MSRT

Windows Malicious Software Removal Tool

取得的进展和观察到的趋势

Microsoft 反恶意软件小组编写的白皮书

Matthew Braverman
项目经理
Microsoft 反恶意软件小组

Microsoft

致谢
我们要感谢下列人员对本文的贡献：Mike Chan、Brendan Foley、Jason Garms、Robert Hensing、Ziv Mador、Mady Marinescu、Michael Mitchell、Adam Overton、Matt Thomlinson 和 Jeff Williams

Microsoft

Windows 恶意软件删除工具：取得的进展和观察到的趋势

摘要

在过去几年中，Microsoft 投入大量资金研究恶意软件和开发能够帮助客户降低恶意软件带来的安全风险的技术。作为这项投资的一部分，Microsoft 组建了一个专门的反恶意软件小组，负责研究恶意软件、间谍软件和其他可能有害的软件，同时还负责发布和维护 Windows 恶意软件删除工具 (MSRT) 和 Windows Defender。该小组还为 Microsoft® Windows Live™ OneCare、Windows Live Safety Center Beta、Microsoft Antigen 以及即将发布的 Microsoft Forefront Client Security 等产品提供核心反恶意软件技术（包括扫描引擎和恶意软件定义更新）。

2005 年 1 月 13 日，Microsoft 以 24 种语言向 Microsoft Windows® 2000、Windows XP 和 Microsoft Windows Server™ 2003 计算机用户提供 MSRT 的第一个版本。此工具旨在帮助识别并删除客户计算机中的流行恶意软件，而且向获得许可的 Windows 用户免费提供。截止到编写本报告时为止，Microsoft 已经发布了此工具的 15 个附加增强版本，并且在每月的第二个星期二继续发布新版本，每个新版本都会增加可检测并删除的新流行恶意软件。自第一次发布 MSRT 以来，此工具已经由至少 2.7 亿台计算机执行了大约 27 亿次。

本报告根据 MSRT1 收集的数据提供对恶意软件现状的深刻见解，并重点介绍 MSRT 在减少恶意软件对 Windows 用户造成的影响方面所取得的成绩。根据这些数据得出的主要观点总结如下，将在本文的正文部分详细讨论。

- **在过去 15 个月中，MSRT 已经从 570 万台 Windows 计算机中删除了 1600 万个恶意软件实例。平均起来，此工具在运行它的计算机中每 311 台计算机至少删除一个恶意软件实例。**
- **在 MSRT 从 2005 年 1 月到 2006 年 2 月所查找的 61 个恶意软件系列中，41 个系列自添加到此工具以后被检测到的频率减少，其中 21 系列的降幅达 75% 以上。**
- **后门特洛伊木马 (Backdoor Trojan) 使攻击者能够控制被感染的计算机并窃取机密信息，对 Windows 用户是切实存在的重大威胁。**MSRT 已经从大约 350 万台计算机中每台至少删除了一个后门特洛伊木马。因此，在此工具从中删除了恶意软件的 570 万台计算机中，62% 的计算机存在后门特洛伊木马。自动程序 (Bot) 是通过 Internet 中继聊天 (IRC) 网络传播的一种后门特洛伊木马，在删除数量中占大多数。
- **Rootkit 为了隐藏或保护某些其他可能为恶意的组件而进行系统更改，是新出现的潜在威胁，但尚未大范围发作。**在此工具从中删除了恶意软件的 570 万台计算机中，14% 的计算机存在 rootkit；如果排除在某些 Sony 音乐 CD 上分布的 WinNT/F4IRootkit，这个数字会下降到 9%。在发现 rootkit 的计算机中，20% 的计算机同时至少发现一个后门特洛伊木马。
- **社会工程攻击也是恶意软件感染的主要来源。**在此工具清理的计算机中，通过电子邮件、对等网络和即时消息客户端传播的蠕虫占 35%。
- **恶意软件问题似乎天生具有迁移性。**在每次发布的 MSRT 清理的计算机中，大多数是此工具从未从中删除恶意软件的计算机。在 2006 年 3 月的 MRST 版本从中删除了恶意软件的计算机中，此工具的较早版本先前从中删除恶意软件的计算机大约为 15 万台，占全部清理计算机的 20%。

MSRT 概述

Windows 恶意软件删除工具 (MSRT) 旨在帮助识别并删除用户计算机中的流行恶意软件，而且并且向 Windows 授权用户免费提供。MSRT 的主要发布机制是通过 Windows Update (WU)/Microsoft Update (WU)/自动更新 (AU)。此工具的各种版本还可从 Microsoft 下载中心下载或作为 Microsoft ActiveX® 控件从 http://www.microsoft.com/malwareremove 网站下载。此工具的当前版本能够检测并删除 61 个不同的恶意软件系列。

Microsoft 发布和维护 MSRT 主要有两个目的：

1. 降低流行恶意软件对 Windows 用户的影响。
2. 使用由 MSRT 收集的数据总结关于实际影响当今 Windows 客户的恶意软件的一组可靠趋势。Microsoft 反恶意软件小组一直在使用这些数据来集中开发工作并尽可能缩短对恶意软件提交作出响应所需的时间。另外，通过此类报告，其他安全性研究人员可以使用这些数据来加深他们对恶意软件现状的理解并合力降低恶意软件对 Windows 用户的影响。

此工具不针对间谍软件和可能有害软件。Windows 用户应该下载并安装最新的反间谍软件应用程序来从他们的计算机中检测并删除间谍软件以及可能有害软件。http://www.microsoft.com/windowsdefender 向正版 Windows 用户免费提供 Microsoft 的反间谍软件解决方案 Windows Defender（在编写本报告时尚为试用版）。

由于 MSRT 没有实时保护功能并且仅使用部分 Microsoft 反病毒签名数据库而使它能够查找并删除流行恶意软件，MSRT 不能替代最新的反病毒解决方案。然而，我们仍建议安装了最新反病毒软件的用户同时运行此工具作为一项纵深防御措施。这些用户也可从 MSRT 间接受益，因为被感染的用户会对共享资源（如 Internet 或局域网）造成有害影响。

我们极力建议 Windows 用户安装并维护可提供实时保护功能以及完整反病毒签名数据库的最新反病毒解决方案。Microsoft Windows Live OneCare 像 http://www.microsoft.com/security/partners/antivirus.asp 上列出的 Microsoft 反病毒合作伙伴提供的其他产品一样可以满足这些要求。

报告背景

本报告提供一些数据和观点，描述 Microsoft 在过去 15 个月中如何通过发布 MSRT 朝着其发布目标前进：减少影响用户的流行恶意软件的数量并获得宝贵数据，可用作 Windows 恶意软件当前状况的重要指南。将来还会发布详述 Microsoft 对恶意软件现状的理解的其他报告，并且会更频繁地发布，同时会包含除 MSRT 之外的其他来源的数据。

本报告包含截至 2006 年 3 月发布的 MSRT 收集的数据。虽然自此报告发布之后又提供了更新的 MSRT 版本，但是必须将数据截止到一个较早的时间点以便进行处理、验证和分析。有关 MSRT 收集的数据的说明，请参阅本文档的附录。

在本报告中使用的数据是通过测量客户计算机上 MSRT 报告的感染得出的。如今，有许多其他技术可用来测量恶意软件的流行程度。一些测量向网络发出请求，另一些测量按威胁跟踪发送的邮件数。然而，类似这样的技术只能监视被感染的计算机散布的威胁份数，不能监视被感染的计算机数，因为一个感染可生成许多份。因此，跟踪特定的感染是确定恶意软件感染流行程度的最准确的方法。对于 MSRT，当考虑相当大的执行次数时，数据的相关性就会变得异常重要。

虽然 MSRT 用户的配置文件各不相同，但是由于发布机制的缘故，大多数用户可能为家庭用户或小企业。因此，本报告中的大部分数据反映了这一群体的情况。然而，整个报告提供的趋势和指导适用于所有 Windows 用户。

本文将引用下列恶意软件相关术语：

- **系列** – 一组恶意软件的类似变种。例如，Win32/Rbot 就是一个恶意软件系列，它包含几千个类似但不相同的变种。
- **变种** – 一小段特定的恶意软件。例如，Win32/Rbot.A 就是 Win32/Rbot 系列的一个变种。
- **实例或感染** – 在计算机上识别特定的恶意软件变种。请注意，一个实例包含一个变种的所有组成部分（文件、注册表项等），每次从计算机中删除恶意软件变种时，均计为一个单独的实例。例如，如果此工具从计算机中同时删除了 Win32/Rbot.A 和 Win32/Rbot.B，这计为两个感染或实例。如果在三个月后此工具再次从同一台计算机中删除 Win32/Rbot.A，则计为另一个感染。

版本统计信息

Windows MSRT 的主要分发渠道是通过 WU/MU/AU。通过这种机制，MSRT 每个月在全球成千上万台计算机上执行，从而提供强大的威胁数据源以供分析。

图 1. MSRT 通过 WU/AU/MU 执行的次数

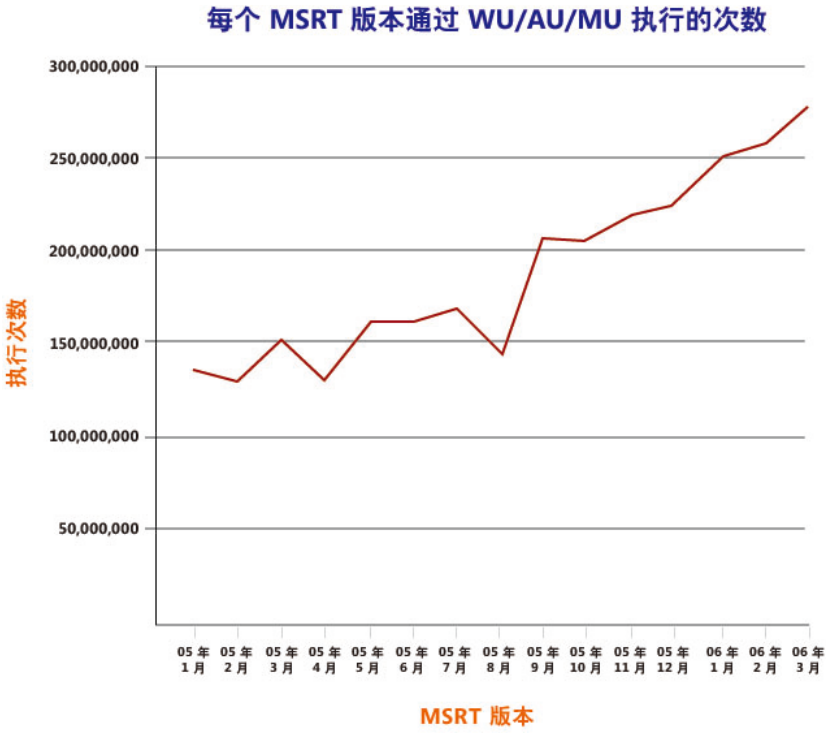


图 1 说明对于从 2005 年 1 月到 2006 年 3 月的 15 个每月发布的版本，计算机执行 MSRT 的次数。请注意，在此图中，图的 X 轴上作为类别列出的值是指 MSRT 的版本，而不是日历月份。例如，MSRT 的 2006 年 2 月版本是在 2006 年 2 月 14 日发布的，然后被 2006 年 3 月 14 日发布的 2006 年 3 月版本取代。另外请注意，此图未列出查杀 Zotob 蠕虫的 8 月编外版本，因为它仅在 Microsoft 下载中心发布以及在 http://www.microsoft.com/malwareremove 上作为 ActiveX 控件发布，而不是通过 WU/MU/AU 发布。

如图 1 所示，除了少数几个例外，每个版本的 MSRT 执行次数都有所增加。特别明显的是此工具的第一个版本和最新版本之间的执行次数差异。从第一个版本到最新版本，计算机执行次数增加了一倍多（从大约 1.25 亿增加到 2.70 亿）。这种差异是由于 Windows 用户使用 WU 和 AU 增多引起的，而使用 WU 和 AU 增多很可能又是 Microsoft 的 Windows XP Service Pack 2 等计划（建议启用 AU）和“保护您的 PC”计划的结果，另外部分原因是与 OEM 供应商的伙伴关系而使他们提供预装 Windows XP SP2 的新计算机。将每个版本的执行次数相加得出 MSRT 通过 WU/AU/MU 执行的次数：自发布之日起，大约 27 亿次。

考虑到当前定期访问 WU/AU 的计算机的增加趋势和目前巨大数量，执行次数同样鼓舞人心。这些 Microsoft 更新机制的增加和及时使用有助于降低威胁对客户的影响。

Microsoft

目标恶意软件详细信息

每个月，Microsoft 反恶意软件小组的成员都研究新流行恶意软件威胁并将它们添加到 MSRT 的下一个版本。我们的小组选择添加到 MRST 的新威胁的标准基于以下三个要素：

- 威胁必须有流行的迹象。
- 威胁必须是恶意的或能够引起恶意情况。
- 威胁在 MSRT 执行时有可能主动运行。

对添加到 MSRT 的新恶意软件的第一项关键要求是威胁有流行的迹象。为了发现新的侯选威胁并确定流行程度，该小组使用一组内部和外部标准。关键内部标准包括由 Windows Live Safety Center Beta (http://safety.live.com) 和 Windows Live OneCare 收集的数据。这两个软件都扫描计算机以查找 Microsoft 已知的全部恶意软件威胁。使用的关键外部标准是 WildList (http://www.wildlist.org)，它是流行恶意软件的实际反病毒业界标准列表以及大多数反病毒产品认证（如 ICSA 反病毒认证和西海岸实验室的认证标志，Windows Live OneCare 最近获得这两项认证）的基础。

对添加到此工具的项目的第二项要求是它们应为恶意软件（例如，病毒、蠕虫、特洛伊木马、自动程序或 rootkit）。在大多数情况下，这是指复制代码、导致明显损害的代码或损害受影响的系统的代码或其他安全风险。此工具不针对间谍软件和可能有害软件。

第三项要求是恶意软件有可能在计算机上主动运行。这项要求是此工具通过 WU/MU/AU 运行的方式产生的。由于在大多数情况下此工具每月运行一次，查找主动运行的和处于自动启动位置的恶意软件，然后退出而没有任何驻留组件。只有恶意软件在当时正在运行或链接到自动启动位置时，此工具才有效。因此，此工具不针对数据文件感染威胁之类的威胁，包括 Microsoft Word 和 Microsoft Excel® 宏病毒。选择要添加到此工具的新恶意软件系列之后，该系列的所有变种也会同时包括在该版本中。该系列的任何新变种都会添加到此工具的每个未来版本中。

图 2. MSRT 检测并删除的恶意软件系列

	电子邮件蠕虫	P2P 蠕虫	IM 蠕虫	漏洞利用蠕虫	后门特洛伊木马	Root Kit	病毒
Alcan		是					
Antinny		是					
Atak	是						
Badtrans	是						
Bagle	是				是		
Bagz	是						
Berbew					是		
Bobax	是			是			
Bofra	是						
Bropia			是				
Bugbear	是						
Codbot				是	是		
Dumaru	是						是
Esbot				是	是		
Eyeveg	是				是		
F4IRootkit						是	
FURootkit						是	
Gael							是
Gaobot					是		
Gibe	是						
Hackdef						是	
IRCbot					是		
Ispro						是	
Kelvir			是				
Korgo				是			
Lovgate	是				是		
Mabutu	是				是		

	电子邮件蠕虫	P2P 蠕虫	IM 蠕虫	漏洞利用蠕虫	后门特洛伊木马	Root Kit	病毒
Mimail	是						
Msblast				是			
Mydoom	是				是		
Mytob	是		是	是	是		
Mywife	是						
Nachi				是			
Netsky	是						
Optix					是		
Optixpro					是		
Parite							是
Randex					是		
Rbot					是		
Ryknos					是		是
Sasser				是			
Sdbot					是		
Sober	是						
Sobig	是						
Spybot		是			是		
Spyboter		是			是		
Swen	是	是					
Torvil	是	是					
Valla							是
Wootbot					是		
Wukill			是				
Yaha	是						
Zafi	是				是		
Zotob				是	是		

图 2 按字母排序列出 MSRT 能够检测的 61 个恶意软件系列，截至 2006 年 3 月版本，分为非互斥的七个类别。虽然根据功能、复制媒介等有许多不同的方式将恶意软件分类，图中所示的七个类别（电子邮件蠕虫、对等 (P2P) 蠕虫、即时消息 (IM) 蠕虫、漏洞利用蠕虫、后门特洛伊木马、rootkit 和病毒）提供一个有用的高级分类系统，本文档后面部分将会使用。上述某些系列中每天都会有新的恶意软件变种出现，因此这些分类在本文发表之后可能会有变化。请注意，在此图中，漏洞利用蠕虫定义为威胁，因为它至少利用一个允许在没有用户操作的情况下执行代码的软件漏洞。此类别不包括利用需要用户操作（例如，查看电子邮件或浏览网站）的漏洞的恶意软件。

Microsoft

对于要与某类别相关联的恶意软件系列，在默认情况下所有已知变种均必须出现与该类别相关联的行为。例如，Bagle 系列只有一个变种 (Bagle.O) 可归类为病毒，因为它感染可执行文件。因此，没有将 Bagle 系列称为病毒。另一个例子，Rbot 系列的很多变种都能够利用软件漏洞。然而，因为在大多数情况下都需要自动程序所有者手动干预来引发这种形式的复制，所以没有将 Rbot 归类为漏洞利用蠕虫。如上所示，图 2 中少数几个系列不能归类为这七个类别中的任一个系列。

请注意，除了上面列出的系列之外，MSRT 还能够检测少量的特定恶意软件变种。这些变种不归入上述系列并，但由此工具检测以提供端对端病毒删除体验。

MSRT 删除的恶意软件

本文档的余下部分将提供有关在过去 15 月中 MSRT 删除的恶意软件的详细信息，包括从中删除了恶意软件的计算机的高级特性（例如，操作系统版本和区域设置）。

概述

本文将首先说明 MSRT 执行的删除次数。

图 3. 每个 MSRT 版本删除的恶意软件数和清理的计算机数

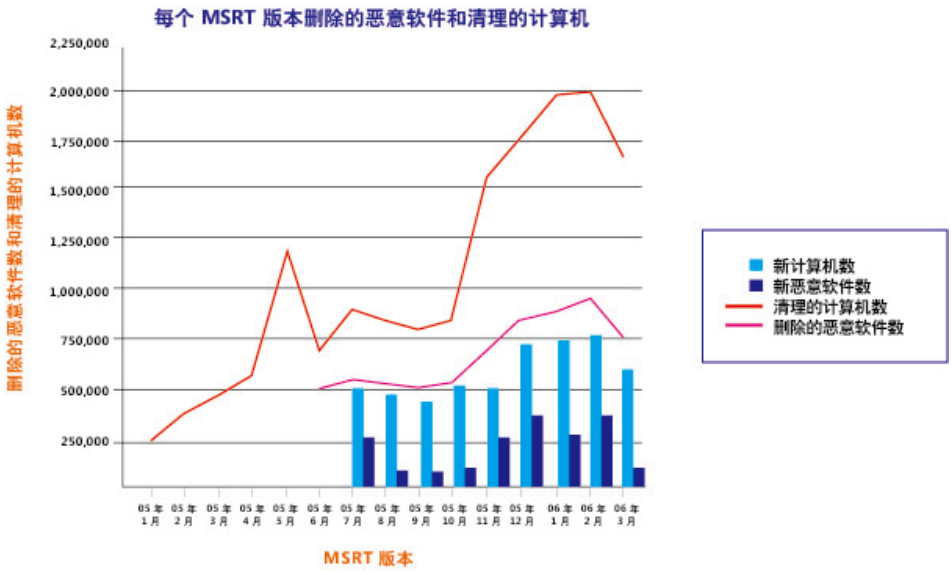


图 3 通过图中的三个数据系列提供下列信息：

- **删除的恶意软件数：**从 2005 年 1 月到 2006 年 3 月，MSRT 的每个版本删除的恶意软件数。历经所有版本，此工具已经删除了 1600 万个恶意软件实例。
- **清理的计算机数：**从 2005 年 6 月到 2006 年 3 月，MSRT 的每个版本清理的计算机数。每个版本清理的计算机数始终少于同一版本删除的恶意软件实例数（可能从一台计算机中删除多个感染）。另请注意，此数据系列从 2005 年 6 月开始，因为这是此工具开始测量此标准的第一个版本。从 2005 年 6 月到 2006 年 3 月，此工具已经从 570 万台计算机中每台至少删除一个恶意软件实例。自此工具第一次发布以来清理的计算机总数大于此数字，但是不知道是多少，因为没有获得有关此测量在 2005 年 6 月之前的数据。
- **新计算机数：**在每个版本清理的计算机总数中，此工具的每个版本从中删除了恶意软件的新计算机数。这里，“新”表示此工具从未从中删除恶意软件的计算机，包括 MSRT 的所有先前版本。对于每个版本，此值永远不会大于清理的计算机总数。因为此数字与清理的计算机数相关联，可测量的第一个版本是 2005 年 7 月版本。请注意，如果用户在其计算机上重新安装操作系统，此系统对于我们的数据是“新”系统。对于本报告，这种情况导致的偏差很小，因此忽略不计。

观察图 3 中显示的数据可得出以下结论：

- 删除的恶意软件数和清理的计算机数增加是由于 MSRT 的执行次数增加（如图 1 所示）以及此工具针对的流行恶意软件系列和变种数增加。特别是自 2005 年 11 月以来的新版本查杀的病毒数显著增加。这些增加都归功于此工具中加入了一个或一套特定流行恶意软件系列。因为有些系列在过去已经发现并且不能确定用户何时第一次感染，所以不能精确地将此数据解读为恶意软件数量的增加。
- 2005 年 11 月：Win32/Mabutu、Win32/Codbot 和 Win32/Bugbear 的组合
- 2005 年 12 月：WinNT/F4IRootkit
- 2006 年 1 月：Win32/Parite
- 2006 年 2 月：Win32/Alcan
- 结合图 1 和图 3 所示的数据，我们可以确定在 MSRT 的最新 2006 年 3 月版本中，受感染的计算机与此工具的执行次数的比率是 0.28%。也就是说，此工具在运行它的计算机中大约每 335 台计算机至少删除一个恶意软件。从 2005 年 6 月到 2006 年 3 月的所有版本的平均比率大致差不多，为 0.32%，即大约每 311 台计算机至少删除一个恶意软件。在所有可测量版本之间，此感染比率保持相对恒定，2005 年 8 月版本较高，为 0.4%；2005 年 9 月版本较低，为 0.24%。
- 对于每个版本，此工具从中删除恶意软件的绝大多数计算机都是此工具第一次删除恶意软件的计算机。相反，对于每个版本，此工具从先前从中删除恶意软件的计算机中删除的恶意软件相对较少。例如，在此工具的 2006 年 3 月版本中，此工具清理的 75 万台计算机中大约有 60 万台 (80%) 是新系统。只有 20% 的计算机是此工具的先前版本从中删除恶意软件的计算机。这些删除数量表示同一台计算机感染不同的恶意软件变种或系列以及再次感染同一恶意软件变种（可能由于没有为计算机打补丁或有效的社会工程）。

每台计算机的删除恶意软件数

要检查的另一个有趣标准是从每台计算机中删除的恶意软件变种数。在大多数情况下，此工具从一台计算机中只删除一个恶意软件变种。然而，某些情况下，此工具会从计算机中删除数十个甚至数百个恶意软件。

图 4. 每台计算机的删除恶意软件变种数

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

图 4 显示计算机上此工具所有执行删除的恶意软件变种数以及相应的计算机数。例如，如果此工具从某计算机中删除了同一个恶意软件变种两次，在图 4 中仅计一次。通过使用图 4 中的数据，我们可以确定每台计算机删除的恶意软件变种平均数量为 1.59。也就是说，此工具更有可能从每台计算机中删除多个恶意软件变种，而不是只删除一个变种。如果删除数量很大，计算机通常感染了许多自动程序变种，很有可能是用户感染了一个自动程序，然后该自动程序的所有者使用这第一个后门恶意软件在该计算机上安装其他自动程序。

Win32/Antinny 是一个对等蠕虫，它几乎是专门影响日语计算机，它也是会使每台计算机大量感染的一种威胁。原因是 Antinny 使用多种社会工程诡计来吸引用户下载并运行该蠕虫。因此，一个用户可能只执行了该蠕虫一次，但其计算机却感染了很多次。

Microsoft

删除的恶意软件详细信息

本节更详细地说明前面几节中提供的数据与 MSRT 能够检测并删除的 61 个恶意软件系列有何关系。

图 5. 按恶意软件系列列出的恶意软件/清理的计算机

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

图 5 列出 MSRT 截至 2006 年 3 月版本能够检测的全部 61 个恶意软件系列以及下列信息：

- 从 2005 年 1 月到 2006 年 3 月，从计算机中删除恶意软件系列的次数。列表根据此值按降序排序。
- 从 2005 年 6 月到 2006 年 3 月，从中删除了恶意软件系列的计算机数。
- 第一次检测到恶意软件系列时 MSRT 的版本。
- 发现系列的第一个变种的月份和年份。

关于图 5 中的数据一些有趣现象包括：

- Win32/Parite、Win32/Alcan 和 WinNT/F4IRootkit 的删除次数居最高之列，尽管对这些系列的检测只是在最后五个版本中添加到此工具。Parite 是一种文件感染型病毒，它特别有趣，在 2001 年首次出现，至今仍然流行。这可能是因为从计算机中彻底清除 Parite 相当困难并且它是侵略型文件感染例程。事实上，删除数量与系列首次发现时间或对它的检测首次加入工具的时间没有明显的关联。
- 自动程序（Rbot、Sdbot 和 Gaobot）在删除总数前五名中占三个。这三个恶意软件系列的流行程度进一步证实了摘要中有关后门特洛伊木马盛行的论点。
- Win32/Antinny 排在第 12 位，通过日文文件共享网络传播。该蠕虫几乎只能在日语系统中发现，但是经过仅仅六个版本的检查之后仍然排在前列，这说明它在日本相当流行并证明对特定地区/语言的威胁。
- Win32/Alcan 是一种通过对等网络复制的鲜为人知的蠕虫，仅仅在 2006 年 2 月加入此工具以后就已经成为删除次数最多的恶意软件之一。该蠕虫的流行可能是由于它利用的很多相当有效的社会工程技巧，包括在运行之后伪装成在安装期间出现错误的应用程序。
- Win32/Zotob 利用 Microsoft 安全公告 MS05-039 解决的漏洞，只从 6132 台计算机中删除过，从而成为列出的所有漏洞利用蠕虫中最不流行的蠕虫。这在漏洞只影响 Windows 2000 计算机的情况下才有意义。具有讽刺意味的是，利用同一漏洞的 Win32/Esbot 排在第 30 位，清理的计算机是 Win32/Zotob 的 10 倍，但引起的关注却少得多。Win32/Msblast 排在第 10 位，仍然是删除次数最多的漏洞利用蠕虫。
- 同样，虽然 Hacker Defender rootkit 系列作为“著名的”rootkit 系列通常最引人关注，实际上它是此工具所查找的最不流行的 rootkit 之一。WinNT/FURootkit 是此工具清除最多的 rootkit，并且常常用来隐藏安装在计算机上的后门特洛伊木马的存在。

图 6. 按恶意软件类型列出的清理计算机

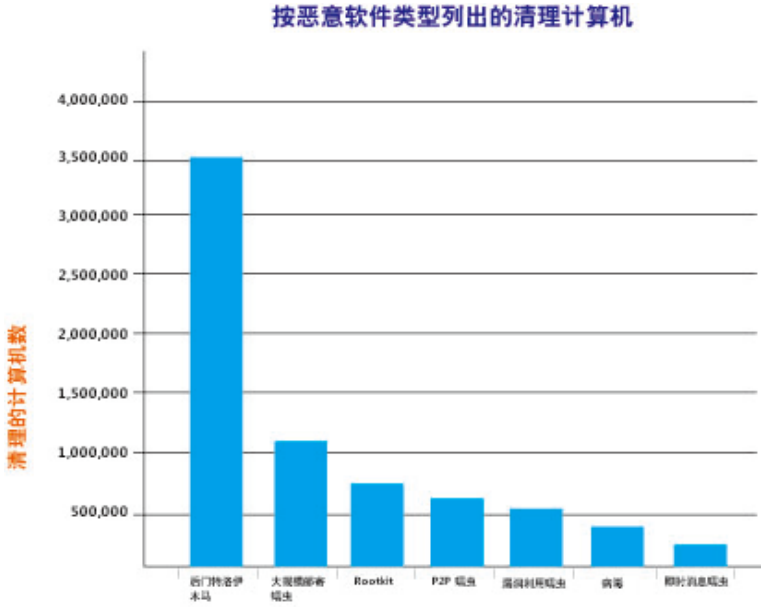


图 6 将图 5 中显示的数据与图 2 中建立的恶意软件分类相结合。在清理的 570 万台计算机中，MSRT 从其中的 350 万台 (62%) 中删除了后门特洛伊木马。最近几次著名的事件说明，攻击者通过建立感染计算机网络并将其作为垃圾邮件、间谍软件和拒绝服务 (DoS) 攻击的中转站和分发点销售，因而频繁地使用这些后门特洛伊木马获利。除了使用最新的反病毒解决方案外，客户应利用双向防火墙来帮助阻止信息泄露以及远程监视/控制这些威胁的发展。

与后门特洛伊木马相比，发现 rootkit 的计算机数要少得多：大约 78 万台。然而，如果忽略对 WinNT/F4IRootkit 的检测，这个数字将降到 53 万左右。特别指出这种情况的原因是：虽然恶意软件随后利用 rootkit 在计算机上隐藏自身，但是 Sony 没有将其作为恶意软件包发布，而是作为反盗版功能，并因此具有零星散发特性而不是病毒散发特性。毫无疑问，与本报告中讨论的其他恶意软件类别一样，此处提供的数据仅与此工具能够检测的恶意软件系列有关。虽然还存在一些由于不是很流行而此工具未检测的已知 rootkit 以及此工具不检测的未知 rootkit，来自 Microsoft 其他产品（如 Windows Live OneCare 和 Windows Live Safety Center Beta）的客户反馈和数据表明 MSRT 已经锁定的五个 rootkit 系列代表目前影响大量用户的 rootkit 的重要部分。

对付 rootkit 最有效的方法是预防。建议客户使其病毒签名保持最新，以便软件的实时保护机制能够检测并阻止 rootkit 而使它无法在计算机上安装，并且尽量不要以管理员的身份运行计算机。对于大多数 rootkit，以标准用户身份运行的用户将无法在其计算机上安装。Microsoft 的下一代操作系统 Microsoft Windows Vista™ 也提供几个功能帮助阻止 rootkit 损害操作系统的关键内部结构。在无法预防并且计算机已经感染 rootkit 的情况下，客户应使用可检测并删除 rootkit 的反病毒产品或删除工具。这种情况下，用户（特别是公司用户）应权衡执行额外步骤解决此问题的得失。

在社会工程威胁方面，电子邮件是最常见的方法，清理的计算机中大约 20% 至少感染了一种能够通过电子邮件传播的威胁。虽然 MSRT 能够检测并删除三种最常见的即时消息蠕虫（Win32/Bropia、Win32/Kelvir 和 Win32/Mytob），但是这三种威胁在相当少的计算机上发现：不到 25 万台。与这个数字相比，清除了通过 P2P 网络传播的 Win32/Alcan 和 Win32/Antinny 的计算机为 45 万台左右。通过 P2P 网络传播的恶意软件能够检测计算机上是否安装有流行的 P2P 应用程序。如果有，他们通常会在 P2P 应用程序用来在网络上共享文件的目录中使用诱人的名称复制自身。通过这种方法，蠕虫就会在 P2P 网络中共享。除了最新的反病毒软件之外，对付此类社会工程威胁的最好的技巧是培训用户以及通过以非管理员的身份运行来限制执行威胁所造成的影响。

即时消息威胁一直无法像 P2P 威胁那样在大量用户中间广泛传播的原因之一是：即时消息程序从开始就具有防止用户防止感染恶意软件的功能。例如，MSN® Messenger 7 禁止用户发送某些可执行文件类型的文件和点击即时消息中需要用户同意的链接。此类保护尚未集成到 P2P 客户端程序中。造成这种差异的另一个重要原因是：与更着重于消息传递的即时消息程序相比，作为交换文件机制的 P2P 应用程序更适合于传播恶意文件。

图 7. 按类型列出的恶意软件感染相关性

	电子邮件蠕虫	P2P 蠕虫	IM 蠕虫	漏洞利用蠕虫	后门特洛伊木马	Rootkit	病毒
电子邮件蠕虫	-	1.0%	1.4%	2.7%	8.2%	0.6%	1.4%
P2P 蠕虫	1.9%	-	1.0%	1.8%	14.3%	1.0%	2.9%
IM 蠕虫	7.0%	2.7%	-	7.0%	17.3%	1.6%	0.5%
漏洞利用蠕虫	5.3%	2.0%	0.7%	-	5.3%	3.6%	1.0%
后门特洛伊木马	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%
病毒	4.3%	4.9%	0.3%	1.5%	6.2%	0.8%	-

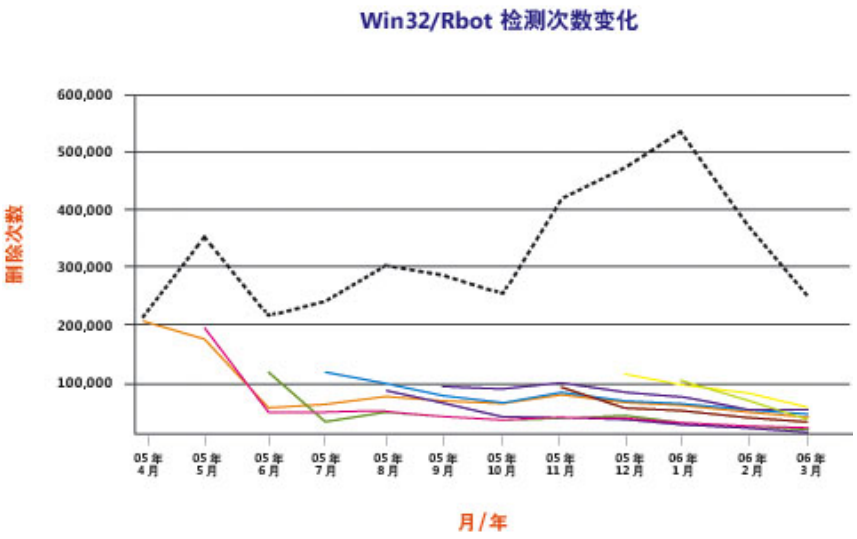
图 7 显示了在计算机上检测上述恶意软件类型之间的重叠。在 MSRT 检测到电子邮件蠕虫所有计算机中，MSRT 同时在 0.1% 的计算机中检测到 P2P 蠕虫。相反，在此工具检测到 P2P 蠕虫的计算机中，1.9% 的计算机同时检测到电子邮件蠕虫。

以上显示在 rootkit 和后门特洛伊木马之间的相关性最紧密。在发现了 rootkit 的计算机中，20% 的计算机同时至少发现一个后门特洛伊木马。这强调后门特洛伊木马传播或利用大量的 rootkit 的趋势。P2P 蠕虫和后门特洛伊木马以及即时消息蠕虫和后门特洛伊木马同时发现的比例也很高。如果很多 P2P 蠕虫和即时消息蠕虫在运行时经常在计算机上放置自动程序，数值也很高。

恶意软件删除数变化

跟踪此工具删除的恶意软件系列变化很有用，原因有二。第一，使 Microsoft 能够监视特定恶意软件系列的活动及流行程度。首次添加到版本后删除次数增加的系列通常表示变种发布活跃并且还在不断地复制。跟踪删除次数变化很有用的另一个原因是：使 Microsoft 能够通过保证工具检测到的恶意软件系列的变种流行程度降低来监视 MSRT 的成功。虽然还有其他因素可导致降低，但是 MSRT 已从计算机上删除了大量的恶意软件系列实例的事实说明该版本至少对流行程度的下降起到部分作用。

图 8. Win32/Rbot 删除次数变化



Microsoft 使用映射至上述两种原因的两种标准来跟踪 MSRT 删除的恶意软件数量变化。图 8 使用 Win32/Rbot 系列说明了这两种标准。请注意，X 轴对应于日历月份和年份。使用此模型中的日期对于显示随时间的进展很重要。假定用户能够运行旧版 MSRT（虽然发行 60 天后会显示警告屏幕）。使用 MSRT 发布月会使此测量值有偏差。

- **系列变化**（黑色虚线）：从首次将某个系列的检测添加此工具起删除数的变化。虽然这很好地显示删除数如何随时间变化，但是如果系列很活跃并且首次添加到此工具以后删除数很少，就会存在偏差。该图形显示了从 2005 年 4 月到 2006 年 3 月 Win32/Rbot 系列的删除总数。通过使用此数据，我们可计算出此系列在过去 11 个月中删除数大约增加了 16%。根据此信息和图 5 中的数据，我们可以得出结论：Rbot 是非常活跃的流行系列。请注意，在图形上，此数据系列代表其下方实线的总和。
- **平均版本变化**（实线）：添加到某个版本的一组特定变种从该组首次添加到此工具到此工具的最新版本的所有版本的平均删除数变化。此标准不受活跃恶意软件系列产生的大量删除的影响，因而是确定此工具在减少系列实例方面取得的效果的较好方法。在图中，实线表示随时间添加到特定版本的一组 Win32/Rbot 变种的删除数。线越长，检测添加到此工具的时间就越长。例如，最长的深蓝色线表示添加到此工具的第一组 Rbot 变种。此处观察到的总体印象是，一组 Rbot 变种的检测添加到此工具时，这些变种的删除数最终降低。如果我们计算每组变种随时间的删除数变化，然后对这些变化求平均值，我们就会发现自添加到 MSRT 以来，Rbot 变种的删除数降低了大约 79%。

图 9. 恶意软件删除数变化

排名	恶意软件系列	系列变化率	平均版本变化率
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	Win32/Korgo	-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	-83%	-77%
18	Win32/Netsky	-82%	-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%

图 9 显示此工具检测到的大多数恶意软件系列以及上面讨论的删除数变化测量标准，按系列变化百分比升序排列。请注意，添加到此工具的 2006 年 3 月版本的三个系列（Win32/Atak、Win32/Torvil 和 Win32/Zlob）不包括在此列表中，因为尚无法确定删除数变化。另外，Win32/Bofra、Win32/Gibe、Win32/Opaserv、Win32/Badtrans 和 Win32/Zotob 也被排除在外，因为还没有足够的删除数（至少 1,000）来生成可靠的变化标准。

如图所示，不难发现绝大多数系列（53 个中的 41 个）自添加到此工具以后流行程度都有所降低，其中 41 个系列中的 33 个降幅超过 50%，41 个系列中的 21 个降幅超过 75%。总体流行程度增高的 12 个系列中，只有 3 个系列（Win32/Gael、Win32/Lovgate 和 Win32/Wukill）在添加到此工具以后每组变种平均值持续增长。其余 9 个系列（包括图 8 中所示的 Win32/Rbot）的每个版本删除数均降低。此数据的其他要点包括：

- 随某些 Sony 音乐 CD 传播的 First4Internet rootkit (WinNT/F4IRootkit) 的删除数自 2005 年 12 月首次添加到此工具以来急速下降。这可能表明此问题引起媒体关注之后，很少用户从受感染的 CD 安装/重新安装该软件。
- Mywife 删除数的急速增长的原因是在此工具中包括 Win32/Mywife.E。Mywife.E 在 2006 年 1 月末出现，新闻媒体也称之为 CME-24 和 Kama Sutra 蠕虫。该蠕虫主要通过电子邮件传播并且能够在每个日历月的第三天损坏关键数据文件。在这种情况下，删除数从 2006 年 1 月的 700 左右急剧增加到 2006 年 2 月的 92,000 左右。
- Win32/Rbot 删除数的增加是由于该恶意软件系列的大量变种添加到 MSRT 的每个版本中。平均每月大约有 2000 个 Win32/Rbot 新变种添加到此工具。
- Win32/Hackdef 和 Win32/Ryknos 等系列的删除数增加是由于初始删除数低，初始删除数低又是由于此工具最初检测到的变种数低。例如，MSRT 的 2005 年 4 月版本能够检测 Win32/Hackdef 系列的 78 个不同变种。在 2006 年 3 月版本中，变种数急剧上升到 439，增幅超过 400%。同样，删除数在此期间从大约 3000 增长到 30,000。因此，虽然 Hackdef 的删除数与其他恶意软件系列相比仍然相对较低，但是自从对它们的检测添加到此工具以来，它们显著增长。如图 9 所示，这些趋势可从此系列的变化中明显看出。虽然删除数大量增长 (842%)，但是此数字是由于该系列的删除数的起始数字很而加剧。该系列的每个版本删除数平均下降 31%。

操作系统信息

通过使用 MSRT 收集的数据信息，Microsoft 能够确定支持的 Windows 版本中检测到的威胁的流行程度。图 10 从各个角度显示 2006 年 3 月版本在这些操作系统中检测到的恶意软件流行程度。

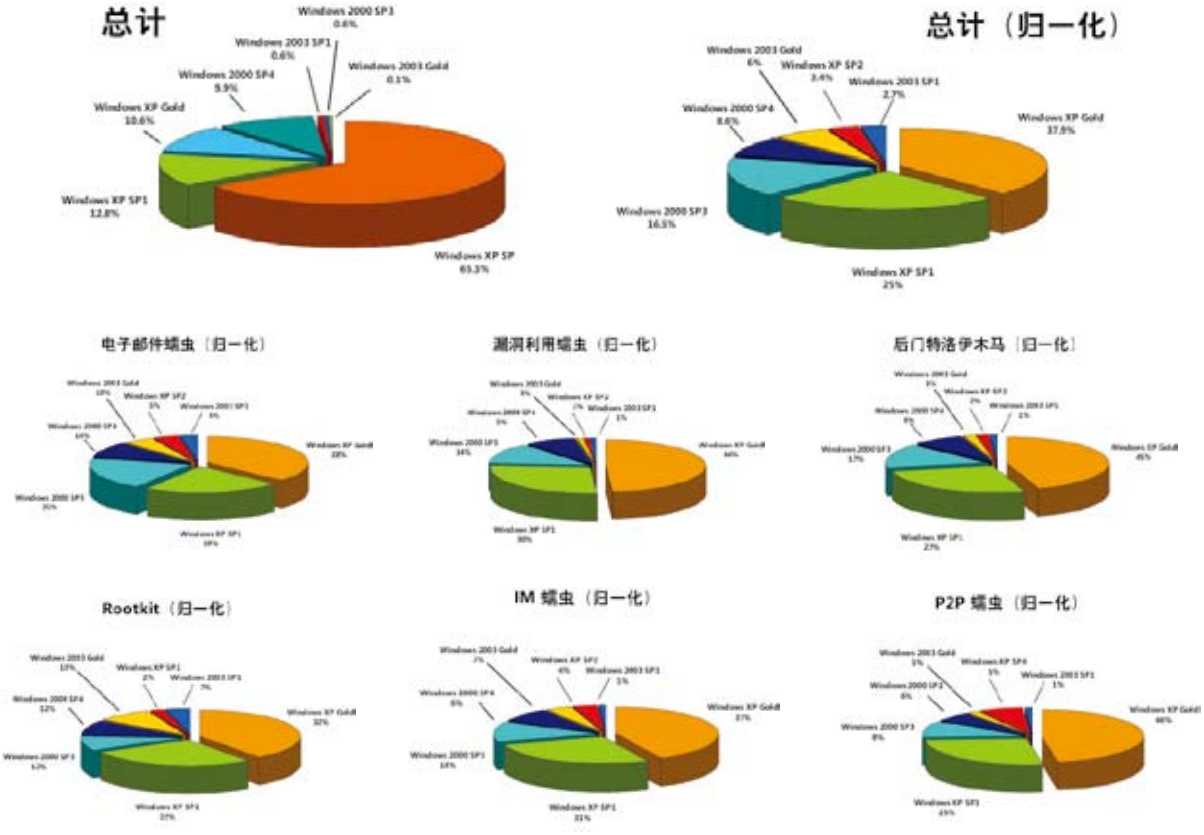
前两个饼图反映此工具的 2006 年 3 月版本检测到的所有恶意软件。在标签为“总计”的图中，可以发现大多数删除来自 Windows XP SP2，其中 Windows XP 占此工具执行的全部删除的 89%。这种来自 Windows XP SP2 计算机的大量病毒清除是正常的，因为此工具的大多数执行都是在 Windows XP SP2 计算机上进行的。因此，要切实了解在某些操作系统上哪种恶意软件更常见，可以“归一化”第一幅图中的数据。

在这种情况下，归一化意味着调整操作系统中病毒清除百分比，将工具在该操作系统上的执行次数考虑在内。也就是说，要减少操作系统大量执行产生的病毒清除百分比偏差，将特定操作系统的病毒清除数除以该操作系统的相对执行百分比。因此，与执行百分比小的操作系统相比，执行百分比较大的那些操作系统的删除数增幅较小。

本例中所用的特定数学公式如下：

归一化删除数（操作系统） = 删除数（操作系统）/执行百分比（操作系统）

图 10. 按操作系统列出的 2006 年 3 月版本清理的计算机数



Microsoft

将此公式应用于 2006 年 3 月版本的删除和执行百分比生成图 10 右上角的图形。该图形显示百分比发生明显变化，Windows XP SP2 的归一化删除数降低到仅 3%，W indows XP Gold 和 SP1 的删除数占 63%。此举对于技术领域和社会领域意义重大。对于前者，Windows XP SP2 包含许多对在旧版 Windows XP 中没有发现的漏洞的安全性增强功能和补丁，令恶意软件更加难以入侵。对于后者，还未升级到最新服务包的用户将可能更易于遭受社会工程攻击。对于 Windows 2000 和 Windows Server 2003 也是如此，相对于旧版操作系统而言，这些操作系统的最新版服务包的归一化删除数最低。

两个主图下面的六个图形显示图 2 所示相同类别的归一化删除数降低。总而言之，考虑所有删除数时，这些图形的结果类似于归一化结果。实际上，操作系统的顺序在所有情况下均相同。具体看 Windows XP SP2，我们会发现此操作系统的删除数的最高百分比均来自通过电子邮件、即时消息和对等网络传播的威胁。这种排列是正常的，因为这些威胁与漏洞利用蠕虫相反，使用社会工程攻击来感染计算机，而这种方法可能会威胁所有操作系统。

区域设置信息

图 11. 按区域设置列出的 2006 年 3 月版本清理的计算机

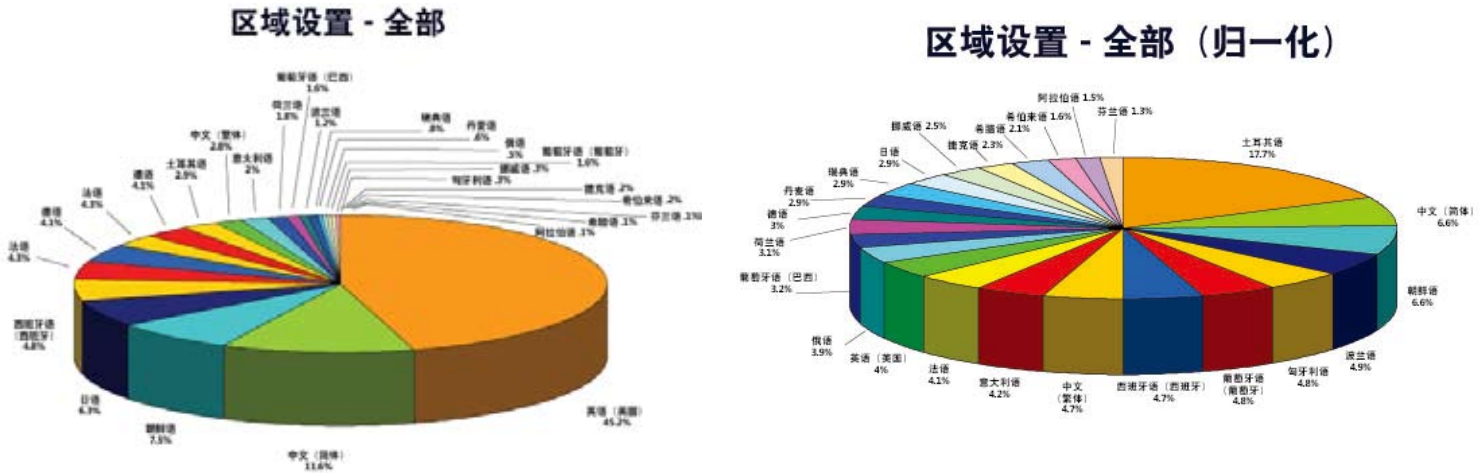


图 11 显示 MSRT 的 2006 年 3 月版本 按操作系统区域设置列出清理计算机细分。请注意，区域设置无需指明地理位置。例如，英语（美国）在全球其他国家/地区非常流行。图 11 的左侧图表显示，大多数清理计算机均使用英文操作系统。然而，与上述 Windows XP SP2 的情况类似，此信息具有少许欺骗性，因为运行此工具的大多数计算机都安装英文操作系统。因此，类似于操作系统版本，清理的计算机可以按区域设置的执行百分比进行归一化。计算方式类似于对操作系统版本执行的计算，使用“执行百分比（区域设置）”取代“执行百分比（操作系统）”。

此计算结果显示在图 11 的右边并产生有趣的结果。这里，归一化过程将删除数相当公平地划分到大多数区域设置中。换言之，当考虑工具删除的所有恶意软件并归一化数值时，该恶意软件的删除数分布在所有 Windows 区域设置中，包括英语。如图所示，土耳其语区域设置是一个例外，归一化后占清理计算机的 20.2%。进一步研究该数据可发现，此模式在所有恶意软件系列中都是类似的。虽然 Microsoft 反恶意软件小组不断努力研究此数据，但土耳其语计算机的归一化删除数百分比高的原因至今仍不明确。

结论

回顾过去的 15 个月，对于 Microsoft 反恶意软件小组和我们的内部公司合作伙伴来说十分令人振奋，我们发布了 Windows 恶意软件删除工具、Windows Defender Beta、Windows Live OneCare Beta 和 Windows Live Safety Center Beta。接下来的 15 个月必定同样令人振奋，我们计划推出上述产品的完整版，同时也推出 Microsoft Forefront Client Security，这是台式机、膝上型计算机和服务器操作系统的综合性恶意软件保护解决方案，易于管理和控制，另外还将继续发布 MSRT。

这些产品的推出，将为 Microsoft 提供更充足的流行恶意软件的数据，类似于 MSRT 收集的数据。收集此数据很重要，它不仅能促进 Microsoft 对威胁现状的理解，更会有效地应对这些威胁，提升 Microsoft 客户的总体计算经验。例如，确定自动程序在 MSRT 检测到的恶意软件中占大多数，反恶意软件响应小组就能针对这些威胁开发出多种自动化分析和特征码生成方法。这显著增加了特征码的产量，并且小组响应新出现的自动程序的能力也大大加强。

Microsoft 相信，与合作伙伴和客户分享此信息意义重大，不仅是证明我们的工具和产品对威胁现状的影响，而且共享我们的知识。本报告是共享此类信息的第一个重要范例；未来将会更加频繁地推介更多实例。我们希望安全行业同行能够利用此数据来加深我们对恶意软件现状的共识，并合力降低恶意软件对 Windows 用户的影响。

附录

MSRT 背景

在 2003 年末，Microsoft 收购了 GeCAD Software（一家反病毒技术供应商），Microsoft 的安全技术部门 (STU) 开始研究有关反病毒软件的工具和技术。从此收购获益的第一个版本是 Blaster 蠕虫删除工具，是由 STU 反恶意软件小组于 2004 年 1 月推出的，旨在对 Microsoft 的 Internet 服务提供商 (ISP) 合作伙伴提供信息表示 Blaster 在当时仍然是一种威胁作出回应。此工具可以删除当时 Msblast 和 Nachi 的所有已知变种，并通过 Windows Update 部署到被感染的计算机。通过 Windows Update (WU)/自动更新 (AU) 向可能已感染病毒的用户提供此工具，使 Microsoft 能够获得有关 Msblast 和 Nachi 在 2004 年流行程度的关键数据，并从 1000 多万台客户计算机中删除了这些恶意软件。后来于 2004 年 3 月和 5 月推出两款独立的清除工具，分别检测并删除 Mydoom 和 Berbew。

Microsoft 收到客户的许多正面反馈，客户表示这种一次性清除工具很有价值，但也有许多客户要求更一致的可预测系统。此反馈促成了 Windows 恶意软件删除工具 (MSRT) 的诞生。

此版本的主要特色如下所示：

- 本工具每月发布一次，于每月的第二个星期二与当月的任何安全性更新一起发布。如果需要，对于高优先级威胁，会编外发布此工具。至今，Microsoft 仅于 2005 年 8 月进行过一次工具的特别更新，为了应对 Zotob 蠕虫。由于 Zotob 蠕虫的传播仅影响某些运行 Windows 2000 的组织，因此更新仅通过 Microsoft 下载中心和网站提供。
- 此工具的所有每月版本同时发布于 Microsoft Update (MU)、WU、AU、Microsoft 下载中心和 MSRT 网站 http://www.microsoft.com/security/malwareremove/default.mspx。
- 此工具的每个版本都是累积的，包括自以前版本工具以来增加的所有威胁。

- 通过 WU/MU/AU 交付时，工具的每个版本仅运行一次，然后退出。如果发现并删除任何恶意软件，此工具会在下次重启时向用户提供消息。如果未发现任何恶意软件，用户将不会看到任何消息或用户界面。想要根据需要每月运行此工具多次的用户可从 Microsoft 下载中心 (http://www.microsoft.com/malwareremove) 下载副本。
- 默认情况下，此工具仅查找当前运行或通过自动启动点链接（例如注册表中）的恶意软件。此工具以这种方式设计，旨在缩短执行时间，特别是通过 WU/AU 执行的时间。
- 此工具便于公司客户部署和管理。特定情况包括通过 Microsoft System Management Server (SMS) 或类似应用程序管理系统分发，以及每次系统登录或启动时执行此工具。在这些情况下执行此工具的管理员可以使用此工具返回的状态码（在 KB891716 中列出）监视其执行和状态。此外，此工具也可以通过 Windows 服务器更新服务 (WSUS) 部署。

此工具应尽可能小，以照顾带宽受限的客户。2005 年 6 月，此工具开始通过 WU/MU/AU 使用 delta 更新。在这种情况下，向运行了此工具近期版本的用户提供一个更小的更新（实际上是用户系统之上已有内容和最近版本间的差异）。目前，大约 80% 的 WU/MU/AU 用户利用这些更小的更新，使得每个用户可节省 1 MB、每个版本可节省大约 80 TB 的已保存数据。