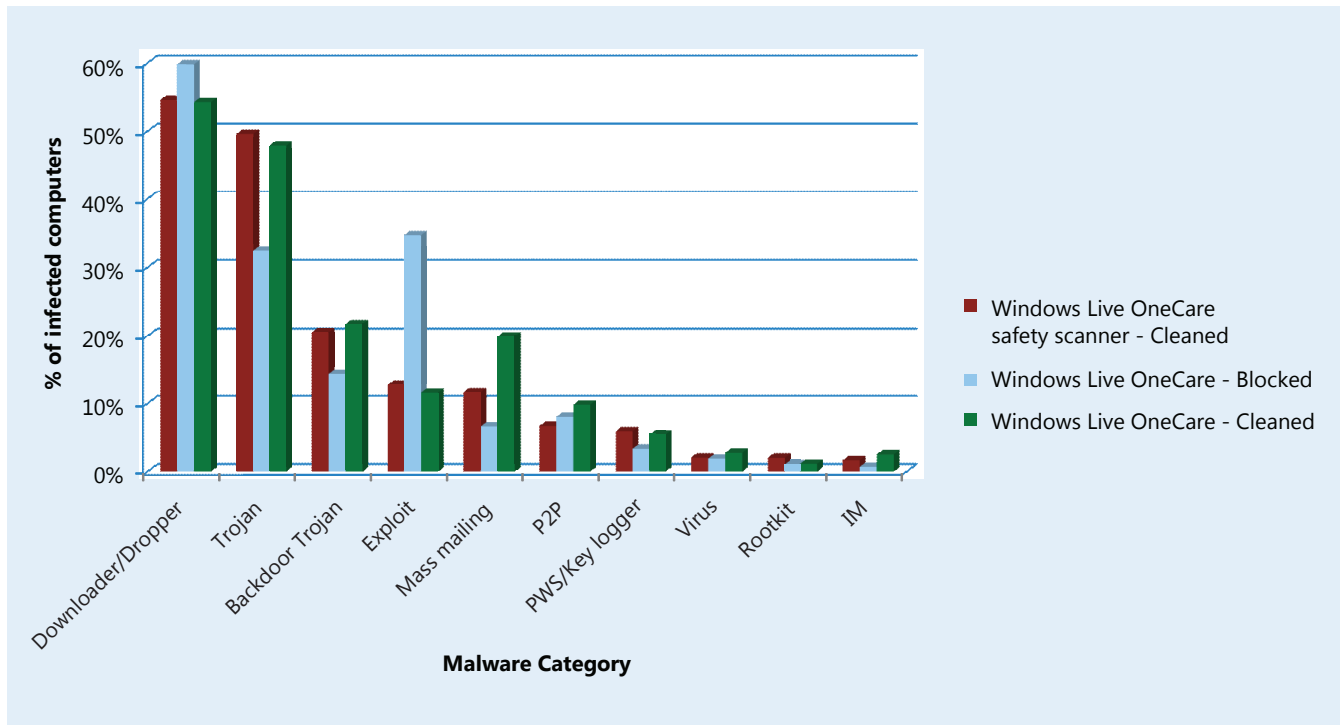
Social engineering-based malicious software attacks continue to be active, especially those that spread through e-mail and P2P networks. Note the following:

- The percentages of machines infected with e-mail worms increased slightly, from 18 percent in H205 to 23 percent in H106. This increase can mainly be linked to the appearance of the Win32/Mywife.E worm (also referred to by CME-24 or as the Kama Sutra worm) in H106.
- P2P networks continue to be a common method of spreading malicious software; 17 percent of machines cleaned in H106 contained at least one P2P worm. The increase from H205 is mainly due to the addition of the Win32/Alcan worm detection to the MSRT. This worm was discovered in April 2005.
- Even though the tool detects some of the most infamous instant messaging worms, including Win32/Kelvir, Win32/Bropia, and Win32/Mytob, data from the MSRT continues to show that instant messaging is a much less common vector for distributing social engineering-based attacks when compared to e-mail and P2P networks. Note that some malicious software uses live chat applications (especially IRC) as a mechanism to communicate between a server and a set of infected clients or zombies. While some vendors classify these threats as instant messaging worms, this report restricts the definition of instant messaging worms to only those that use the instant messaging mechanism to replicate.

Detections of rootkit families decreased between H205 and H106, from 17 percent to 8 percent. Detection of Windows NT/F4IRootkit, found on select Sony CDs, was added to the MSRT in December 2005. This generated a significant number of detections during that period, which quickly dropped off in January 2006. Decreases in Windows NT/FURootkit and Windows NT/Ispro detections during H106 also contribute to the dropoff. While several new and high profile rootkits such as Win32/Rustock.A appeared in the first half of 2006, most were targeted attacks with high press coverage rather than actual widespread threats. Because of a rootkit’s ability to hide the presence of an attack, it is likely that this category will continue to be popular for smaller, targeted intrusions.

Figure 6 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 5 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 actively found running on the computer and then removed (cleaned). This makes it simpler to compare the Windows Live OneCare data to the Windows Live OneCare safety scanner data, since the Windows Live OneCare safety scanner does not block malicious software from infecting a computer.

Figure 6. Types of malware removed by the Windows Live OneCare safety scanner and Windows Live OneCare in H106



There are clear differences between the data shown for these three data sources and the data shown in Figure 5 for the MSRT. The greatest difference is in the high prevalence of downloaders and Trojans detected in the malicious software cleaned by the Windows Live OneCare safety scanner and Windows Live OneCare, comprising about 50 percent of the activity, compared to the MSRT. This difference is expected, since the MSRT does not include detection for a large number of these categories of malicious software programs, especially downloaders. The MSRT focuses mainly on resident and active malicious software, whereas downloaders usually run for a short period of time, retrieve additional software, execute that additional software, and exit.

Since both the Windows Live OneCare safety scanner and Windows Live OneCare include the full set of malicious software signatures, and since both scan the entire computer, it was expected that the results from the Windows Live OneCare safety scanner and Windows Live OneCare-cleaned figures would be similar, as Figure 6 illustrates. It also shows some key differences between malicious software that was blocked and malicious software that was cleaned by Windows Live OneCare, with the most significant difference existing in the Exploit category. The large number in the exploit category is the result of Windows Live OneCare blocking a significant amount of malicious software that leveraged the WMF exploit. Soon after the appearance of several malware programs that exploited the WMF vulnerability, the Microsoft antimalware team was able to create and deploy a generic signature that was highly effective in detecting malicious software that leveraged this exploit. As a result, many users were protected from infecting their computers with this type of malicious software.

“The large number in the exploit category is the result of Windows Live OneCare blocking a significant amount of malicious software that leveraged the WMF exploit.”

Prevalence by Family

Figure 7 (on the next page) lists the top 25 malware families removed by the MSRT during the first half of 2006. Figure 7 includes both the number of disinfections for each malware family and the number of unique computers cleaned. It is sorted by the latter. The number of disinfections for each family is greater than the number of unique computers cleaned because the MSRT can remove several variants of a specific malware family from a computer during each execution. Figure 7 also shows the percentage change in the number of computers cleaned for each family since the previous six-month period (H205). 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 July 2005.

Figure 7. Top 25 malware families cleaned by the MSRT during H106

Rank	Malware Family	Disinfections	Computers Cleaned	Change in Computers Cleaned Since H205	Rank from H205
1	Win32/Rbot	2,543,162	1,216,168	6.30%	1
2	Win32/Parite	1,779,654	588,563	-	-
3	Win32/Alcan	833,553	514,886	-	-
4	Win32/Wukill	684,955	378,306	-	-
5	Win32/Sdbot	655,145	351,348	-14.34%	2
6	WinNT/FURootkit	306,582	153,562	-43.82%	3
7	Win32/Bagle	255,829	126,655	22.80%	9
8	Win32/Mywife.E	286,351	118,839	-	-
9	WinNT/F4IRootkit	193,665	116,608	-	-
10	Win32/Zlob	256,511	98,408	-	-
11	Win32/Mytob	141,927	90,666	-26.33%	7
12	Win32/Gaobot	203,875	87,921	-52.70%	4
13	Win32/Netsky	152,095	86,248	-31.31%	6
14	Win32/Antinny	252,393	71,438	-	-
15	Win32/Spybot	112,867	70,006	-9.01%	13
16	Win32/IRCbot	109,124	63,162	-	-
17	Win32/Codbot	83,616	52,450	-	-
18	Win32/Lovgate	162,294	50,190	-11.19%	17
19	Win32/Berbew	100,634	45,818	-44.98%	12
20	Win32/Nachi	61,308	40,002	8.37%	21
21	Win32/Wootbot	86,132	39,898	-58.40%	10
22	Win32/Msblast	91,275	39,278	-27.87%	18
23	Win32/Gael	65,487	37,746	-	-
24	Win32/Korgo	47,565	29,532	-29.36%	19
25	WinNT/Ispro	97,210	22,559	-66.98%	14

As first shown in Figure 5, one trend also apparent in Figure 7 is the decrease in disinfections and computers cleaned for the bot families during the first half of 2006. While the number of computers infected with Win32/Rbot topped 1 million and increased by more than 6 percent during this period due to the appearance of new variants, this is a small increase compared with the 29 percent increase in executions of the MSRT during the period. While the Win32/Sdbot and Win32/Gaobot families ranked second and fourth, respectively, in H205, in H106 their rankings fell to fifth and twelfth, with decreases in computers cleaned of approximately 14 percent and 53 percent respectively.

Detections of most of the families listed in Figure 7 have decreased during H106, making way for newer families, such as Win32/Parite and Win32/Alcan, for which detection was added to the MSRT in H106. The high prevalence of these two families was surprising. For Parite, it was unexpected that the malware family is still highly prevalent today

since it first appeared five years ago. It seems that this is due to the aggression with which it infects a target computer. The high prevalence of Win32/Alcan is likely due to the effective social engineering techniques it leverages, which include posing as pirated software on various file sharing networks, and using dynamic filenames that reflect recent and in-demand software.

In addition to Win32/Rbot, the Win32/Nachi and Win32/Bagle families have shown increases in the number of computers cleaned. The relatively large increase in Win32/Bagle infections can be linked to several new and prevalent Bagle variants added to the MSRT in the first half of 2006. The reason for the increase in Nachi detections is not immediately clear. Since the increase is relatively small, it could be due to a variety of factors. For example, a modest increase in installations of Windows operating systems that do not include the patch for the vulnerability that the Nachi worm exploits could help contribute to this increase.

Figure 8 lists the top malicious software programs detected by Windows Live OneCare and the Windows Live OneCare safety scanner during H106, ranked by the number of unique computers on which each malware family was detected.

Windows Live OneCare Blocked		Windows Live OneCare Cleaned		Windows Live OneCare safety scanner	
Rank	Malware Family	Rank	Malware Family	Rank	Malware Family
1	Win32/Wmfap	1	Java/Classloader	1	Win32/Small
2	Win32/Small	2	Java/Bytverify	2	Java/Classloader
3	Win32/Agent	3	Win32/Small	3	Win32/Agent
4	Win32/Wmfpfv	4	Win32/Agent	4	Java/Bytverify
5	Win32/VB	5	Java/OpenConnection	5	Win32/Istbar
6	Java/Classloader	6	Java/OpenStream	6	Java/OpenConnection
7	Win32/Alcan	7	Win32/Istbar	7	Win32/VB
8	JS/Onload	8	Win32/Alcan	8	Java/OpenStream
9	Win32/Rbot	9	Win32/VB	9	Win32/Rbot
10	Win32/Istbar	10	Win32/Bagle	10	Win32/Wmfap
11	Java/Bytverify	11	Win32/Netsky	11	Win32/Alcan
12	Win32/Zlob	12	Win32/Wmfap	12	Win32/Adialer
13	Win32/Renos	13	Win32/Rbot	13	Win32/Netsky
14	JS/Drost	14	Win32/Sober	14	Win32/Sdbot
15	Win32/P2Pworm	15	HTML/Bankfraud	15	Win32/Bagle
16	JS/Mult	16	Win32/Lowzones	16	Win32/Dyfuca
17	Win32/Swizzor	17	Win32/Zlob	17	Win32/Delf
18	Win32/Adialer	18	Tool:PornDialer	18	Win32/Sober
19	Tool:PornDialer	19	Win32/Sdbot	19	Win32/Swizzor
20	VBS/Small	20	Win32/TSUpdate	20	Win32/Startpage
21	WinNT/Smallrk	21	Win32/Adialer	21	Win32/TSUpdate
22	Win32/Lowzones	22	Win32/Delf	22	Win32/Adload
23	Win32/Sdbot	23	Exploit:ContentMismatch	23	HTML/MhtRedir
24	Win32/TSUpdate	24	Exploit:LongName	24	Win32/Zlob
25	HTML/Winload	25	Win32/Swizzor	25	Win32/Lowzones

Figure 8. Top 25 malware families detected by Windows Live OneCare and Windows Live OneCare safety scanner during H106

While many of the malware families listed in Figure 8 are common to the three lists, there is less overlap found when comparing these lists to Figure 7, which lists the top malicious software detected by the MSRT. As was true when comparing the categories of malware removed, as shown in Figures 5 and 6, the difference in the sets of lists is due to the restrictions in the type of malware targeted by the MSRT.

Win32/Small and Win32/Agent both represent large collections of Trojan downloaders and are highly ranked in all three lists in Figure 8. As indicated in the “Malicious Software Activity” section, detection for a large number of variants of these families was added during H106, contributing to the high amount of detections.

Another set of families prevalent in Figure 8 are those related to the WMF exploit. For example, Win32/Wmfap was the top malware program blocked by Windows Live OneCare during H106. These families are ranked lower on the cleaned and the Windows Live OneCare safety scanner lists because, while many user computers appear to have been exposed to malicious software that exploited the vulnerability in the WMF format, a smaller set of those computers were actually infected.

Prevalence by Operating System

Figure 9 shows percentages of computers cleaned by the MSRT, by operating system.

The first two pie charts show the percentages for H205 and H106. The major trends illustrated in these two charts reflect a combination of the following:

- An expected movement of customers to newer and more secure service packs.
- A decrease in detections by the MSRT of malicious software that relies for replication on software vulnerabilities resolved in Windows XP® Service Pack 2 (SP2).
- An increase in social engineering malware, as illustrated in Figure 5.

The highest number of disinfections takes place on computers running Windows XP SP2. This is because most of the executions of the MSRT are on computers running Windows XP SP2 by means of Windows Update (WU)/Automatic Updates (AU), which users are recommended to enable when first installing Windows XP SP2. In fact, during H106, 88 percent of the MSRT executions via WU/AU were on computers running Windows XP SP2, compared to 1.5 percent for Windows XP and 3.0 percent for Windows XP Service Pack 1 (SP1) computers.

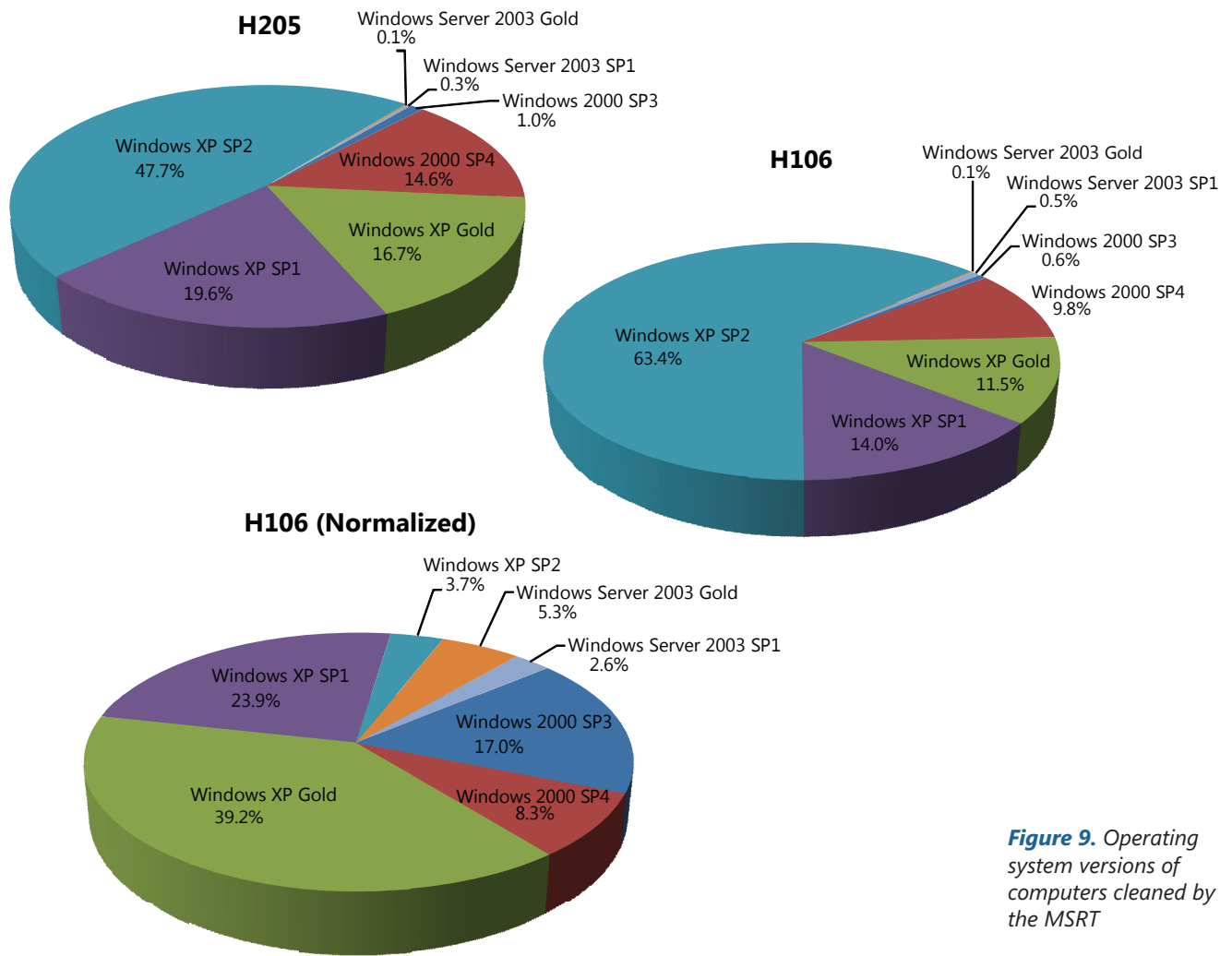


Figure 9. Operating system versions of computers cleaned by the MSRT

For a more realistic view of which malware programs are more commonly found on which operating systems, the data in the first two charts needs to be normalized by adjusting the disinfection percentage across operating systems to take into account the number of executions of the MSRT on each operating system. In other words, to reduce the numerical bias in the disinfection percentage introduced by a high number of executions on an operating system, divide the number of disinfections from a specific operating system by the relative percentage of executions on that operating system.

The normalization formula used is as follows:

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

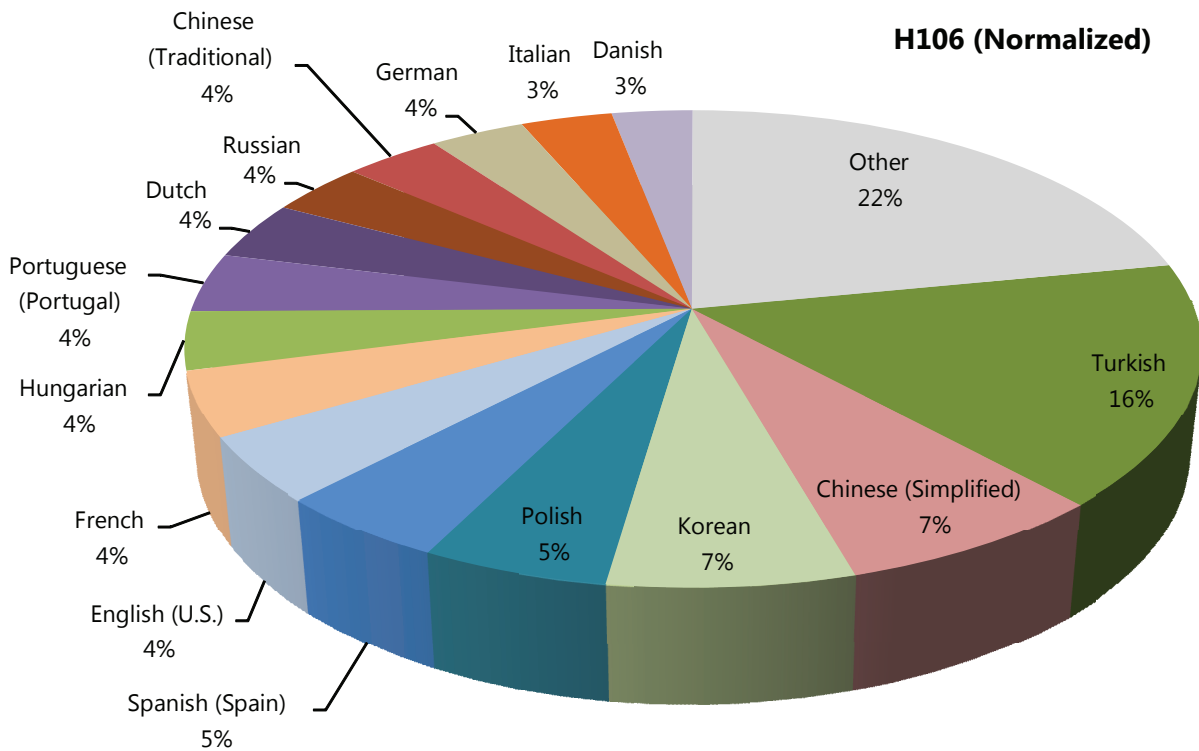
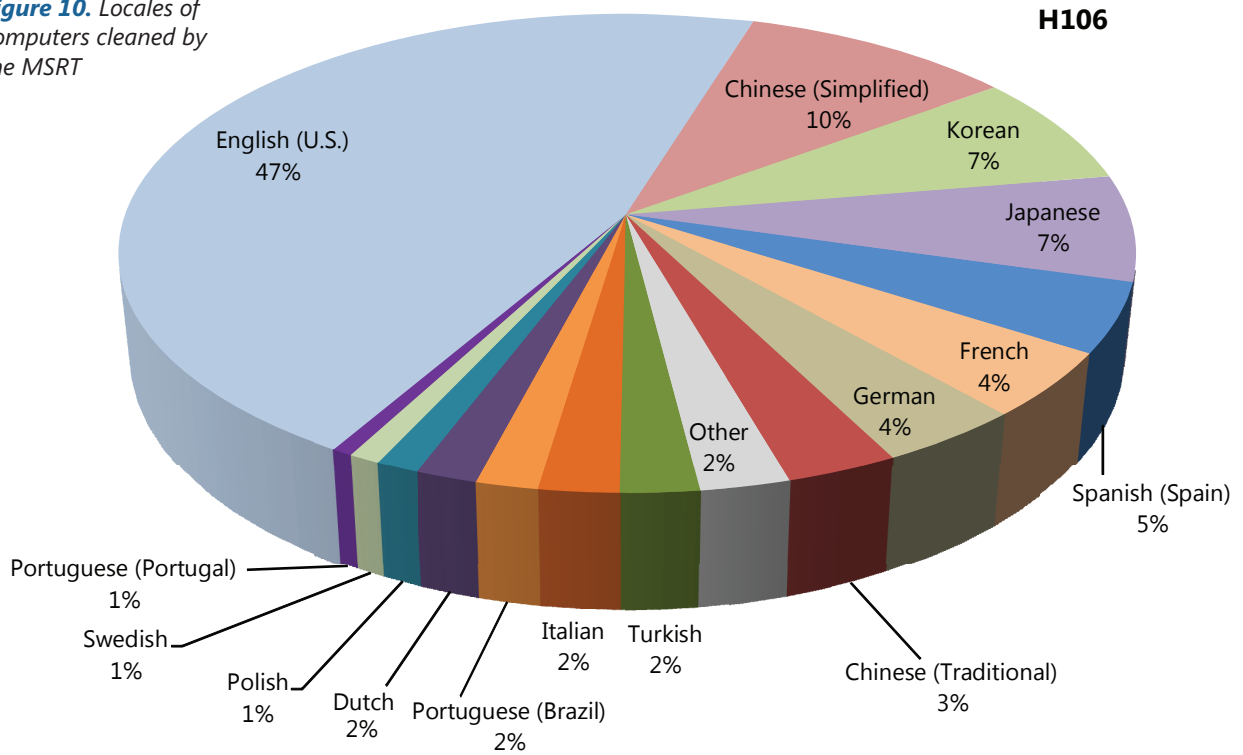
Applying this formula to the figures for H106 yields the H106 (Normalized) chart in Figure 9. This chart shows a dramatic change in the percentages, with Windows XP SP2 dropping to only 4 percent of the normalized disinfections and Windows XP and Windows XP SP1 accounting for 63 percent of the disinfections. This normalization makes sense for both technical and social reasons. Technically, Windows XP SP2 includes a number of security enhancements and updates for vulnerabilities not found in earlier versions of Windows XP, making it more difficult to be infected by malware in some cases. Socially, it is likely that a user who has not yet upgraded to the latest service pack would be more susceptible to social engineering attacks. This also holds true for Windows® 2000 and Windows Server™ 2003, for which the latest versions of the service packs have a lower number of normalized disinfections when compared to the older versions of the operating systems.

Prevalence by Locale

Figure 10 shows a breakdown of computers cleaned by operating system locale (or language) by the MSRT during H106. Although the MSRT is available in 24 different languages, only the top 15 languages are shown, to conserve space. The remaining locales are represented by the “Other” slice. Note that the locale is not necessarily indicative of geographical location. For example, using the English (U.S.) locale is fairly popular in other countries around the world.

The first chart in Figure 10 shows that a high percentage of the computers cleaned have an English language operating system. This metric is deceptive, because 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 9.

Figure 10. Locales of computers cleaned by the MSRT



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 H106 (Normalized) chart in Figure 10. Here, the normalization process has distributed the disinfections quite 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. As shown in the chart, there are a few exceptions to this even distribution, such as Turkish and Chinese (Simplified). One can make some conjectures about the reasons for these exceptions. For example, the differences might reflect a low usage and maintenance of antimalware products in areas associated with those locales, especially since the distribution is similar for most malware families.

While English is the top locale for most of the malware families targeted by the MSRT, there are several exceptions. In most cases, these exceptions correspond to regional threats, where the malicious software is tailored to a specific set of regions or locales. Amongst the families targeted by the MSRT, the most significant example of this type of threat is the Win32/Antinny worm, which affects only Japanese language operating systems. Naturally, the top locale of computers cleaned by Antinny is Japanese, which accounts for more than 99 percent of the computers cleaned in that locale.

Figure 11 shows two other threats where locales other than English compose most of the computers cleaned: Win32/Wukill (a mass mailing worm) and Win32/Parite (a virus). Note that the figures are *not* normalized in these graphs, since normalization would only further accentuate the low percentage of English disinfections.

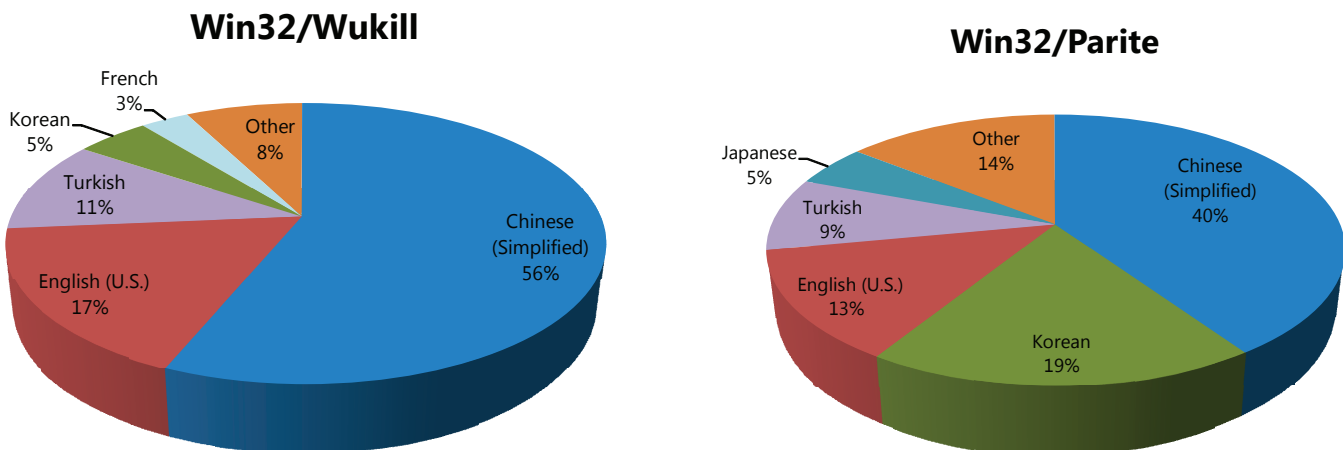


Figure 11. Locale breakdowns for Win32/Wukill and Win32/Parite

The high percentage of Chinese (Simplified) computers from which Wukill was removed makes sense given the fact that several variants of the worm construct e-mail messages using Chinese language characters. The figures for Win32/Parite are more perplexing. Although the percentages for Chinese (Simplified) and Korean language computer attacks are high, the virus includes no content specific to those languages. The high figures could be due to the lack of antivirus products used in these regions or their inability to successfully remove Parite from a computer. In any case, these charts show that regional attacks can seem somewhat unintentional and unrelated to the nature of the malware itself.

Infected Message Prevalence

The final set of malicious software prevalence data discussed in this report relates to the number of infected messages caught by Microsoft Exchange Hosted Filtering (EHF) between January 2005 and July 2006, as shown in Figure 12.

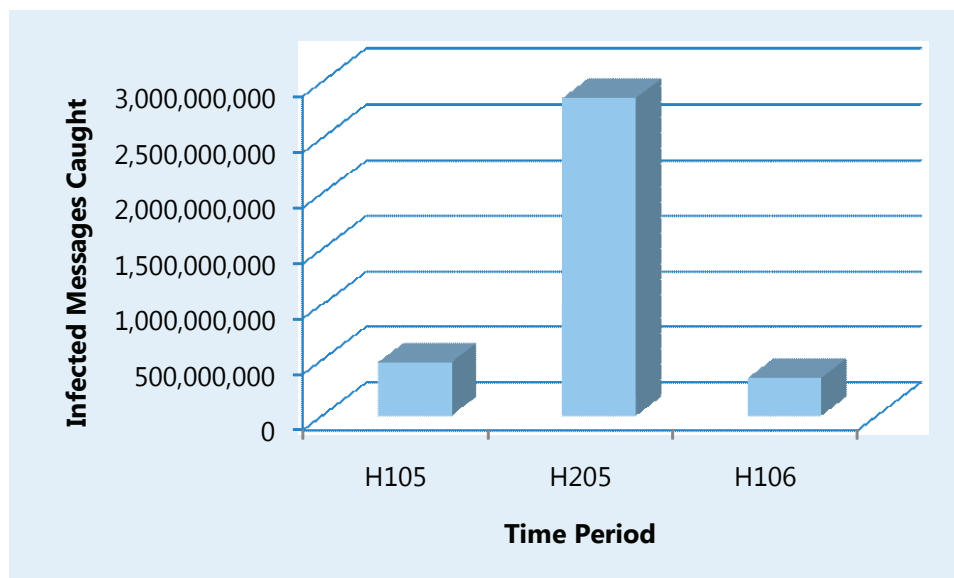


Figure 12. Infected messages caught by Microsoft Exchange Hosted Filtering between January 2005 and July 2006

The large spike in infected messages detected in H205 is the result of the Win32/Sober.Z worm (also identified as CME-681), released in November 2005. During H205, EHF identified and blocked a large number of e-mail messages containing this worm. This is an especially interesting case because the general infection prevalence numbers do not reflect a significant spike in Win32/Sober.Z infections. In fact, the MSRT has only ever removed 38,680 instances of Win32/Sober.Z, which is a much lower number of removals than its number of removals for other mass mailing worms. For example, the MSRT removed over 200,000 instances of Win32/Mywife.E, released in February 2006, but this did not cause the same spike in EHF figures. This suggests that there is not necessarily

a strong correlation between infected message prevalence and true infection prevalence. There are many scenarios, as with Win32/Sober.Z, where the worm simply generates a significant amount of message traffic.

Potentially Unwanted Software

This section describes the software removed by Microsoft® Windows® Defender Beta 2 and the Microsoft Windows Live OneCare safety scanner. It includes an analysis of geographical differences for the software removed by Windows Defender and a separate discussion of adware removal that features four popular adware programs.

“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.”

To understand this data from Windows Defender, it is important to remember two things: Each potentially unwanted software program has been assigned an alert rating of Low, Medium, High, or Severe; and each software program has also been assigned a default recommended action from the following list of possible actions:

- **Ignore:** to ignore the alert for the current session.
- **Ignore Always:** to ignore the alert from that point forward, even if the software is seen again.
- **Prompt:** to prompt the user to make a decision about what to do with the software.
- **Quarantine:** to remove the software in such a way that it can be restored at a later point.
- **Remove:** to remove the software from the system. Software rated with an alert level of High or Severe is removed automatically 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, choosing Remove usually indicates a clear, active choice. Choosing Ignore Always usually suggests that the user wants to keep the software. Users chose 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.

Software Removed by Windows Defender

On April 11, 2006, Microsoft released Windows Defender Beta 2. This section describes software removed by Windows Defender Beta 2 customers between April 11 and June 30, 2006. For purposes of this report, this data will be looked at in a variety of ways, but it is important to remember that the data presented here does not take into account several factors, including: whether the potentially unwanted software was installed by itself or as part of a bundle; whether the value proposition presented in an otherwise consensual installation was fulfilled; and whether the person responsible for the actions which led to installation was the primary operator of the computer. Because these variables are not included, one must be careful not to draw unwarranted conclusions from the data.

Figure 13 lists the top 25 programs detected by Windows Defender Beta 2, ranked according to what percentage of the time they are removed. The table also lists the relative percentages for the actions taken when the software was identified.

Figure 13. Top 25 software programs detected by Windows Defender Beta 2 between April 11 and June 30, 2006

Rank	Name	Category	% Remove	% Quarantine	% Ignore Always	% Ignore
1	ABetterInternet.DrPMon	Adware	98.49%	0.12%	0.00%	0.03%
2	TV Media Display	Adware	97.88%	1.14%	0.07%	0.38%
3	Twain Tech	Adware	96.30%	1.26%	0.20%	0.42%
4	Monnet	Trojan Downloader	94.21%	0.21%	0.00%	4.79%
5	TargetSaver	Trojan Downloader	92.17%	1.53%	0.02%	4.45%
6	Look2Me	Spyware	90.74%	0.34%	0.01%	8.06%
7	ABetterInternet	Adware	85.56%	1.26%	0.03%	6.47%
8	BlockChecker	Adware	83.35%	3.03%	0.46%	7.10%
9	WebHancer	Spyware	81.24%	2.27%	0.06%	15.10%
10	NewDotNet	Adware	79.15%	2.19%	0.11%	17.28%
11	Altnet P2P Networking	Adware	73.71%	0.95%	1.20%	3.48%
12	SurfSideKick	Settings Modifier	70.58%	0.43%	0.01%	28.61%
13	cmdService	Adware	67.72%	0.21%	0.02%	31.14%
14	C2.Lop	Spyware	64.48%	0.56%	0.03%	34.21%
15	WhenU.SaveNow	Adware	59.24%	1.44%	1.07%	25.33%
16	Need2FindBar	Adware	55.20%	0.58%	0.19%	31.73%
17	Altnet	Adware	53.60%	1.04%	0.65%	28.55%
18	PowerRegScheduler	Potentially Unwanted	52.12%	3.63%	1.80%	37.15%
19	KaZaA	Software Bundler	48.87%	0.77%	4.14%	35.69%
20	BearShare	Software Bundler	47.82%	0.83%	8.61%	28.77%
21	Qoologic	Adware	45.47%	0.31%	0.02%	53.76%
22	Hotbar	Adware	44.61%	0.43%	0.16%	51.91%
23	CNSMin	Spyware	42.68%	0.65%	0.20%	56.26%
24	Zango.SearchAssistant	Adware	38.19%	0.18%	0.15%	60.70%
25	Virtumonde.C	Adware	28.88%	0.25%	0.02%	70.70%

The top 25 software programs, ranked by removal count, account for nearly 50 percent of all removals in this period, even though there are thousands of families of potentially unwanted software removed by Windows Defender Beta 2. The top 10 software programs, ranked by removal count, represent 30 percent of all detections and 28.5 percent of all removals. Windows Defender Beta 2 removed 2,849 unique families of potentially unwanted software during this period.

For all of the potentially unwanted software detected, it is worth noting the low number of users who responded to detections with Ignore Always, a choice that would seem to indicate that the computer user actively wants to keep the software on their computer. Peer-to-peer (P2P) programs such as KaZaA, BearShare, and eDonkey 2000, and tools which can be used consensually (though are often installed without consent), such as Real VNC and CNSMin, tend to have a much higher percentage of detections responded to with Ignore Always than do software programs in the spyware and adware categories.

Overall, 22.27 million pieces of potentially unwanted software were detected by Windows Defender Beta 2 between April 11 and June 30, 2006, resulting in 13.83 million removals. This translates to an average removal ratio of 62 percent.

Individual users make different decisions about whether to keep or remove a piece of potentially unwanted software identified by Windows Defender Beta 2. 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 are active choices that represent individual, personal decisions. In still other cases, an individual may choose to ignore

“Overall, 22.27 million pieces of potentially unwanted software were detected by Windows Defender Beta 2 between April 11 and June 30, 2006...”

a piece of software (sometimes more than once) because they are not prepared to make a decision. They may have incomplete information, for example, about what would happen if they chose Remove, Quarantine, or Always Allow. They may want to defer the decision to a later time, when it is more convenient for them. Or they may be planning to remove the software later, once they have completed a particular course of action. Because it is not possible to infer users' intentions from the data, one should be careful not to jump to conclusions about why a particular piece of

software is or is not removed; instead, one is advised to look at the aggregate decisions of all voting members of SpyNet in any particular category. Also consider this: In a case where a user has chosen Ignore, that same user may have chosen Remove or Always Ignore at a later date.

Software Removed by the Windows Live OneCare Safety Scanner

As of March 15, 2006, the Windows Live OneCare safety scanner also has the ability to detect and remove spyware and other potentially unwanted software. The top 25 removals of potentially unwanted software between March 15 and June 30, 2006, are listed in Figure 14. This list is slightly different from the results shown in the Windows Defender Beta 2 list because the users of the Windows Live OneCare safety scanner are generally users who believe that they have been infected with unwanted software or malware and, because of this, have a different mix of software identified on their systems.

Rank	Family
1	WhenU.SaveNow
2	NewDotNet
3	KaZaA
4	Claria
5	Hotbar
6	Zango.SearchAssistant
7	PowerReg Scheduler
8	Tool:PornDialer
9	CnsMin
10	Altnet
11	BearShare
12	Twain Tech
13	WinSoftware
14	WebHancer
15	Trojan
16	IST
17	AvenueMedia
18	RealVNC
19	WindUpdates
20	Yazzle
21	ABetterInternet
22	MessengerPlus
23	WindUpdates.MediaGateway
24	FindTheWebsiteYouNeed
25	Hotbar.ShoppingReports

Figure 14. Top 25 removals of potentially unwanted software by the Windows Live OneCare safety scanner between March 15 and June 30, 2006

Geographical Differences

Using data from Windows Defender Beta 2, Figure 15 lists the top 25 countries, ranked by the total number of detections, and includes the total number of removals for each of those countries. As one would expect for a product whose customers are predominantly English speakers, these removal numbers are skewed heavily to the United States, United Kingdom, Canada, and Australia. The beta of Windows Defender was available only in

English throughout the Beta 1 period, and Beta 1 participants who upgraded to Windows Defender Beta 2 represent a sizable percentage of overall beta participants.

It is important to note the difference between the geographic area used in this section and the locale discussed previously in connection with the MSRT data. Locale refers to the language setting of the operating system (such as English, Chinese [Simplified], or Portuguese), whereas the geographic area is a location set by the individual in the Date, Time, Language, and Regional Options category of Control Panel or during setup. When looking at data from a geographical perspective, there is a higher correlation between the geographic area and the location of the computer than there is between the locale and the location of the computer.

The countries included in Figure 15 are listed in order of the number of total detected items. Because different countries have different removal percentages for any particular item, the total number of removed items occasionally differs in sort order from the overall rank, which is based on the number of times the item was detected.

Figure 15. Top 25 countries ranked by total number of detected items

Rank	Country	Removed
1	United States	8,160,414
2	United Kingdom	1,210,678
3	Canada	503,536
4	Netherlands	300,449
5	Australia	299,817
6	France	228,545
7	Brazil	160,404
8	China	140,919
9	Spain	126,325
10	Portugal	139,796
11	Germany	119,606
12	Belgium	106,832
13	Turkey	101,004
14	Mexico	106,679
15	Italy	91,044
16	Norway	82,837
17	Sweden	79,524
18	Denmark	71,028
19	Hong Kong S.A.R.	45,346
20	Poland	44,179
21	Switzerland	43,451
22	Singapore	47,567
23	Japan	52,622
24	Taiwan	37,256
25	New Zealand	42,239

Windows Defender beta users are located worldwide. This report, however, includes detailed geographical reporting only for those countries with a beta available in the predominant language. In addition, each country included represents more than 1 percent of worldwide detections in this period. More than 78 percent of Windows Defender Beta 2 installations are in the United States, United Kingdom, Australia, and Canada.

Removals in the top 25 countries represent over 89 percent of all removals worldwide. This metric will probably change, perhaps dramatically, as Windows Defender is introduced in additional languages following the conclusion of the beta, and as Windows Defender is more widely adopted. Currently, Windows Defender Beta 2 is available in English, Japanese, and German.

Figure 16 shows the top 10 detections in six countries.

Figure 16. Top 10 detections by country

United States	
Rank	Name
1	SurfSideKick
2	Qoologic
3	WhenU.SaveNow
4	Virtumonde.C
5	Zango.SearchAssistant
6	NewDotNet
7	Hotbar
8	KaZaA
9	BearShare
10	PowerRegScheduler

Canada	
Rank	Name
1	SurfSideKick
2	Hotbar
3	Virtumonde.C
4	WhenU.SaveNow
5	Zango.SearchAssistant
6	KaZaA
7	C2.Lop
8	BearShare
9	PowerRegScheduler
10	Altnet

United Kingdom	
Rank	Name
1	SurfSideKick
2	C2.Lop
3	Zango.SearchAssistant
4	WhenU.SaveNow
5	Hotbar
6	KaZaA
7	BearShare
8	Altnet
9	Monnet
10	cmdService

Australia	
Rank	Name
1	SurfSideKick
2	WhenU.SaveNow
3	Zango.SearchAssistant
4	Hotbar
5	BearShare
6	C2.Lop
7	Virtumonde.C
8	cmdService
9	NewDotNet
10	Look2Me

Germany	
Rank	Name
1	Zango.SearchAssistant
2	WhenU.SaveNow
3	BearShare
4	Hotbar
5	eDonkey 2000
6	KaZaA
7	C2.Lop
8	NewDotNet
9	RealVNC
10	Altnet

Japan	
Rank	Name
1	CNSMin
2	WhenU.SaveNow
3	RealVNC
4	Hotbar
5	NewDotNet
6	C2.Lop
7	KaZaA
8	Look2Me
9	cmdService
10	BearShare

As shown in Figure 16, there are significant differences as well as similarities among countries. These differences reflect the distribution practices of the software publisher, the cultural and social computing practices in each country, and the local language.

Several interesting observations can be made about the data used to create Figure 16:

- SurfSideKick is the number one program detected and removed in countries where English is the predominant language, but it is not even in the top 10 for Germany (15) or Japan (13).
- There are 10 times more removals of CNSMin in Japan than any other detected item. CNSMin is removed 79 percent of the time in Japan when it is detected by a Windows Defender Beta 2 customer, and the customer chooses Ignore Always less than 1 percent of the time. More than one third of all detections in Japan are CNSMin.
- The P2P software listed in the top 10 removals in Germany represents 15.4 percent of all detections in Germany. Four of the top 10 detections in Germany are P2P software. This prevalence is unique to Germany when compared to the other countries reviewed for this report.
- RealVNC is a shareware remote control package that is frequently used as a backdoor by malicious software, in addition to being used legitimately for remote administration. In countries where RealVNC is in the top 10 detections, it is removed approximately 25 percent of the time. Ignore Always is chosen approximately 30 percent of the time, presumably by those who have installed the software by choice and who want it to remain present indefinitely. It is expected that users sufficiently advanced to use this tool legitimately are also able to ignore any alerts regarding the software.

A Focus on Adware

There has been a great deal of press relating to adware and the companies who produce and distribute it. These discussions often highlight the complex monetary relationships between the various parties involved¹ and the specific tactics used to entice users to install the software. Community forums such as CastleCops, Spyware Warrior, Spyware Info, and Bleeping Computer are full of inquiries from individuals who want to remove the software, and who often don't know how they obtained the software in the first place. Adware distribution has been linked with drive-by downloads, exploit-based installations, and questionable consent experiences, as well as with less contentious installations where a value proposition is presented to the user, such as media content, games, or other software.

¹ CDT "Follow the Money" reports: Part I <http://www.cdt.org/privacy/20060320adware.pdf>, Part II <http://www.cdt.org/privacy/20060809adware.pdf>.

Because opinions regarding the relative merit of adware vary greatly, it is useful to provide additional detail on the choices made by Windows Defender beta customers. For this discussion, four adware programs common to the top 25 rankings of all six countries listed in Figure 16 have been selected for closer review. Together, these four adware programs account for 15 percent of all detections by Windows Defender Beta 2 on a worldwide basis.

Hotbar

Hotbar accounts for 4.65 percent of detections worldwide.

Hotbar displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity. The toolbar appears in Microsoft Internet Explorer and Microsoft Windows Explorer. The toolbar contains buttons that change depending on the current Web page and the keywords on that page. Clicking a button on the toolbar may open an advertisement Web site or a paid search site. Hotbar also installs graphical skins for Internet Explorer, Microsoft Outlook, and Microsoft Outlook Express. Hotbar may collect user-related information and may silently download and run updates or other code from its servers.

Figure 17 lists the top 10 countries that removed Hotbar, ranked by total number of removals.

Rank	Country	% Remove	% Quarantine	% Ignore Always	% Ignore
1	United States	45.73%	0.48%	0.21%	53.58%
2	United Kingdom	52.22%	0.52%	0.16%	47.11%
3	Brazil	45.73%	0.32%	0.05%	53.90%
4	France	40.05%	0.79%	0.13%	59.02%
5	Spain	35.18%	0.29%	0.08%	64.46%
6	Turkey	32.54%	0.10%	0.04%	67.32%
7	Portugal	42.51%	0.24%	0.07%	57.18%
8	Canada	49.55%	0.48%	0.13%	49.83%
9	Mexico	36.13%	0.19%	0.05%	63.63%
10	Netherlands	51.50%	0.33%	0.11%	48.07%

Figure 17. Top 10 countries ranked by total number of Hotbar removals

Hotbar, like most adware programs, has an alert rating of Medium, which means that Windows Defender prompts the individual to decide what they want to do with the software. The main difference between the two different ways to ignore an alert is this: Choosing Ignore Always suggests that the person probably does want the software; whereas choosing Ignore suggests several possibilities—the user may be unsure what will happen if the software is removed, the user may tolerate the software in the immediate term but is not prepared to make a final decision, the user may plan to remove the software at a later, more convenient date, or the user may want to make a decision after

evaluating the software’s behavior and impact. A very small percentage of users choose Ignore Always or Quarantine when alerted to the presence of Hotbar, suggesting that there is not a significant number of users who intend to keep the software long term.

WhenU.SaveNow

WhenU.SaveNow accounts for 4.07 percent of detections worldwide.

WhenU.SaveNow is a program that may display pop-up advertisements based on user-related information that it may collect after it is installed. The software may install a browser helper object for this purpose. The program may run in the background without a user interface. WhenU.SaveNow may also install other software.

Figure 18 lists the top 10 countries that removed WhenU.SaveNow, ranked by total number of removals.

Figure 18. Top 10 countries ranked by total number of WhenU.SaveNow removals

Rank	Country	% Remove	% Quarantine	% Ignore Always	% Ignore
1	United States	57.70%	1.52%	1.10%	39.68%
2	United Kingdom	60.87%	1.63%	1.10%	36.40%
3	Netherlands	60.25%	1.22%	1.31%	37.22%
4	Canada	58.41%	1.59%	1.36%	38.65%
5	Australia	62.41%	1.93%	1.34%	34.32%
6	Germany	63.88%	1.26%	1.06%	33.80%
7	France	59.72%	1.53%	0.57%	38.18%
8	Belgium	61.12%	1.07%	1.24%	36.58%
9	Brazil	62.14%	1.03%	0.63%	36.20%
10	Italy	60.46%	1.11%	0.76%	37.67%

WhenU.SaveNow represents 10.2 percent of all detections in Germany, 7.2 percent in the United Kingdom, 5.1 percent in Australia, 3.8 percent in Canada, and 3.5 percent in the United States. In Japan it represents 3 percent of detections, owing to the large number of CNSMin detections, which skew the results. When CNSMin detections are ignored, the percentage is 4.5 percent.

The Removal and Quarantine percentages of WhenU.SaveNow are notably higher than those of other adware programs profiled in this section. WhenU.SaveNow has an alert rating of Medium with a default action of Prompt, which means that these removals are the choice of the individual and not an automatic action. WhenU.SaveNow also has a higher percentage of Ignore Always than the other adware programs profiled in this section, suggesting that while a relatively small percentage of individuals installing the software want the software, the value proposition for WhenU.SaveNow probably exceeds the value proposition for other adware profiled here.

Zango.SearchAssistant

Zango.SearchAssistant accounts for 3.78 percent of detections worldwide.

Zango.SearchAssistant monitors a user's current Web browsing and displays pop-up advertisements related to the Internet sites the user is viewing.

Figure 19 lists the top 10 countries that removed Zango.SearchAssistant, ranked by total number of removals.

Rank	Country	% Remove	% Quarantine	% Ignore Always	% Ignore
1	United States	41.85%	0.18%	0.14%	57.83%
2	United Kingdom	35.75%	0.24%	0.17%	63.85%
3	Netherlands	27.10%	0.07%	0.13%	72.69%
4	Canada	42.77%	0.24%	0.15%	56.83%
5	Australia	37.21%	0.26%	0.15%	62.38%
6	Germany	28.90%	0.16%	0.16%	70.78%
7	Belgium	29.13%	0.10%	0.16%	70.61%
8	Denmark	27.10%	0.11%	0.12%	72.68%
9	Norway	30.06%	0.04%	0.12%	69.78%
10	Italy	27.97%	0.14%	0.10%	71.79%

Figure 19. Top 10 countries ranked by total number of Zango.SearchAssistant removals

Zango.SearchAssistant is often made available with media content or other bundled software. As the figures within this section of the report show, the Ignore percentage is higher for Zango.SearchAssistant than for the other adware programs profiled. It is likely that many users recognize that Zango.SearchAssistant is present, but they choose to ignore its presence while consuming the content or using the additional software, even in a case where they would otherwise prefer not to have the software installed. In such cases, choosing Ignore often represents a deferred decision, and the later decision may be to choose Remove or Ignore Always, or to remove the software manually using Add/Remove Programs. Because the choice of ignoring a piece of software identified as potentially unwanted is faster than removing it, it is expected that the number of Ignores is inflated by users who download during a single session multiple pieces of content, all of which install Zango.SearchAssistant.

TVMedia Display

TVMedia Display accounts for 1.02 percent of detections worldwide.

TVMedia Display is a program that may monitor a user’s Web browsing activity in order to display targeted advertising, usually as pop-up advertisements. The program may install a browser helper object for this purpose. The program may collect user-related information such as Web pages visited, user response to advertisements, and host system configuration. TVMedia Display may install silently and may install updates automatically, in the background, without notifying the user at the time of the update.

Figure 20 lists the top 10 countries that removed TVMedia Display, ranked by total number of removals.

Figure 20. Top 10 countries ranked by total number of TVMedia Display removals

Rank	Country	% Remove	% Quarantine	% Ignore Always	% Ignore
1	United States	98.00%	1.09%	0.06%	0.85%
2	United Kingdom	97.16%	1.32%	0.09%	1.43%
3	Canada	98.04%	1.25%	0.10%	0.62%
4	Australia	97.16%	1.96%	0.14%	0.74%
5	Netherlands	98.41%	1.01%	0.10%	0.48%
6	Belgium	94.96%	1.10%	0.33%	3.62%
7	Norway	91.27%	1.15%	0.00%	7.58%
8	France	96.85%	1.89%	0.13%	1.13%
9	Sweden	97.56%	1.22%	0.00%	1.22%
10	Switzerland	95.69%	2.28%	0.00%	2.03%

The high Removal and Quarantine percentages for TVMedia Display compared to other profiled adware are probably a result of its Severe alert level. There are numerous instances of TVMedia distribution via non-consensual installations which package TVMedia with other spyware and adware.

Conclusion

Thank you for reviewing the first 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 able to provide customers and partners with data that is highly relevant and accurate. 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:

- **Enable Automatic Updates** to help ensure that computers stay up to date with critical operating system and application updates.
- **Enable a firewall**, such as the Windows Firewall in Microsoft Windows XP Service Pack 2.
- **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.msp>.

“Future editions of this report will include data from additional sources, as required by the shifting landscape of security threats.”

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

- **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 it is run under least privilege.
- **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.

- **Use an application management system** within your organization to help control the programs that end users can run. For example, users should not be permitted to run certain peer-to-peer (P2P) network software within most organizations, because software downloaded by these programs can be hosts for malicious and potentially unwanted software. 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.
- **Educate your organization about malicious and potentially unwanted software.** In relation to the trends described in the executive summary, there are at least two levels of education:
 - All users should be educated about the danger of social engineering threats, especially those that spread through e-mail. Many e-mail worms today use enticing and familiar content within the e-mail message to lure readers into executing an infected attachment.
 - IT administrators should educate themselves about the trends and capabilities of malicious software. For example, as rootkits become more targeted threats, administrators should familiarize themselves with behaviors associated with a computer infected with a rootkit and with respective detection tools and techniques to help identify these threats.
- **Investigate tools which 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 in. Note that these tools are not a replacement for up-to-date antimalware. 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: Security Enhancements in Windows Vista

Microsoft recommends that customers investigate and evaluate Windows Vista, currently in Release Candidate 1, 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:** User Account Control (UAC) is a new approach that 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. This feature is designed to help decrease the impact of social engineering attacks.
- **Kernel Patch Protection for x64 Windows:** Kernel Patch Protection improves security and makes it more difficult for hackers to hide malware, such as rootkits, deep in the OS where antimalware technologies may have a more difficult time removing it. This protection also helps prevent other software from making unauthorized or unsupported modifications to the operating system. Also, with Windows Vista on 64-bit systems, security at the kernel level has been greatly enhanced by requiring that all kernel-mode drivers be digitally signed.
- **Internet Explorer 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 that 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 integrated its antispymware 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.

Appendix B: Microsoft Antimalware Offerings

Microsoft provides the following antimalware offerings for individual users:

Windows Malicious Software Removal Tool

The 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 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 June 2006, the tool is capable of detecting and removing 69 different malware families.

The tool does not target spyware and potentially unwanted software. Also, the MSRT is not a replacement for an up-to-date antivirus solution, because of its lack of real-time protection and its use of only the portion of the Microsoft antivirus signature database that enables it to target prevalent malicious software.

The MSRT has been available since January 2005 and has a user base of over 290 million unique computers. During the first half of 2006 (H106), the tool was executed 1.6 billion times, bringing the total number of executions since January 2005 to 3.6 billion.

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 varied, although most are probably home users or small business users. Because the MSRT is 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 Beta 1 of Microsoft AntiSpyware 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 Beta 1, the Microsoft antimalware team began to enhance the technology, working to better integrate it with other Microsoft technologies and platforms, and help ensure scalability so that the technology and its infrastructure could support hundreds of millions of users worldwide.

In April 2006, Microsoft released Windows Defender Beta 2 in English, providing improved capabilities for detection and removal to the more than 14 million beta users. This release also included improvements to the telemetry infrastructure for SpyNet. In May 2006, Microsoft expanded availability of the beta to two additional languages,

Japanese and German. The data in this security intelligence report relating to Windows Defender is limited to data collected by Beta 2 and, as a result, the period is truncated from the overall report to include April 11 to June 30. The technology, processes, and infrastructure which support Windows Defender Beta 2 also support Windows Live OneCare, Windows Live OneCare safety scanner, and Microsoft Forefront Client Protection.

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 that computer's operator. We recognize that technology alone will not address the serious problem of spyware. Because of this, in addition to our efforts to improve technology, we are also 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 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/athome/security/spyware/software/default.aspx>.

Windows Live OneCare

Microsoft introduced Windows Live OneCare to help address the average consumer's challenge of keeping their computers protected and maintained in response to ever-changing Internet threats and technologies. Designed to help meet this need, Windows Live OneCare is a comprehensive, automatic, and self-updating computer care service that continually manages vital computer security and maintenance tasks on behalf of the consumer. This increases the user's ease and peace of mind.

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

- **Protection Plus**, with continuous, real-time antivirus monitoring and a managed, two-way firewall, helps protect against viruses, worms, Trojan horses, hackers, and other threats. Windows Live OneCare also integrates Windows Defender for antispyware technology.

“With Windows Defender, Microsoft puts better control and visibility of what runs on a Windows computer into the hands of that computer's operator.”

- **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, or external hard disk.
- **Instant Support** provides online and phone support 24 hours a day, seven days a week.

After being in beta for the duration of 2005, the Windows Live OneCare subscription service was officially launched in the United States in June 2006, and it is now available directly from the Web at <http://onecare.live.com> and from U.S. retailers. 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.

Windows Live OneCare Safety Scanner

To help support the Windows Live network and a healthier online ecosystem, the Windows Live OneCare safety scanner, <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. A full-service scan will 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 for free 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 7 million scans since its debut and detected almost 3 million instances of malware, spyware, or potentially unwanted files over the same period. As a result, the Windows Live OneCare safety scanner has cleaned more than 575,000 computers. In addition to the Windows Live OneCare safety scanner, the 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 family, which also includes services for e-mail archiving, e-mail encryption, and e-mail continuity. Microsoft acquired the hosted services in 2005 through the acquisition of FrontBridge Technologies.

Exchange Hosted Filtering operates “in the cloud” 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. The core of Exchange Hosted Filtering is a distributed network of data centers located at key sites along the Internet backbone. The data centers meet strict security standards, and Service Level Agreements for e-mail delivery time and network availability are included. The Exchange Hosted Filtering network processes more than 6 billion business e-mails a month for more than 4,000 enterprises worldwide.

“The core of Exchange Hosted Filtering is a distributed network of data centers located at key sites along the Internet backbone.”

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 that ensures 100 percent blocking of known viruses.
- **Spam protection:** Powered by multiple filtering engines and an around-the-clock team of anti-spam experts, Exchange Hosted Filtering virtually eliminates spam from inboxes. Performance is backed by a Service Level Agreement that ensures 95 percent of spam will be filtered and quarantined with no more than 1 in 250,000 messages being misclassified as spam.
- **Disaster recovery:** In the event 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-ruled writer enables users to monitor and manage messages based on virtually any message attribute, from originating IP to sender/recipient.

Microsoft Forefront Client Security

Microsoft Forefront Client Security delivers unified protection from current and emerging malware, so you can feel confident that your business systems are better protected 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 emerging threats, such as spyware and rootkits, as well as against traditional threats, such as viruses, worms, and Trojan horses. By delivering simplified administration through central management and providing critical visibility into threats and vulnerabilities, Forefront Client Security helps you protect your business with greater confidence and efficiency. Forefront Client Security integrates with your existing infrastructure software, such as Active Directory, and 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, so you can feel confident that your business systems are better protected.
 - One solution for spyware and virus protection
 - Built on protection technology used by millions of people worldwide
 - Effective threat response
- **Simplified administration** through central management, so you can protect your business with greater efficiency.
 - Define one policy to manage all protection agent settings on one or more protected computers.
 - Deploy malware protection signatures and software faster.
 - Integrate with your existing infrastructure.
- **Critical visibility and control** through insightful, prioritized security reports and a summary dashboard view, so you have visibility and control over malware threats.
 - View insightful reports.
 - Stay informed with state assessment scans and security alerts.

Forefront Client Security is currently in development. Microsoft plans to make a public beta of the product available to customers in the fourth quarter of 2006.

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

Microsoft Forefront Security for Exchange Server

Microsoft Forefront Security for Exchange Server helps businesses defend their Exchange 2007 e-mail environments against viruses, worms, and spam. Its tight integration with Exchange 2007, several scanning innovations, and flexible performance bias controls enable IT professionals to shield messaging servers from malicious intent while actually maximizing their availability and performance.

E-mail viruses remain the single most costly threat to businesses today in time and productivity losses. Whether virulent or benign, viruses, worms, spam, and other malware can cripple communications, overwhelm server resources, crash systems, and bring work to a halt.

And although nearly 97 percent of businesses used antivirus software in 2006, 65 percent of those businesses still suffered attacks from viruses, worms, and spam (CSI/FBI 2006 Survey).

Why? Because many companies rely on software that has only one antivirus scan engine to protect every device. A virus slips through while the engine is being updated, or the engine fails to recognize the latest risk. And a threat at one node, such as an Internet server on the perimeter, means trouble at every internal hub and mailbox, because they all use the same engine.

Overreactive defense practices create their own setbacks. Entire messages get blocked when only a part of them is suspect, leaving users without vital mail. Scanning every message at every server delays delivery. Installing multiple, competing antivirus products increases administrative troubles. Redundant scanning of years-old e-mail drains server resources.

It all adds up to slower e-mail delivery, greater enterprise vulnerability, hefty management and recovery costs, and lost productivity—all of which affect business success.

Microsoft Forefront Security for Exchange Server solves these problems by providing advanced, multilayered antivirus protection and improving the availability, performance, and management of Exchange 2007 messaging systems. Here is how:

- **Forefront Security for Exchange Server provides maximum threat protection by enabling IT professionals to run up to five scan engines at once, at multiple layers** throughout the Exchange 2007 infrastructure. When one engine goes offline for an update, the others are still active, protecting all periphery, hub, and storage servers—even mail coming from mobile devices.

“...Although nearly 97 percent of businesses used antivirus software in 2006, 65 percent of those businesses still suffered attacks from viruses, worms, and spam.”

– CSI/FBI 2006 Survey

- **Signature updates for each engine are rapid, secure, and automated**, giving companies unprecedented protection against the latest threats and single points of failure.
- **For premium spam protection, Forefront Security for Exchange ensures that all Exchange 2007 spam filters are always current.** And its file-filtering innovations can actually inspect file attachments and recognize files whose extensions have been changed. It can also pass along safe attachments while removing the unsafe ones, so users get the messages they need but without the tagalong viruses.
- **Forefront Security for Exchange uses the new antivirus technology of Exchange 2007** to eliminate repeat scanning of messages after they have safely passed the first server. Without redundant scanning in transit, mail flows faster, users get mail sooner, and servers don't stall from overload.
- **To enhance performance at storage servers, IT professionals can selectively scan stored e-mail** for only the most likely virus candidates (such as mail that is two to 36 hours old or that has attachments). Such intermittent background scanning keeps mail moving, increases reaction times during a crisis, and releases server resources from unnecessarily scanning megabytes of old mail.
- **Bringing all antivirus efforts under centralized management** leads to greater cost efficiency and ease. Forefront Security for Exchange not only manages all scan engines and their updates, it also includes Forefront Security Management Console for one-stop configuration and control of all antivirus activities.
- **Forefront Security for Exchange Server is designed to share data and information with Microsoft Operations Manager**, so virus data can become part of analysis and reporting. That means IT teams are less harried, and the company can make full use of its server and software investment.

The Microsoft Forefront Security for Exchange Server Beta is available for download today from <http://www.microsoft.com/forefront/serversecurity/exchange/download.msp>. The product is scheduled for release in the fourth quarter of calendar year 2006.

Microsoft Antigen for Exchange

Microsoft Antigen for Exchange helps protect your e-mail infrastructure from infection and downtime through an approach that emphasizes layered defenses, optimization of Exchange Server performance and availability, and enforcement of corporate content policies. Combining these protection technologies at multiple layers throughout the infrastructure helps stop the latest e-mail threats before they affect businesses and users.

- **Layered Defenses:** Antigen for Exchange protects organizations against the latest threats by managing multiple antivirus scan engines at multiple layers throughout the e-mail infrastructure.

This approach allows Antigen for Exchange to minimize the average window of exposure for emerging e-mail threats by providing continual signature updates from multiple antivirus labs around the world. Dual scanning at both the SMTP stack and the Exchange Information Store provides a further layer of protection.

The layered defenses of Antigen for Exchange also protect against downtime. If one engine fails or goes offline to update, other engines remain active to provide protection, ensuring mail delivery is not compromised or delayed.

- **Server Optimization:** Antigen for Exchange provides tight integration with the Microsoft Exchange platform, optimizing server performance and ensuring e-mail protection that doesn't overtax server resources—even during outbreaks. With features such as in-memory scanning, distributed, multithreaded scanning processes, and performance bias settings, businesses can achieve the benefits of multiple engine scanning without introducing additional mail processing time or server performance degradation.

