MSRT

Windows Malicious Software Removal Tool

Progress Made, Trends Observed

A White Paper from the Microsoft Antimalware Team

Matthew Braverman
Program Manager
Microsoft Antimalware Team

Microsoft

Acknowledgements
I would like to thank the following individuals for their contribution to this paper: Mike Chan, Brendan Foley, Jason Garms, Robert Hensing, Ziv Mador, Mady Marinescu, Michael Mitchell, Adam Overton, Matt Thomlinson, and Jeff Williams

The Windows Malicious Software Removal Tool: Progress Made, Trends Observed

Executive Summary

Microsoft has made significant investments over the past few years in the research of malicious software (or "malware") and in developing technology to help customers mitigate the security risk that it creates. As part of this investment, Microsoft has created a dedicated Antimalware team that is responsible for researching malicious software, spyware, and other potentially unwanted software, and the release and maintenance of the Windows Malicious Software Removal Tool (MSRT) and Windows Defender. The team also supplies the core antimalware technology (including the scanning engine and malware definition updates) to products such as Microsoft® Windows Live™ OneCare, Windows Live Safety Center Beta, Microsoft Antigen, and the upcoming Microsoft Forefront™ Client Security release.

Microsoft delivered the first version of the MSRT on January 13, 2005 in 24 languages to users of Microsoft Windows® 2000, Windows XP, and Microsoft Windows Server™ 2003 computers. The tool is designed to help identify and remove prevalent malware from customer computers and is available at no charge to licensed Windows users. As of the writing of this report, Microsoft has shipped 15 additional, enhanced versions of the tool and continues to ship a new version on the second Tuesday of each month, each adding new prevalent malware to detect and remove. Since the initial release of the MSRT, the tool has been executed approximately 2.7 billion times by at least 270 million unique computers.

This report provides an in-depth perspective of the malware landscape based on the data collected by the MSRT[1], and highlights the impact that the MSRT has had in reducing the impact of malware on Windows users. Key insights from the data are summarized below and are covered in greater detail in the body of the paper.

- **The MSRT has removed 16 million instances of malicious software from 5.7 million unique Windows computers over the past 15 months. On average, the tool removes at least one instance of malware from every 311 computers it runs on.**
- **41 of the 61 malware families targeted by the MSRT from January 2005 to February 2006 have been detected less frequently since being added to the tool with 21 of the families experiencing decreases greater than 75%.**
- **Backdoor Trojans, which can enable an attacker to control an infected computer and access confidential information, are a significant and tangible threat to Windows users.** The MSRT has removed at least one backdoor Trojan from approximately 3.5 million unique computers. Thus, of the 5.7 million unique computers from which the tool has removed malware, a backdoor Trojan was present in 62% of computers. Bots, a sub-category of backdoor Trojans which communicate through the Internet Relay Chat (IRC) network, represent a majority of the removals.
- **Rootkits, which make system changes for the purpose of hiding or protecting some other, possibly malicious components, are a potential emerging threat but have not yet reached widespread prevalence.** Of the 5.7 million unique computers that the tool has removed malware from, a rootkit was present in 14% of the cases; this figure drops to 9% if WinNT/F4IRootkit, the rootkit distributed on select Sony music CDs, is excluded. In 20% of the cases when a rootkit was found on a computer, at least one backdoor Trojan was found as well.
- **Social engineering attacks represent a significant source of malware infections.** Worms that spread through e-mail, peer-to-peer networks, and instant messaging clients account for 35% of the computers cleaned by the tool.
- **The malware problem appears to be migratory in nature.** Most of the computers cleaned with each release of the MSRT are computers from which the tool has never removed malware. In the March 2006 version of the MSRT, the tool removed malware from approximately 150,000 computers (20% of all computers cleaned) from which some malware had previously been removed by the tool in an earlier release.

[1] The tool does not collect any personally identifiable information (PII) and thus can not be used to tie a specific user to an infection report. For information on data collected by the tool, please refer to the Appendix. For Microsoft's definition of PII, please refer to the Microsoft Security Glossary at http://www.microsoft.com/security/glossary.mspx.

MSRT Overview

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). Versions of the tool are also made available for download from the Microsoft Download Center and as a Microsoft ActiveX® control on the http://www.microsoft.com/malwareremove Web site. The current release of the tool is capable of detecting and removing 61 distinct malware families.

In releasing and maintaining the MSRT, Microsoft has two main objectives:

1. To reduce the impact of prevalent malicious software on Windows users.
2. To use the data collected by the MSRT to assemble a reliable set of trends on the malicious software actually affecting Windows customers today. This data has been used by the Microsoft Antimalware team to focus development efforts and to minimize the time required to respond to malware submissions. In addition, through reports such as this, other security researchers can use this data to enhance their understanding of the malware landscape and focus on the shared goal of reducing the impact of malware to the Windows user base.

The tool does not target spyware and potentially unwanted software. Windows users should download and install an up-to-date antispyware application to detect and remove spyware and potentially unwanted software from their computers. Windows Defender, the antispyware solution from Microsoft, currently in beta at the time of this report, is offered to genuinely licensed Windows users at no charge at http://www.microsoft.com/windowsdefender.

The MSRT is not a replacement for an up-to-date antivirus solution, due to its lack of real-time protection and use of only the portion of the Microsoft antivirus signature database that enables it to target prevalent malicious software. However, we recommend that users who have up-to-date antivirus software installed also run the tool as a defense-in-depth measure. Such users also indirectly benefit from the MSRT because infected users can detrimentally impact shared resources, such as the Internet or a local area network.

We highly recommend that Windows users install and maintain an up-to-date antivirus solution offering real-time protection and a complete antivirus signature database. Microsoft Windows Live OneCare fulfills these requirements as do other products offered by Microsoft antivirus partners, listed at http://www.microsoft.com/security/partners/antivirus.asp.

Report Background

This report provides data and insight describing how Microsoft, through the release of the MSRT, has been able to make progress on its release objectives over the past 15 months: reducing the amount of prevalent malicious software affecting users, and obtaining valuable telemetry that functions as an essential road map for the current state of Windows malware. Additional reports which detail Microsoft's understanding of the malware landscape will be released in the future, with greater frequency, and with data from sources additional to the MSRT.

This report includes data up to and including the March 2006 release of the MSRT. Although newer versions of the MSRT have been made available since the release of this report, it was necessary to freeze the data at an earlier point to allow for processing, verification, and analysis. For a description of the data collected by the MSRT, please see the Appendix of this document.

The data used in this report was derived by measuring infections on customer computers, as reported by the MSRT. There are many other techniques in use today that are used to measure malware prevalence. Some measure requests to a network, others track the number of e-mail messages sent by threats. However, techniques such as these only monitor the number of copies of threats being distributed by infected computers, not the number of infected computers, as one infection can generate many copies of itself. Therefore, tracking specific infections is the most accurate method of determining malware infection prevalence. In the case of the MSRT, the relevance of the data becomes especially significant when the scale of the number of executions is considered.

The profiles of the users of the MSRT are varied but it is likely that most users, due to the release mechanisms, are home users or small businesses. Therefore, most of the data in this report reflects this audience. However, the trends and the guidance supplied throughout are applicable to all Windows users.

This paper will refer to the following malware-related terms:

- **Family** – A grouping of similar variants of malicious software. For example, Win32/Rbot is a malware family containing thousands of similar, yet distinct, variants.
- **Variant** – A specific piece of malicious software. For example, Win32/Rbot.A is a variant within the Win32/Rbot family.
- **Instance or infection** – The identification of a specific malware variant on a computer. Note that one instance includes all of the components (files, registry keys, etc.) of a single variant and that each time a malware variant is removed from a computer; it is counted as a separate instance. For example, if the tool removes Win32/Rbot.A and Win32/Rbot.B from a computer at the same time, this is counted as two infections or instances. If, three months later, the tool removes Win32/Rbot.A again from that same computer, that is counted as an additional infection.

Release Statistics

The main delivery vehicle for the Windows MSRT is through WU/MU/AU. Through this mechanism, the MSRT is executed on hundreds of millions of computers per month on a worldwide basis, providing a strong source of threat data for analysis.

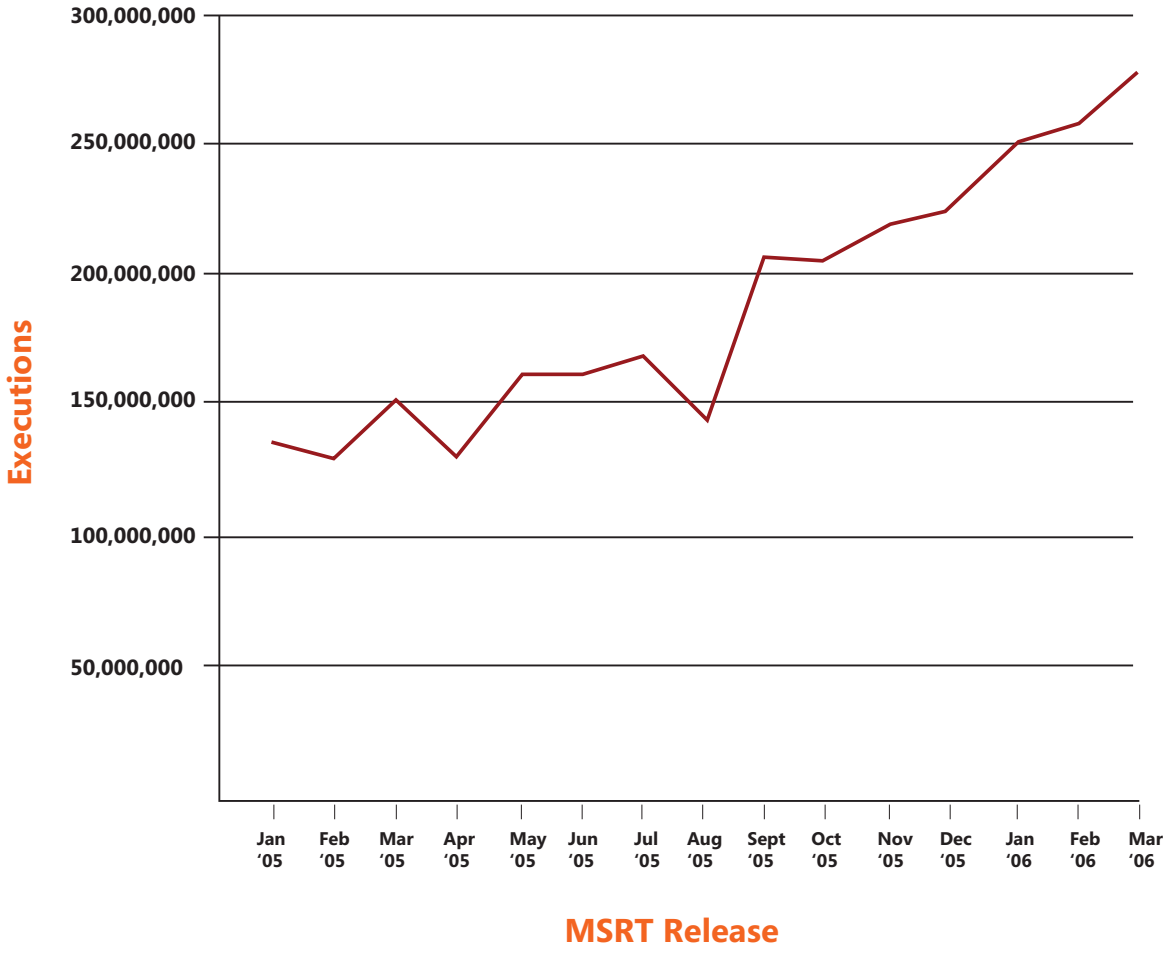

Figure 1. Executions of the MSRT through WU/AU/MU

Figure 1 illustrates the number of executions of the MSRT by unique computers for each of the 15 monthly releases from

January 2005 through March 2006. Note that, in this graph, the values listed as the categories for the X-axis of the graph refer to releases of the MSRT, not calendar months. For example, the February 2006 release of the MSRT was released on February 14, 2006 and then superseded by the March 2006 release on March 14, 2006. Also, note that the August out-of-band release in response to the Zotob worm is not listed in this figure, because it was released to the Microsoft Download Center and as an ActiveX control on the http://www.microsoft.com/malwareremove Web site, but was not released through WU/MU/AU.

As shown in Figure 1, with few exceptions, the executions of the MSRT have increased with each release. Particularly striking is the difference in the number of executions between the first release of the tool and the most recent release. Between those releases, the executions per release have more than doubled—from approximately 125 million to 270 million executions by unique computers. The difference is due to increased usage of WU and AU by Windows users which is, in turn, likely due to Microsoft initiatives such as Windows XP Service Pack 2, which recommended enabling AU, and the Protect Your PC initiative, in addition to partnerships with OEM vendors to ship new computers with Windows XP SP2 preinstalled. Summing the executions for each release produces the total number of executions of the MSRT through WU/AU/MU: approximately 2.7 billion since release.

The number of executions is also encouraging with respect to the increasing trend and current high number of computers accessing WU/AU on a regular basis. Increased and timely usage of these Microsoft update mechanisms can help decrease the impact of threats on customers.

Targeted Malware Details

Each month, members of the Microsoft Antimalware team research new prevalent malware threats to add to the next version of the MSRT. The criteria for how our team chooses new threats to be added to the MSRT is based on three factors:

- The threat must appear to be prevalent.
- The threat must be malicious or capable of inciting a malicious scenario.
- The threat should likely be actively running when the MSRT executes.

The first key requirement for new malicious software added to the MSRT is that the threat appears to be prevalent. To find new candidate threats and determine prevalence, the team uses a set of internal and external metrics. Key internal metrics include data gathered by the Windows Live Safety Center Beta (http://safety.live.com) and Windows Live OneCare both of which scan computers for the full set of malware threats known to Microsoft. The key external metric used is the WildList (http://www.wildlist.org), the de facto antivirus industry standard listing of prevalent malicious software and the basis for most antivirus product certifications such as the ICSA Antivirus Certification and West Coast Labs' Check-Mark, both of which were recently bestowed upon Windows Live OneCare.

The second requirement for items added to the tool is that they be malicious software (for example, viruses, worms, Trojans, bots, or rootkits). In most cases, this refers to replicating code, code that causes explicit damage, or code that can expose an affected system to compromise, or other security risks. The tool does not target spyware and potentially unwanted software.

The third requirement is that the malware is likely to be actively running on a computer. This requirement is a byproduct of how the tool runs through WU/MU/AU. Because, in most cases, the tool runs once a month, looks for malware actively running and in auto-start locations, and then exits without any resident components, the tool will only be effective if the malware is running at that time or linked to from an auto-start location. Thus, the tool does not target such threats as data file infecting threats, including Microsoft Word and Microsoft Excel® macro viruses.When a new family of malicious software is chosen to be added to the tool, all variants of that family are also included in that release. With each future release, any new variants of that family are added to the tool.

Malware Family	Email worm	P2P worm	IM worm	Exploit worm	Backdoor Trojan	Rootkit	Virus
Alcan		Yes					
Antinny		Yes					
Atak	Yes						
Badtrans	Yes						
Bagle	Yes				Yes		
Bagz	Yes						
Berbew					Yes		
Bobax	Yes			Yes			
Bofra	Yes						
Bropia			Yes				
Bugbear	Yes						
Codbot				Yes	Yes		
Doomjuice							
Dumaru	Yes						Yes
Esbot				Yes	Yes		
Eyeveg	Yes				Yes		
F4IRootkit						Yes	
FURootkit						Yes	
Gael							Yes
Gaobot					Yes		
Gibe	Yes						
Hackdef						Yes	
Hacty					Yes	Yes	
IRCbot					Yes		
Ispro						Yes	
Kelvir			Yes				
Korgo				Yes			
Lovgate	Yes				Yes		
Mabutu	Yes				Yes		
Magistr	Yes						Yes
Maslan	Yes	Yes		Yes	Yes		

Malware Family	Email worm	P2P worm	IM worm	Exploit worm	Backdoor Trojan	Rootkit	Virus
Mimail	Yes						
Msblast				Yes			
Mydoom	Yes				Yes		
Mytob	Yes		Yes	Yes	Yes		
Mywife	Yes						
Nachi				Yes			
Netsky	Yes						
Opaserv							
Optix					Yes		
Optixpro					Yes		
Parite							Yes
Purstiu							
Randex					Yes		
Rbot					Yes		
Ryknos					Yes		
Sasser				Yes			
Sdbot					Yes		
Sober	Yes						
Sobig	Yes						
Spybot		Yes			Yes		
Spyboter					Yes		
Swen	Yes	Yes					
Torvil	Yes	Yes					
Wootbot					Yes		
Wukill	Yes						
Yaha	Yes						
Zafi	Yes						
Zindos							
Zlob							
Zotob				Yes	Yes		

Figure 2. Malware Families Detected and Removed by the MSRT

Figure 2 lists the 61 malware families that the MSRT is capable of detecting in alphabetical order, as of the March 2006 release, classified into seven non-mutually exclusive categories. Although there are many different ways to classify malware, based on capabilities, replication vector, etc., the seven categories shown in the figure—e-mail worm, peer-to-peer (P2P) worm, instant messaging (IM) worm, exploit worm, backdoor Trojan, rootkit, and virus—provide a useful high-level classification system that will be used in the remainder of this document. As new malware variants in some of the above families are appearing on a daily basis, these classifications may change following the publication of this paper. Note that, in this figure, an exploit worm is defined as a threat that exploits at least one software vulnerability which permits execution of code without action from the user. Malware which exploit a vulnerability that does require user action (for example, viewing an e-mail message or navigating to a Web site) are not included in this category.

For a malware family to be associated with a category, all known variants must, by default, exhibit the behavior associated with that category. For example, only one variant of the Bagle family (Bagle.O) can be categorized as a virus because it infects executable files. Thus, the Bagle family is not characterized as a virus. As another example, many variants of the Rbot family are capable of exploiting software vulnerabilities. However, because in most of these cases manual intervention by the bot owner is required to trigger this form of replication, Rbot is not classified as an exploit worm. As shown above, a small amount of the families in Figure 2 do not fit into any of the seven categories.

Note that the MSRT is capable of detecting a small number of specific malware variants beyond the families listed above. These variants are dropped by the families listed above and are detected by the tool to provide an end-to-end disinfection experience.

Malware Removed By the MSRT

The remainder of this document will feature details about the malicious software that the MSRT has removed over the past 15 months, including high-level characteristics (for example, operating system versions, and locales) of the computers from which the malicious software has been removed.

Overview

To begin, the paper will illustrate the magnitude of the removals performed by the MSRT.

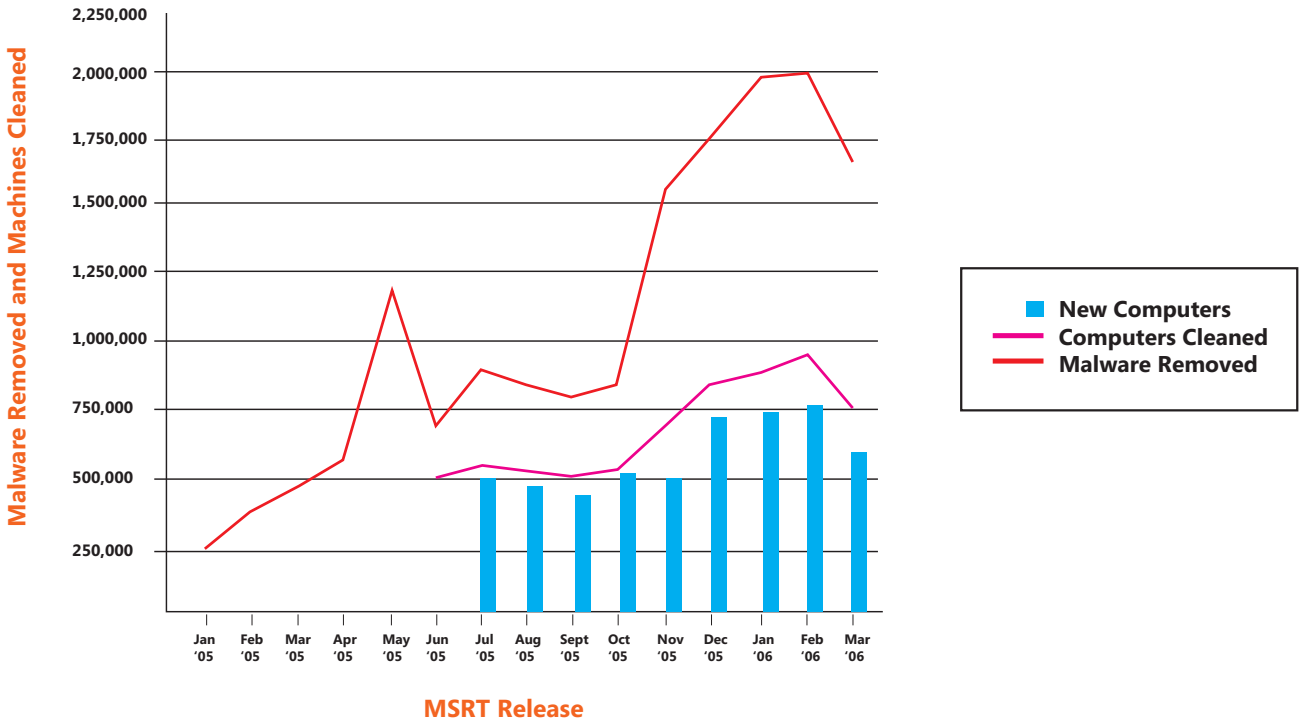

Figure 3. Malware Removed and Computers Cleaned Per MSRT Release

Figure 3 provides the following information through the three data series in the graph:

- **Malware Removed:** The number of malware removed by the MSRT for each release from January 2005 to March 2006. Across all releases, the tool has removed 16 million instances of malicious software.
- **Computers Cleaned:** The number of unique computers cleaned by the MSRT, per release, from June 2005 to March 2006. The number of unique computers cleaned per release will always be less than the number of instances of malware removed for that same release (multiple infections can be removed from a single computer). Also note that this data series begins in June 2005 because this was the first release that the tool began measuring this metric. From June 2005 to March 2006, the tool has removed at least one instance of malicious software from 5.7 million unique computers. The total number since the tool's initial release is larger than this figure but is unknown because data on this measurement is not available prior to June 2005.
- **New Computers**: From the number of total computers cleaned per release, the number of new, unique computers that the tool removed malware from with each release. Here, "new" refers to a computer that the tool has never removed malware from, including all previous releases of the MSRT. For each release, this value will never be greater than the number of total computers cleaned. As this figure is associated with the number of computers cleaned, the first release that can be measured is July 2005. Note that if a user reinstalls the operating system on his or her computer, this system will appear to be "new" to our telemetry. For this report, the bias introduced by this scenario is assumed to be small and is thus not taken into account.

There are several observations that can be made from the data shown in Figure 3:

- The increase in malware removed and computers cleaned are due to both an increase in executions of the MSRT (as shown in Figure 1) and an increase in the number of prevalent malicious software families and variants targeted by the tool. In particular, recent releases since November 2005 have seen a significant increase in the number of disinfections. Each of these increases is attributable to the inclusion of one or a set of specific prevalent malicious software families in the tool. As some of these families were discovered in the past and it is impossible to determine when a user was first infected, it would not be accurate to interpret this data as a rise in the amount of malicious software.
  - November 2005: A combination of Win32/Mabutu, Win32/Codbot, and Win32/Bugbear
  - December 2005: WinNT/F4IRootkit
  - January 2006: Win32/Parite
  - February 2006: Win32/Alcan
- Combining the data shown in Figure 1 with that shown in Figure 3 allows us to determine that, in the most recent March 2006 release of the MSRT, the rate of infected computers per executions of the tool was 0.28%. In other words, the tool removed malware from approximately one in every 355 computers on which it ran. The average rate across all releases from June 2005 to March 2006 is similar, at 0.32%, or approximately one in every 311 computers. This infection rate has remained relatively constant across the measurable releases, with the high being 0.4% in August 2005 and the low being 0.24% in September 2005.
- For each release, the majority of computers from which the tool removes malware are computers that the tool is removing malware from for the first time. Conversely, with each release, the tool removes malware from a comparatively small number of computers from which it has previously removed some malware. For example, in the March 2006 of the tool, approximately 600,000 out of 750,000 (80%) computers cleaned with the tool were new systems. In 20% of the cases, the tool had removed some malware from the same computers in a previous release. These removals represent the same computer being infected with a different malware variant or family as well as re-infections of the same malware variant (likely due to a non-patched computer or effective social engineering).

Malware Removed Per Computer

Another interesting metric to examine is the number of unique malware variants removed from each computer. In most cases the tool has only removed a single malware variant from a computer. However, in some cases the tool has removed dozens and even hundreds of malware from computers.

Malware Variants Removed	Computers	Malware Variants Removed	Computers	Malware Variants Removed	Computers	Malware Variants Removed	Computers
1	3,857,990	22	249	43	19	66	6
2	1,216,124	23	195	44	11	67	3
3	334,833	24	176	45	7	68	1
4	143,026	25	144	46	10	69	1
5	68,575	26	103	47	7	71	1
6	38,086	27	98	48	12	72	1
7	22,382	28	65	49	5	73	1
8	14,090	29	70	50	11	77	4
9	9,248	30	52	51	7	82	2
10	6,243	31	47	52	5	85	1
11	4,570	32	47	53	2	86	1
12	3,274	33	33	54	5	91	1
13	2,635	34	37	55	3	99	1
14	1,757	35	23	56	3	101	1
15	1,279	36	38	57	2	102	1
16	948	37	20	58	4	104	1
17	764	38	20	59	2	106	1
18	539	39	17	60	1	108	1
19	503	40	23	61	3	131	1
20	411	41	16	62	2	159	1
21	302	42	11	63	2	219	1
						251	1

Figure 4. Unique Malware Variants Removed Per Computer

Figure 4 shows the number of computers for which a certain number of unique, individual malware variants were removed across all executions of the tool on a computer. For example, if the tool removed the same malware variant twice from a computer, it is only counted in Figure 4 once. Using the data in Figure 4, we can determine that the average number of unique malware variants removed per computer is 1.59. In other words, the tool is slightly more likely to remove more than one malware variant per computer than just one variant.

In cases with a significant amount of removals, computers are usually infected with a variety of bot variants, likely because a user becomes infected with a single bot and then the bot owner uses that first backdoor to install other bots on that computer.

Win32/Antinny, a peer-to-peer worm that almost exclusively affects Japanese language computers, is also a threat which is known to have a high number of infections per computer. The reason is that Antinny uses a variety of social engineering tricks to entice user to download and run the worm. Thus, a user who is likely to execute the worm once and infect his/her computer is likely to do so multiple times.

Malware Removed Details

This section provides more detail on how the data provided in the above sections relates to the 61 malware families that the MSRT is capable of detecting and removing.

Rank	Family Names	Removals	Computers	First Added	First Discovered
1	Win32/Rbot	4,431,422	1,914,046	Apr-05	Aug-03
2	Win32/Sdbot	1,507,546	677,619	May-05	Apr-03
3	Win32/Parite	946,024	330,337	Jan-06	Oct-01
4	Win32/Gaobot	794,575	260,091	Jan-05	Nov-03
5	WinNT/FURootkit	762,662	386,304	May-05	Feb-05
6	Win32/Netsky	602,634	192,212	Feb-05	Feb-04
7	Win32/Alcan	571,488	344,028	Feb-06	Apr-05
8	Win32/Wukill	520,947	279,095	Oct-05	Sep-05
9	Win32/Bagle	450,245	199,958	Mar-05	Jan-04
10	Win32/Msblast	427,667	85,434	Jan-05	Aug-03
11	WinNT/F4IRootkit	420,494	250,227	Dec-05	Oct-05
12	Win32/Antinny	413,214	123,718	Oct-05	Aug-03
13	WinNT/Ispro	406,702	91,262	May-05	Feb-05
14	Win32/Berbew	379,982	120,305	Jan-05	Apr-04
15	Win32/Korgo	303,007	65,298	Feb-05	May-04
16	Win32/Mytob	293,762	187,138	Jun-05	Apr-05
17	Win32/Spybot	261,464	161,050	Jun-05	Aug-04
18	Win32/Lovgate	253,339	89,228	Jun-05	Mar-03
19	Win32/Wootbot	225,807	121,545	Jul-05	Sep-04
20	Win32/Hackdef	215,115	55,212	Apr-05	Mar-05
21	Win32/Mywife	155,932	73,117	Oct-05	Sep-05
22	Win32/Codbot	133,942	79,136	Nov-05	Feb-05
23	Win32/IRCbot	132,166	75,994	Dec-05	May-04
24	Win32/Purstiu	112,057	76,952	Jul-05	Jun-05
25	Win32/Nachi	101,716	62,508	Jan-05	Aug-03
26	Win32/Sasser	98,061	26,581	Jan-05	Apr-04
27	Win32/Mabutu	88,552	31,632	Nov-05	Jul-05
28	Win32/Sober	86,318	37,942	Mar-05	Feb-05
29	Win32/Bugbear	85,252	18,942	Nov-05	Sep-02
30	Win32/Esbot	80,782	65,905	Sep-05	Aug-05
31	Win32/Mydoom	80,670	22,906	Jan-05	Jan-04
32	Win32/Optixpro	65,664	39,526	Jul-05	Jul-04
33	Win32/Gael	65,031	40,728	Sep-05	Jul-05
34	Win32/Bropia	64,373	29,316	Mar-05	Jan-05
35	Win32/Spyboter	59,597	41,445	Aug-05	Apr-03
36	Win32/Bobax	43,509	22,700	Sep-05	Aug-05
37	Win32/Zlob	39,744	20,596	Mar-06	Mar-05
38	Win32/Zafi	33,216	9,771	Feb-05	Sep-04
39	Win32/Kelvir	27,222	22,991	Jun-05	Apr-05
40	Win32/Maslan	22,180	13,044	Jan-06	Jan-05
41	Win32/Sobig	19,336	6,371	Mar-05	Jan-03
42	Win32/Eyeveg	12,577	5,371	Feb-06	Aug-03
43	Win32/Ryknos	12,243	9,003	Dec-05	Nov-05
44	Win32/Bagz	11,861	6,416	Aug-05	Oct-04
45	Win32/Optix	8,581	6,398	Jul-05	Dec-01
46	Win32/Zotob	8,191	6,132	Sep-05	Aug-05
47	Win32/Dumaru	7,290	4,265	Aug-05	Aug-03
48	Win32/Randex	4,338	2,246	Feb-05	Dec-03
49	Win32/Swen	3,980	1,600	Nov-05	Sep-03
50	Win32/Mimail	2,822	1,148	Apr-05	Aug-03
51	Win32/Torvil	2,630	1,983	Mar-06	Sep-03
52	Win32/Yaha	1,926	1,504	Sep-05	Jun-02
53	Win32/Doomjuice	1,921	541	Jan-05	Feb-04
54	Win32/Magistr	1,362	681	Feb-06	Mar-01
55	Win32/Hacty	1,267	656	Jul-05	Jun-05
56	Win32/Goweh	1,110	379	Mar-05	Nov-04
57	Win32/Opaserv	442	162	Nov-05	Sep-02
58	Win32/Bofra	151	124	Jan-06	Dec-05
59	Win32/Gibe	106	77	Oct-05	Mar-02
60	Win32/Badtrans	103	62	Feb-06	Mar-03
61	Win32/Zindos	10	3	Jan-05	Jul-04

Figure 5. Malware/Computers Cleaned By Malware Family

Figure 5 lists all 61 malware families that the MSRT is capable of detecting as of the March 2006 release along with the following information:

- The number of times that the malware family has been removed from a computer from January 2005 to March 2006. The list is sorted in decreasing order by this value.
- The number of unique computers that the malware family has been removed from, from June 2005 to March 2006.
- The release of the MSRT for which detection of the malware family was first present in the tool.
- The month and year in which the first variant of the family was discovered.

Some interesting points to highlight about the data in Figure 5 include:

- Removals of Win32/Parite, Win32/Alcan, and WinNT/F4IRootkit rank amongst the highest despite detection for the families only being added to the tool within the last five releases. Parite, a file infecting virus, is especially interesting because it first appeared in 2001 and continues to be prevalent. This is likely due to the difficulty associated with completely cleaning Parite from a computer and its aggressive file infection routine. In fact, there are no significant correlations between number of removals and when the family was first discovered or when detection for it was first added to the tool.
- Bots (Rbot, Sdbot, and Gaobot) compose three of the top five slots in terms of total number of removals. The prevalence of these three malware families reinforce the point made in the executive summary regarding the pervasiveness of backdoor Trojans.
- Win32/Antinny, at #12, spreads via a Japanese file sharing network. The fact that the worm is almost exclusively found on Japanese language systems but is still ranked so high after only six releases means it was fairly prevalent within Japan and illustrates the threat of region/language-specific threats.
- Win32/Alcan, a little-known worm that replicates over peer to peer networks already has one of the highest removal figures after just being added to the tool in February 2006. The worm's prevalence is likely due to a number of fairly effective social engineering techniques it leverages, including masquerading as an application that encounters an error during install after being run.
- Win32/Zotob, which exploited a vulnerability addressed by Microsoft Security Bulletin MS05-039, was removed from only 6,132 computers, making it the least prevalent of all exploit worms listed. This makes sense given the vulnerability only affected Windows 2000 computers. Ironically, Win32/Esbot, at #30, which exploits the same vulnerability, was removed from 10 times as many computers compared to Win32/Zotob but received much less attention. Win32/Msblast, at #10, remains the exploit worm with the top number of removals.
- Similarly, while the Hacker Defender rootkit family usually receives most of the attention around "notable" rootkit families, it actually one of the least prevalent rootkits targeted by the tool. WinNT/FURootkit is the top rootkit removed by the tool and is often used to hide the presence of a backdoor Trojan installed on a computer.

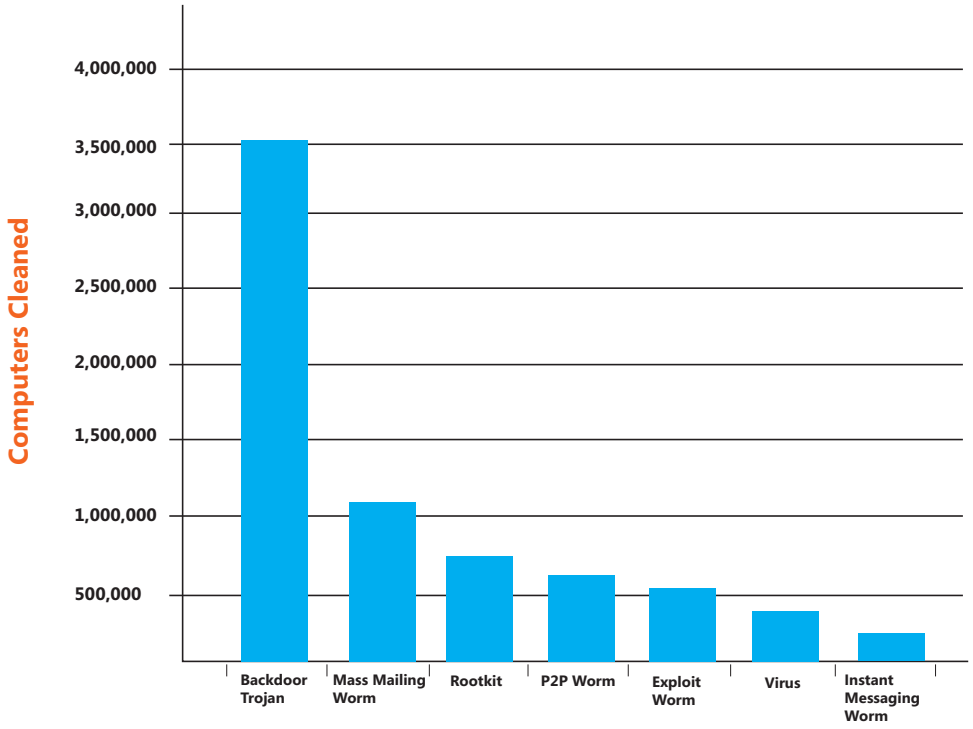

Figure 6. Computers Cleaned By Malware Type

Figure 6 combines the data shown in Figure 5 with the malware classifications established in Figure 2. Out of the 5.7 million computers cleaned, the MSRT has removed a backdoor Trojan from over 3.5 million (62%) of them. As documented by several recent high-profile cases, attackers frequently use these backdoor Trojans for financial gain by establishing networks of infected computers and selling them as relays and distribution points for spam, spyware, and denial of service (DoS) attacks. In addition to using an up-to-date antivirus solution, customers should leverage bidirectional firewalls to help prevent information disclosure and the remote monitoring/controlling aspects of these threats.

Compared to backdoor Trojans, rootkits were found on a much smaller number of computers: approximately 780,000. This figure drops to around 530,000, however, if detections of WinNT/F4IRootkit are ignored. This case is highlighted specifically because, while malicious software has subsequently appeared that leverages the rootkit to conceal itself on a computer, Sony did not release it as a malicious software package, but rather as anti-piracy functionality, and consequently had retail distribution characteristics rather than viral distribution characteristics. Naturally, as with the other malware categories discussed in this report, the data provided here is only relevant to the malware families that the tool is capable of detecting. Although there are known rootkits that are not detected by the tool due to low prevalence and, likely, unknown rootkits not detected by the tool, customer feedback and telemetry from such other Microsoft offerings as Windows Live OneCare and Windows Live Safety Center Beta indicate that the five rootkit families already targeted by the MSRT represent a significant portion of the rootkits actively affecting a large group of users today.

The most effective technique against rootkits is prevention. Customers are advised to keep their antivirus signatures up to date so the software's real-time protection mechanism is capable of detecting and blocking the rootkit before it can be installed on the computer and, where possible, to run as a non-administrator. Users who run as standard users will not have the ability to install most rootkits on their computers. Microsoft's next generation operating system, Microsoft Windows Vista™, also includes several features to help block rootkits from tampering with the operating system's key internal structures. In the case that prevention is not possible and a computer is already affected by a rootkit, customers should utilize an antivirus product or removal tool capable of detecting and removing the rootkit. In this case, users, especially corporate users, should weigh the trade-offs of taking additional steps to resolve the situation.

In terms of social engineering threats, e-mail is the most common form of the techniques shown above with about 20% of the computers cleaned being infected with at least one threat capable of spreading through e-mail. Although the MSRT is capable of detecting and removing three of the top instant messaging worms (Win32/Bropia, Win32/Kelvir, and Win32/Mytob), these threats have been found on a comparatively small number of computers: just less than 250,000. Compare this to the 450,000 or so computers cleaned of Win32/Alcan and Win32/Antinny alone, which spread through P2P networks. Malware that spread through a P2P network have the capability to detect if popular P2P applications are installed on a computer. If so, they will create copies of themselves, usually using enticing names, in the directories that the P2P applications use to share files on the network. In doing so, the worm is then shared on the P2P network. In addition to up-to-date antivirus software, the best techniques against such social engineering threats are user education and limiting the impact of executing a threat by running as a non-administrator.

One of the reasons recent IM threats have been less successful in spreading to a widespread audience compared to P2P threats is that IM programs are beginning to build in features that help prevent users from infecting themselves with malware. For example, MSN® Messenger version 7 prevents users from sending files with certain executable file types, and clicking links within instant messages requires additional user consent. Such protections have not yet been integrated into P2P client programs. The other significant reason for this difference is that P2P applications, as a mechanism for exchanging files, are much more suited to the spread of malicious files compared to IM programs, which focus more on messaging.

	Email Worm	P2P Worm	IM Worm	Exploit Worm	Backdoor Trojan	Rootkit	Virus
Email Worm	-	1.0%	1.4%	2.7%	8.2%	0.6%	1.4%
P2P Worm	1.9%	-	1.0%	1.8%	14.3%	1.0%	2.9%
IM Worm	7.0%	2.7%	-	7.0%	17.3%	1.6%	0.5%
Exploit Worm	5.3%	2.0%	0.7%	-	5.3%	3.6%	1.0%
Backdoor Trojan	2.7%	2.6%	1.2%	4.7%	-	4.3%	0.7%
Rootkit	0.9%	0.8%	0.5%	2.7%	19.5%	-	0.4%
Virus	4.3%	4.9%	0.3%	1.5%	6.2%	0.8%	-

Figure 7. Correlation of Malware Infections by Type

Figure 7 shows the overlap between the detections of the above malware types on a computer. Of all the computers on which MSRT detected an e-mail worm, MSRT also detected a P2P worm in 1.0% of those cases. Conversely, in 1.9% of the cases where the tool detected a P2P worm an e-mail worm was also detected.

The largest correlation shown above is between rootkits and backdoor Trojans. In approximately 20% of the cases in which a rootkit was found on a computer, at least one backdoor Trojan was found as well. This emphasizes the trend of a large number of rootkits being distributed or leveraged by backdoor Trojans. The percentages are also high between P2P worms and backdoor Trojans and IM worms and backdoor Trojans. The high values here are also expected given that many P2P worms and IM worms will often drop bots on the computer when they are run.

Changes in Malware Removals

Tracking changes in malware family removals by the tool is useful for two reasons. First, it allows Microsoft to monitor activity and prevalence of specific malware families. Families that experience increases in removals since first being added to the release usually indicate cases in which variants are being actively released and replicating. Tracking changes in removals is also useful because it allows Microsoft to monitor the success of the MSRT by ensuring that variants of the malware families detected by the tool are decreasing in prevalence. Although other factors may be due to the decrease, the fact that the MSRT has removed a significant amount of instances of these malware families from computers means that the release is at least partially responsible for decreases in prevalence.

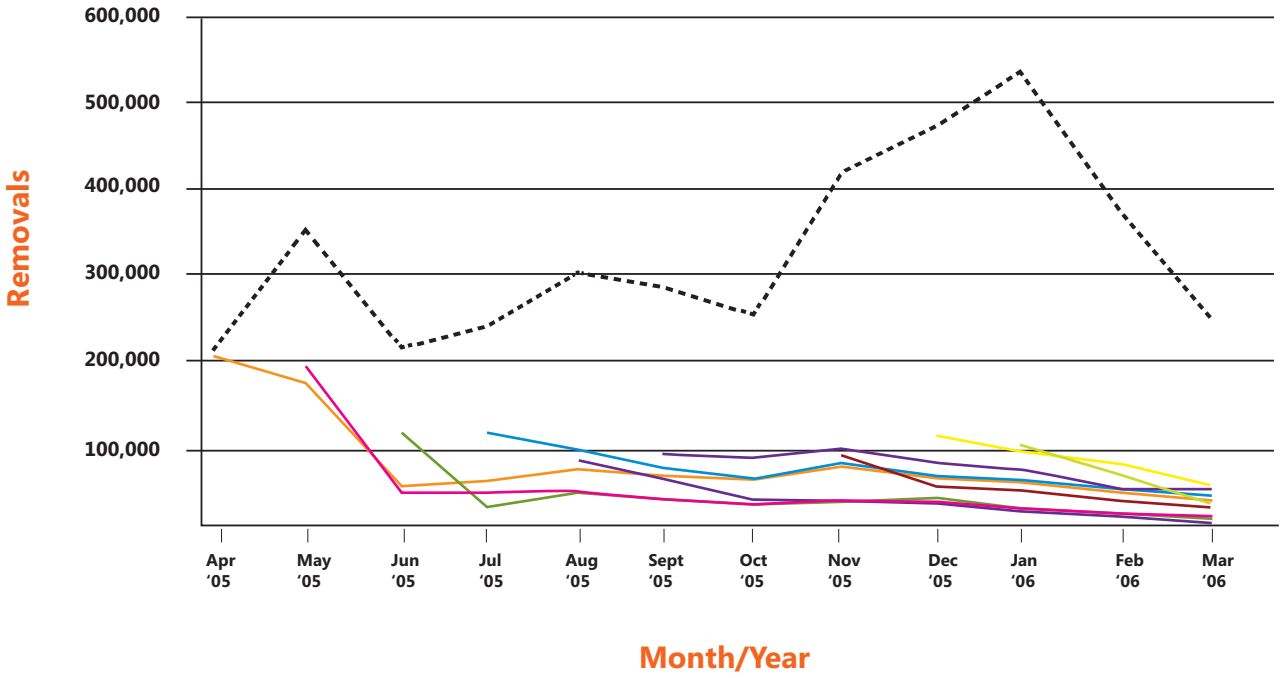

Figure 8. Change in Win32/Rbot Removals

Microsoft

Microsoft tracks the change in malware removals by the MSRT with two metrics which are mapped to the reasons described above. Figure 8 provides an illustration of these metrics using the Win32/Rbot family. Note that the X-axis corresponds to calendar months and years. Using the date in this model is important to show progression over time. Given that users are able to run older versions of the MSRT (although a warning screen is shown 60 days after release), using the MSRT release month would skew this measurement.

- **Family Change** (black dotted line): The change in removals for a family from the time detection for it was first added to the tool to the latest release. Although this provides an excellent view into how removals of a family have changed over time it is skewed by families which are active and which, when first added to the tool, encountered a small number of removals. The graph shows the total number of removals of the Win32/Rbot family from April 2005 to March 2006. Using this data, we can calculate that the number of removals of this family has increased by approximately 16% over the past 11 months. Given this information and the data from Figure 5, we can conclude that Rbot is a very active and prevalent family. Note that, graphically, this data series represents the sum of the solid lines below it.
- **Average Per-Release Change** (solid lines): The change in the number of removals for a specific set of variants added to a single release from the time the set was first added to the tool to the latest version of the tool, averaged across all releases. This metric is resistant to the large number of removals produced by active malware families and is thus a better measure for determining how well the tool has done at reducing the instances of a family in the wild. In the graph, the solid lines represent the number of removals from a set of Win32/Rbot variants added to a specific release, over time. The longer the line, the longer the detections have been in the tool. For example, the longest, orange line represents the first set of Rbot variants added to the tool. The general observation here is that when detection for a set of Rbot variants is added to the tool, the number of removals of those variants have eventually decreased. If we calculate the change in removals for each of those sets of variants over time and then take the average of those changes, we find that removals of Rbot variants have decreased by approximately 79% since being added to the MSRT.

Rank	Malware Family	Family Change	Avg. Per-Release Change
1	Win32/Esbot	-97%	-64%
2	Win32/Sobig	-94%	-94%
3	Win32/Swen	-94%	-94%
4	Win32/Zafi	-94%	-94%
5	Win32/Mabutu	-93%	-68%
6	Win32/Bropia	-93%	-82%
7	Win32/Spyboter	-92%	-95%
8	Win32/Korgo	-92%	-38%
9	WinNT/F4IRootkit	-91%	-91%
10	Win32/Mimail	-91%	-91%
11	WinNT/Ispro	-88%	-88%
12	Win32/Eyeveg	-86%	-86%
13	Win32/Optix	-86%	-86%
14	Win32/Msblast	-83%	-83%
15	Win32/Yaha	-83%	-83%
16	Win32/Sasser	-83%	-83%
17	Win32/IRCbot	-82%	-77%
18	Win32/Netsky	-79%	-79%
19	Win32/Berbew	-79%	-54%
20	Win32/Purstiu	-78%	-87%
21	Win32/Codbot	-76%	-67%
22	Win32/Bugbear	-74%	-74%
23	Win32/Wootbot	-72%	-75%
24	Win32/Spybot	-71%	-84%
25	Win32/Sdbot	-70%	-83%
26	Win32/Dumaru	-70%	-63%
27	Win32/Randex	-69%	-43%
28	WinNT/Alcan	-67%	-67%
29	Win32/Zotob	-64%	-49%
30	Win32/Sober	-64%	-86%
31	Win32/Antinny	-63%	-62%
32	Win32/Mytob	-57%	-77%
33	Win32/Doomjuice	-57%	-53%
34	Win32/Maslan	-49%	-49%
35	Win32/Mydoom	-45%	-67%
36	Win32/Bagle	-31%	-85%
37	Win32/Bagz	-30%	-66%
38	Win32/Gaobot	-28%	-79%
39	Win32/Goweh	-19%	-19%
40	Win32/Parite	-12%	-12%
41	Win32/Magistr	-5%	-5%
42	Win32/Optixpro	7%	-19%
43	Win32/Kelvir	11%	-48%
44	Win32/Bobax	12%	-24%
45	Win32/Rbot	16%	-79%
46	WinNT/FURootkit	38%	-36%
47	Win32/Gael	46%	46%
48	Win32/Lovgate	86%	86%
49	Win32/Wukill	170%	32%
50	Win32/Nachi	278%	-15%
51	Win32/Ryknos	509%	-92%
52	Win32/Hackdef	842%	-31%
53	Win32/Mywife	2675%	-50%

Figure 9. Changes in Malware Removals

Figure 9 shows most of the malware families detected by the tool along with the two measures for removal changes discussed above, arranged by percentage of family change in increasing order. Note that the three families added in the March 2006 release of the tool (Win32/Atak, Win32/Torvil, and Win32/Zlob) are not included in this listing because there has not yet been an opportunity to determine a change in the number of removals. In addition, Win32/Bofra, Win32/Gibe, Win32/Opaserv, Win32/Badtrans, and Win32/Zotob are excluded because there are not enough removals (at least 1,000) to generate a reliable change metric.

As indicated by the figure, it is encouraging to see that the majority of the families (41 of 53) have decreased in prevalence since being added to the tool with 33 of the 41 families exhibiting more than a 50% decrease and 21 of the 41, more than a 75% decrease. Of the 12 families that have increased in prevalence overall, only three (Win32/Gael, Win32/Lovgate, and Win32/Wukill) have seen, on average, a consistent increase in each set of variants added to the tool. The remaining nine families (including, as shown in Figure 8, Win32/Rbot) have all experienced a net decrease in removals per release. Other highlights of this data include:

- Removals of WinNT/F4IRootkit, the First4Internet rootkit distributed with certain Sony music CDs, have rapidly decreased since detection was first added to the release in December 2005. This likely indicates that few users installed/re-installed the software from affected CDs after the media attention that this issue garnered.
- The rapid growth in Mywife removals is due to the inclusion of Win32/Mywife.E in the tool. Mywife.E appeared in late January 2006 and was also referred to as CME-24 and the Kama Sutra worm by the news media. The worm spread predominantly over e-mail and was capable of damaging key data files on the third day of every calendar month. In this case, the removals shot up from about 700 removals in January 2006 to about 92,000 in February 2006.
- The increase in Win32/Rbot removals is due to a large number of variants of that malware family being added to the MSRT each release. On average, approximately 2,000 new variants of Win32/Rbot have been added to the tool each month.
- Increases of removals of such families as Win32/Hackdef and Win32/Ryknos are due to the number of initial removals being low which is, in turn, due to the number of variants initially detected by the tool also being low. For example, the April 2005 release of the MSRT was capable of detecting 78 different variants of the Win32/Hackdef family. The number of variants dramatically increased to 439 in March 2006, representing more than a 400% increase. Similarly, the number of removals increased from about 3,000 to 30,000 during that time. Thus, although the number of Hackdef removals is still comparatively low to other malware families, they have increased significantly since detection of the family was added to the tool. These trends are evident from the change metrics for this family, shown in Figure 9. Although there has been a large increase in removals (842%), this figure is exacerbated by the fact that removals of the family began with a low figure. Removals of the family, per release, have decreased by an average of 31%.

OS Information

Using the telemetry information collected by the MSRT, Microsoft is able to determine the prevalence of the threats detected on the supported versions of Windows. Figure 10 shows various views of the malware prevalence across these operating systems for the March 2006 release.

The first two pie charts reflect all malware detected by the tool during the March 2006 release. In the chart labeled "Total", you can see that most of the removals are from Windows XP SP2, with Windows XP composing 89% of all removals by the tool. This high number of disinfections from Windows XP SP2 computers is expected because most of the executions of the tool are on Windows XP SP2 computers. Therefore, to get a more realistic view of what malware is more common on certain operating systems, the data in the first figure can be "normalized."

In this case, normalization means adjusting the disinfection percentage across operating systems to take into account the number of executions of the tool on that operating system. In other words, to reduce the bias in the disinfection percentage introduced by a high number of executions from an operating system, we divide the number of disinfections from a specific operating system by the relative percentage of executions from that operating system. Thus, those operating systems with a large percentage of executions will have the number of disinfections increased by a smaller amount compared to an operating system with a low percentage of executions.

The specific mathematical formula used in this case is the following:

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

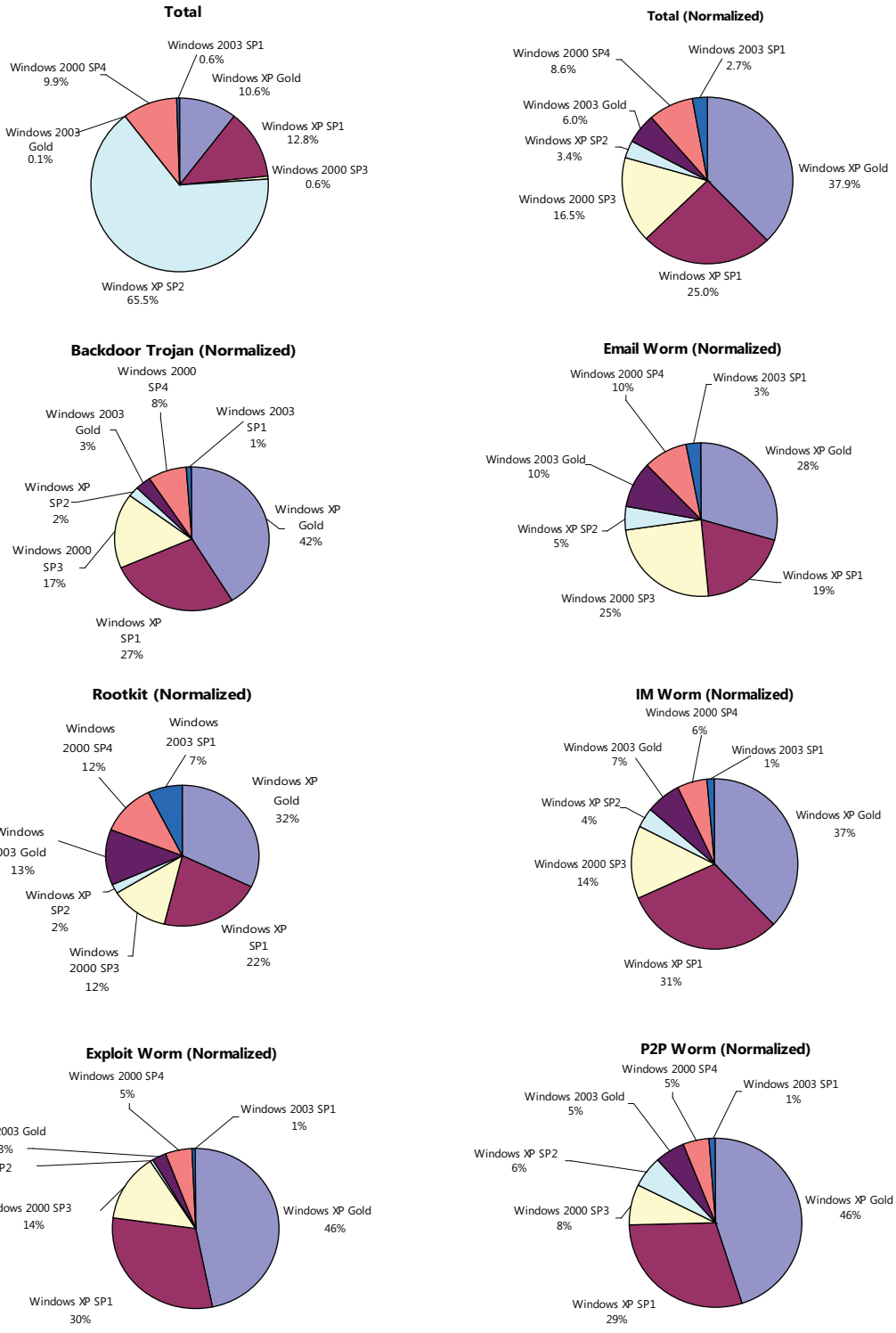

Figure 10. Computers Cleaned by the March 2006 Release, by Operating System

Microsoft

Applying this formula to the disinfection and execution percentages for the March 2006 release yields the graph in the upper-right corner of Figure 10. The graph shows a dramatic change in the percentages with Windows XP SP2 dropping to only 3% of the normalized disinfections and Windows XP Gold and SP1 accounting for 63% of the disinfections. This arrangement makes sense for both technical and social reasons. For the former, Windows XP SP2 includes a number of security enhancements and patches for vulnerabilities not found in earlier versions of Windows XP, making it more difficult to be infected by malware in some cases. For the latter, it is likely that a user who has not yet upgraded to the latest service pack would be more susceptible to attacks based on social engineering attacks. This also seems to hold true for Windows 2000 and Windows Server 2003, in which the latest versions of the service packs for those operating systems have the lowest number of normalized disinfections compared to the older versions of the operating systems.

The six graphs following the two main charts show the normalized disinfections broken down by the same categories shown in Figure 2. In general, the results from these graphs are similar to the normalized results when all disinfections are taken into account. In fact, the ordering of the operating systems is identical in all cases. When looking at Windows XP SP2 specifically, it is interesting to see that the highest percentages for disinfections of this operating system are from threats that spread over e-mail, instant messaging, and peer-to-peer networks. This arrangement is expected, because these threats, in contrast to exploit worms, for example, use social engineering attacks to infect a computer, a method to which all operating systems are susceptible.

Locale Information

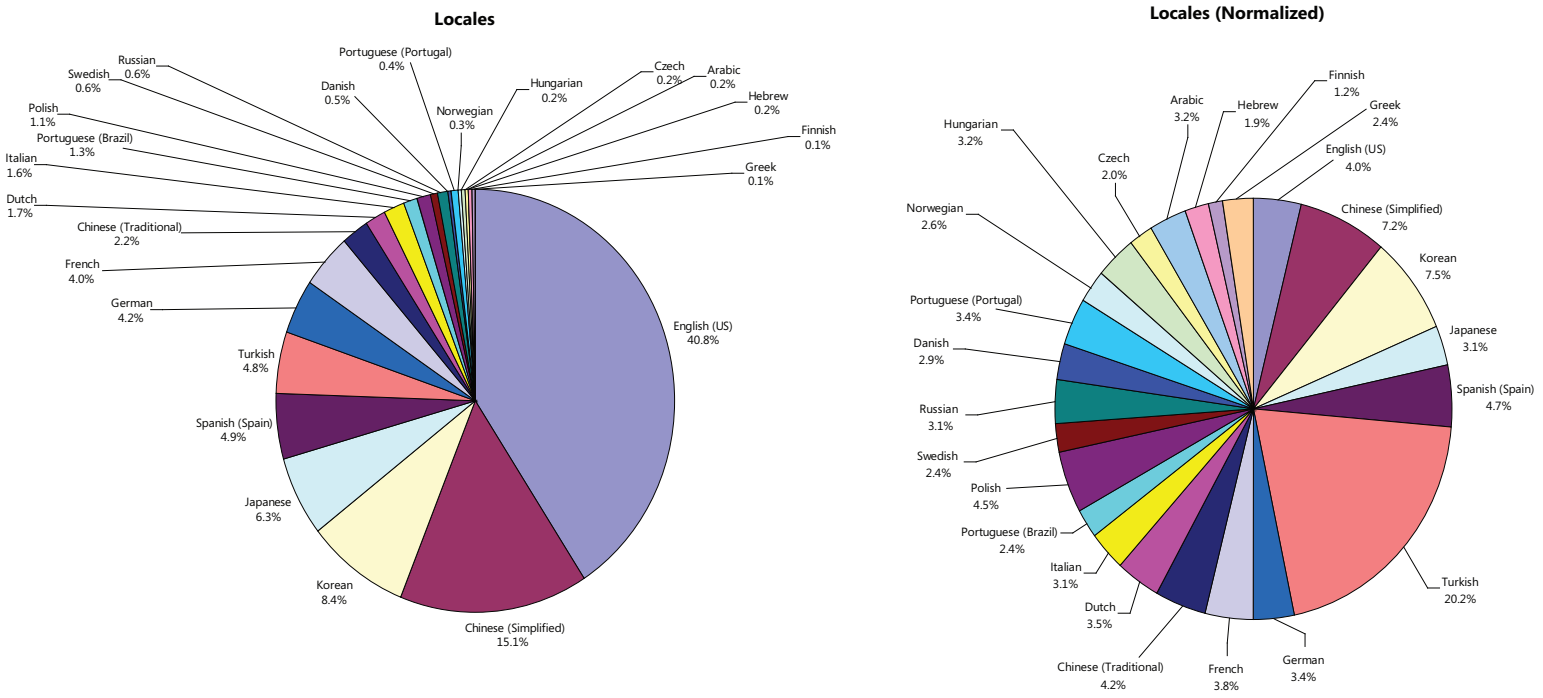

Figure 11. Computers Cleaned by the March 2006 Release, by Locale

Figure 11 shows the breakdown of computers cleaned by operating system locale for the March 2006 release of the MSRT. Note that the locale is not necessarily indicative of geographical location. For example, English (US) is fairly popular in other countries around the world. The chart on the left side of Figure 11 shows that a large amount of the computers cleaned have an English language OS. However, similar to the case with Windows XP SP2 above, this metric is slightly deceptive because a large amount of the computers on which the tool is run have an English language OS installed. Therefore, similar to operating system versions, the computers cleaned can be normalized by the execution percentage of a locale. The calculation is similar to the one performed for operating system version, with Execution Percentage$_{Locale}$ used in place of Execution Percentage$_{OS}$.

The result of this calculation is displayed in the right side of Figure 11 and yields interesting results. Here, the normalization process has divided the disinfections quite fairly amongst the majority of locales. In other words, when all malware removed by the tool is taken into account and the values are normalized, the removals of that malware are spread across all Windows locales, including English. As evident in the graph, the exception to this statement is the Turkish locale, which accounts for 20.2% of the computers cleaned post-normalization. A deeper drill-down into the data shows that this pattern is similar across all malware families. Although the Microsoft Antimalware team is continuing to research this data, the specific reason for why a high percentage of normalized detections come from Turkish language computers is unknown.

Conclusions

Looking back, the past 15 months have been an exciting period of time for the Microsoft Antimalware team and our intra-company partners, with the release of the Windows Malicious Software Removal Tool, the Windows Defender Beta, Windows Live OneCare Beta, and the Windows Live Safety Center Beta. The next 15 months promise to be just as exciting with full releases of these offerings expected in addition to the launch of Microsoft Forefront™ Client Security, a unified malware protection solution for desktops, laptops, and server operating systems that is easier to manage and control, and the continued delivery of the MSRT.

The introduction of these offerings will provide Microsoft with additional sources of data on the prevalence of malicious software, similar to the data collected by the MSRT. The collection of this information is important to Microsoft's understanding of the threat landscape and efforts to combat these threats and improve the overall computing experience for Microsoft customers. For example, the identification of bots as a significant majority of the detections by the MSRT resulted in the development of several automated analysis and signature generation techniques for these threats by the Antimalware response team. This has dramatically increased the output of signatures and the team's ability to respond to the appearance of new bots.

Microsoft believes that there is significant value in sharing this information with partners and customers, not only to demonstrate the impact of our tools and products on the threat landscape, but also to share our knowledge. This report is the first significant example of sharing such information; more will follow in the future and with increased frequency. Our hope is that others in the security industry can use this data to enhance our common understanding of the malware landscape and focus on the shared goal of reducing the impact of malware to the Windows user base.

Appendix

MSRT Background

In late 2003, Microsoft acquired assets from GeCAD Software, a provider of antivirus technology, allowing the Microsoft Security Technology Unit (STU) to begin investigating tools and technologies related to antivirus software. The first release to benefit from this acquisition was the Blaster Worm Removal Tool, which the STU's Antimalware team shipped in January 2004, in response to information from Microsoft's Internet service provider (ISP) partners that Blaster was still a threat at that time. The tool was capable of removing all known variants of Msblast and Nachi at the time and was deployed to infected computers through Windows Update. Users who were likely to be infected were offered the tool through Windows Update (WU)/Automatic Updates (AU), allowing Microsoft to obtain key telemetry about the prevalence of Msblast and Nachi in 2004 and resulting in the removal of these malware from over 10 million customer computers. Subsequent and independent cleaner tools were released in March 2004 and May 2004 to detect and remove Mydoom and Berbew, respectively.

Microsoft received positive feedback from customers that these one-off cleaner tools were valuable, but many asked for a more consistent, predictable system. This feedback resulted in the creation of the Windows Malicious Software Removal Tool (MSRT).

Key features of the release are as follows:

- The tool is released once a month, on the second Tuesday of the month, with any security updates for that month. If necessary, the tool is released out-of-band of this schedule for high-priority threats. So far, Microsoft has only shipped one out-of-band update of the tool, which occurred in August 2005 to counteract the Zotob worm. Because the spread of the Zotob worm was anticipated to be limited to specific organizations running Windows 2000, the update was only distributed through the Microsoft Download Center and the Web site.
- All monthly releases of the tool are distributed simultaneously to Microsoft Update (MU), WU, AU, the Microsoft Download Center, and the MSRT Web site at http://www.microsoft.com/security/malwareremove/default.mspx.
- Each release of the tool is cumulative, including all threats added from previous releases of the tool.
- When delivered through WU/MU/AU, each release of the tool runs only once and then exits. If any malicious software is found and removed, the tool provides a message to the user after the next reboot. If no malicious software is found, no messages or user interface is shown to the user. Users who want to run the tool more than once a month, on-demand, can download a copy from the Microsoft Download Center at http://www.microsoft.com/malwareremove.
- By default, the tool only looks for malware that are currently running or linked to through an auto-start point, such as in the registry. The tool was designed this way to minimize the execution time, especially through WU/AU.
- The tool is instrumented so that it can easily be deployed and managed by corporate customers. Specific target scenarios include distribution through Microsoft System Management Server (SMS) or a similar application management system and execution of the tool at each system logon or startup. Administrators who implement the tool in one of these scenarios can use the status codes returned by the tool (listed in KB891716) to monitor its rollout and status. The tool is also available for deployment through Windows Server Update Services (WSUS).

The tool's size is kept as small as possible to accommodate customers with limited bandwidth. In June 2005, the tool began to utilize delta updates through WU/MU/AU. In this scenario, users who have run a recent version of the tool are offered a smaller update (essentially the difference between what the user already had on his/her system and the most recent version). Currently, approximately 80% of WU/MU/AU users leverage these smaller updates, resulting in an average savings of one megabyte (MB) per user and approximately 80 terabytes (TB) of saved data per release.

Data Collection Details

To enable the Microsoft Antimalware team to obtain accurate data about the state of malware within the Windows ecosystem, the MSRT collects select infection-related information from customer computers, none of which can be used to personally identify a specific user. Note that this information is only sent to Microsoft in the event that the tool detects any malicious software on a computer. Users also have an option to prevent the software from reporting back to Microsoft by modifying the registry. The tool does not transmit any information back to Microsoft on computers that are updated by a WSUS server.

The following information is sent back to Microsoft:

- The name of the malicious software detected on the computer.
- The result of attempting to remove the malicious software.
- The operating system version, including the service pack number.
- The locale of the operating system.
- The processor architecture.
- The version number of the tool.
- An indicator that denotes whether the tool is being run from WU/AU, from the Download Center, or from the MSRT Web site.
- An anonymous GUID that is used to track the number of unique computers that have removed malware. It is generated explicitly for this scenario.
- A cryptographic one-way hash (MD5) of the path and file name of each malicious software file that is removed from the computer. The path and file name themselves are not sent as this could be considered personal information.

In cases in which the tool detects software on a computer that may be malicious, users are prompted to send the file(s) to Microsoft along with the cryptographic one-way hash (MD5). The Microsoft Antimalware team analyzes the submissions and adds them to the threat database if necessary.