An in-depth perspective on software vulnerabilities and exploits, malware, potentially unwanted software, and malicious websites

Microsoft Security Intelligence Report

Volume 14

July through December, 2012

Running Unprotected: Measuring the Benefits of Real-Time Security Software

Microsoft Security Intelligence Report

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

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Authors

Danielle Alyias
Microsoft Trustworthy Computing

Dennis Batchelder
Microsoft Protection Technologies

Joe Blackbird
Microsoft Malware Protection Center

Joe Faulhaber
Microsoft Malware Protection Center

David Felstead
Bing

Paul Henry
Wadeware LLC

Jeff Jones
Microsoft Trustworthy Computing

Jimmy Kuo
Microsoft Malware Protection Center

Marc Lauricella
Microsoft Trustworthy Computing

Le Li
Microsoft Windows Safety Platform

Nam Ng
Microsoft Trustworthy Computing

Tim Rains
Microsoft Trustworthy Computing

Vidya Sekhar
Microsoft Malware Protection Center

Holly Stewart
Microsoft Malware Protection Center

Matt Thomlinson
Microsoft Trustworthy Computing

Terry Zink
Microsoft Forefront Online Protection for Exchange

Contributors

Horea Coroiu
Microsoft Malware Protection Center

Meths Ferrer
Microsoft Malware Protection Center

Tanmay Ganacharya
Microsoft Malware Protection Center

Enrique Gonzalez
Microsoft Malware Protection Center

Heather Goudey
Microsoft Malware Protection Center

Angela Gunn
Microsoft Trustworthy Computing

Satomi Hayakawa
CSS Japan Security Response Team

Ben Hope
Microsoft Malware Protection Center

Aaron Hulett
Microsoft Malware Protection Center

Michael Johnson
Microsoft Malware Protection Center

Lesley Kipling
Microsoft EMEA Security Incident Response Team

Aneesh Kulkarni
Microsoft Windows Safety Platform

Jenn LeMond
Microsoft IT Information Security and Risk Management

Greg Lenti
CSS Security Readiness & Response Team

Wei Li
Microsoft Malware Protection Center

Marianne Mallen
Microsoft Malware Protection Center

Daric Morton
Microsoft Services

Yurika Muraki
CSS Japan Security Response Team

Jeong Wook Oh
Microsoft Malware Protection Center

Takumi Onodera
Microsoft Premier Field Engineering, Japan

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Anthony Penta
Microsoft Windows Safety Platform

Hilda Larina Ragragio
Microsoft Malware Protection Center

Tim Reckmeyer
Microsoft Services

Laura A. Robinson
Microsoft Information Security & Risk Management

Cynthia Sandvick
Microsoft Trustworthy Computing

Richard Saunders
Microsoft Trustworthy Computing

Jasmine Sesso
Microsoft Malware Protection Center

Frank Simorjay
Microsoft Trustworthy Computing

Chris Stubbs
Microsoft Malware Protection Center

Norie Tamura
CSS Japan Security Response Team

Vincent Tiu
Microsoft Malware Protection Center

Henk van Roest
CSS Security EMEA

Steve Wacker
Wadeware LLC

Shawn Wang
Microsoft Malware Protection Center

Iaan Wiltshire
Microsoft Malware Protection Center

Dan Wolff
Microsoft Malware Protection Center

Table of Contents

About this report

The *Microsoft Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, and malicious and potentially unwanted software. Past reports and related resources are available for download at www.microsoft.com/sir. We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their organizations, software, and users.

Reporting period

This volume of the *Microsoft Security Intelligence Report* focuses on the third and fourth quarters of 2012, with trend data for the last several years presented on a quarterly basis. Because vulnerability disclosures can be highly inconsistent from quarter to quarter and often occur disproportionately at certain times of the year, statistics about vulnerability disclosures are presented on a half-yearly basis.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, where *yy* indicates the calendar year and *n* indicates the half or quarter. For example, 1H12 represents the first half of 2012 (January 1 through June 30), and 4Q11 represents the fourth quarter of 2011 (October 1 through December 31). To avoid confusion, please note the reporting period or periods being referenced when considering the statistics in this report.

Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware and potentially unwanted software. For information about this standard, see "Microsoft Malware Protection Center Naming Standard" on the MMPC website. In this report, any threat or group of threats sharing a common unique base name is considered a family for the sake of presentation. This includes threats that may not otherwise be considered families according to common industry practices, such as adware programs and generic detections.

Infection rates are given using a metric called *computers cleaned per mille* (CCM), which represents the number of computers cleaned for every 1,000 executions of the MSRT. For example, if the MSRT has 50,000 executions in a particular location in the first quarter of the year and removes infections from 200 computers, the CCM for that location in the first quarter of the year is 4.0 (200 ÷ 50,000 × 1,000). For periods longer than a quarter, the CCM is averaged for all quarters contained in the period.

Executive Foreword

Welcome to Volume 14 of the *Microsoft Security Intelligence Report*. Over the past six and a half years we've published literally thousands of pages of threat intelligence in this report. Categories of focus continue to include trends and insights on security vulnerabilities, exploit activity, malware and potentially unwanted software, spam, phishing, malicious websites, and security trends from 105+ locations around the world.

Volume 14 contains the latest intelligence with analysis completed, focused on the second half of 2012 and inclusive of trend data going back a year or more. To summarize across the findings of hundreds of pages of new data: industry-wide vulnerability disclosures are down, exploit activity has increased in many parts of the world, several locations with historically high malware infection rates saw improvements but the worldwide malware infection rate increased slightly, Windows 8 has the lowest malware infection rate of any Windows-based operating system observed to date, Trojans continue to top the list of malware threats, spam volumes went up slightly, and phishing levels remained consistent.

We've also included some new, previously unpublished data in this volume of the report that helps quantify the value of using antimalware software. Characterizing the value of security software in a way that resonates relative to other IT investments persists as a challenge for many organizations; especially those who have successfully avoided a security crisis for a long period of time. And, the efficacy of antimalware software is often the source of discussion by Security professionals. Based on telemetry from hundreds of millions of systems around the world, Volume 14 returns the data on malware infection rates for unprotected systems versus systems that run antimalware software. The verdict is in: systems that run antimalware software have significantly lower malware infection rates, even in locations with the highest malware infection rates in the world. This data will likely help many people understand the value of using antimalware software – which we continue to consider a best practice and strongly recommend to all of our customers.

I hope you find this volume of the *Microsoft Security Intelligence Report* useful and enlightening. I also encourage people to visit microsoft.com/sir which includes a variety of additional information.

Adrienne Hall
General Manager, Trustworthy Computing
Microsoft

Trustworthy Computing: Security engineering at Microsoft

Amid the increasing complexity of today's computing threat landscape and the growing sophistication of criminal attacks, enterprise organizations and governments are more focused than ever on protecting their computing environments so that they and their constituents are safer online. With more than a billion systems using its products and services worldwide, Microsoft collaborates with partners, industry, and governments to help create a safer, more trusted Internet.

Microsoft's Trustworthy Computing organization focuses on creating and delivering secure, private, and reliable computing experiences based on sound business practices. Most of the intelligence provided in this report comes from Trustworthy Computing security centers—the Microsoft Malware Protection Center (MMPC), Microsoft Security Response Center (MSRC), and Microsoft Security Engineering Center (MSEC)—which deliver in-depth threat intelligence, threat response, and security science. Additional information comes from product groups across Microsoft and from Microsoft IT (MSIT), the group that manages global IT services for Microsoft. The report is designed to give Microsoft customers, partners, and the software industry a well-rounded understanding of the threat landscape so that they will be in a better position to protect themselves and their assets from criminal activity.

Running unprotected: Measuring the benefits of real-time security software

Practicing safe browsing habits, such as using a web browser with built-in safety features and paying attention to alerts and warnings encountered while browsing, is one of the most important steps Internet users can take to protect themselves from malicious software (malware).[1] Nevertheless, it can sometimes be difficult for even experienced Internet users to avoid coming into contact with malware. The cybercriminals who publish and distribute malware devote significant effort to convincing or tricking Internet users into clicking links that lead to malware, or that download malicious attachments or applications. Even familiar and trusted websites can sometimes be exploited by attackers to distribute malware using tactics such as drive-by downloads. (See page 78 for more information about drive-by downloads.)

An antivirus or antimalware product that offers real-time protection is one of the most crucial defenses a computer user has against these and other malware distribution tactics. Unfortunately, many computers are not protected by real-time antimalware software, either because no such software has been installed, because it has expired, or because it has been disabled intentionally by the user or secretly by malware. New data analyzed by Microsoft reveals the magnitude of the additional risk that such computers and their users face: in the second half of 2012, computers that did not have real-time antimalware protection were more than 5 times as likely to be infected with malware and potentially unwanted software as computers that did have protection.

This section of the *Microsoft Security Intelligence Report* provides additional details about these findings, including statistics that pertain to different countries and regions and to different operating systems and service pack levels. Although the figures may vary slightly between different regions and platforms, the overall message is very clear: using real-time antimalware software from a reputable vendor and keeping it up to date is one of the most effective steps individuals and organizations can take to reduce their exposure to malware.

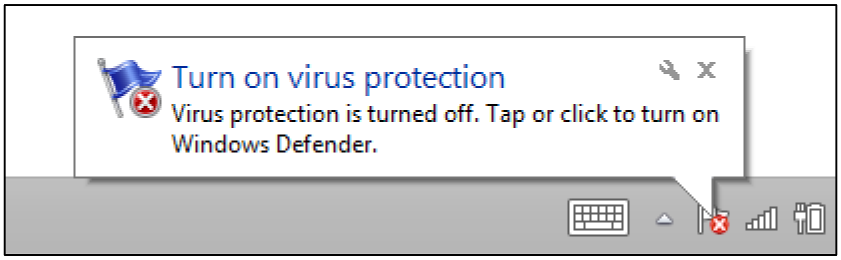
Why go without real-time antimalware protection?

Windows users have many options for effective real-time antimalware protection. Enterprise IT departments typically use Group Policy to install security software on client computers and keep it updated. For home users and others, a number of vendors offer basic real-time products that can be

[1] See www.microsoft.com/security for informative tips and advice about staying safe online.

downloaded or installed inexpensively or at no charge. In addition, all currently supported versions of Windows include mechanisms for monitoring the state of security software running on the computer and displaying alerts and other visual cues to inform the computer user when security software is not installed, not running, or out of date.

Figure 1. Windows alerts the user if antimalware software is disabled or not installed



Turn on virus protection

Virus protection is turned off. Tap or click to turn on Windows Defender.

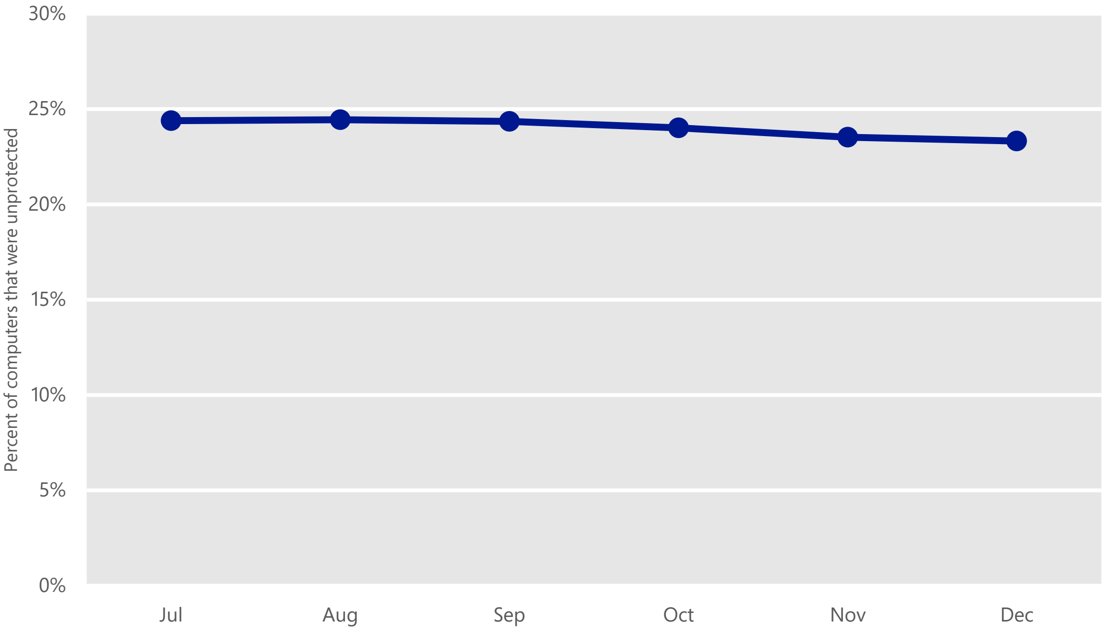
With so many options and reminders, why would users choose to go unprotected? For some users, it may not be a choice. A number of prevalent malware and potentially unwanted software families are capable of disabling some security products, potentially without the user even knowing. Other users may disable or uninstall security software intentionally because of perceived performance issues, a belief that protection is not necessary, or a desire to run programs that would be quarantined or removed by security software. In other cases, users lose up-to-date real-time protection when they don't renew paid subscriptions for their antimalware software, which may come pre-installed with their computers as limited-time trial software. Whatever the reason, users who don't have functioning real-time antimalware protection face significantly greater risk from malware infection than users who do, as the following pages will reveal.

Real-time protection statistics

The *Microsoft Security Intelligence Report* measures computer infection rates with a metric called *computers cleaned per mille* (CCM), which indicates the number of computers cleaned by the Microsoft Malicious Software Removal Tool (MSRT) for every 1,000 computers scanned by the tool. (See page iv for more information about the CCM metric.)

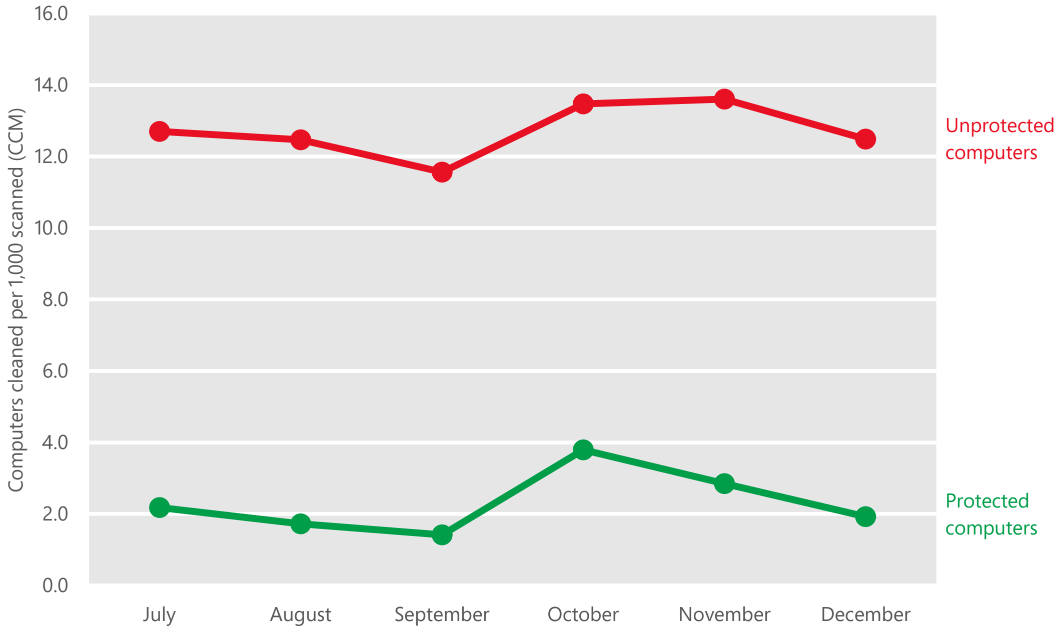
Most computers that run the MSRT obtain each monthly release of the tool automatically through a Microsoft update service such as Windows Update. It executes in the background and automatically removes selected prevalent malware families from the computer. Recent releases of the MSRT collect and report details about the state of real-time antimalware software on the computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

Figure 2. Unprotected computers each month in 2H12



On average, about 24 percent of computers scanned by the MSRT each month in 2H12 were not running real-time antimalware software or were running out-of-date antimalware software at the time they were scanned (referred to as "unprotected computers" in this section). As Figure 3 shows, these computers were significantly more likely to be infected with malware than computers with up-to-date real-time protection ("protected computers").

Figure 3. Infection rates for protected and unprotected computers each month in 2H12

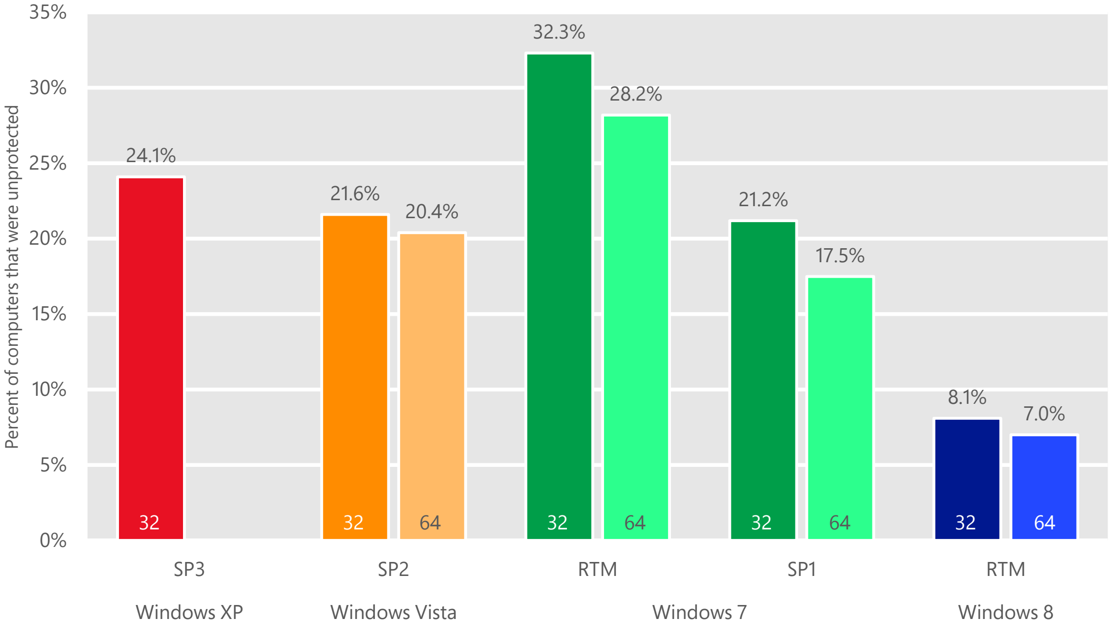


Computers that did not have up-to-date real-time antimalware protection were 5.5 times more likely on average to report malware infections each month than computers that did have protection. The CCM for unprotected computers ranged from 11.6 to 13.6, and the CCM for protected computers ranged from 1.4 to 3.8.

Operating system statistics

Computers running newer Windows versions and service pack levels were generally more likely to run up-to-date real-time antimalware software, as shown in Figure 4.

Figure 4. Unprotected computers in 2H12, by operating system version and service pack level



32 = 32-bit edition; 64 = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.05 percent of total MSRT executions in 2Q12 shown.

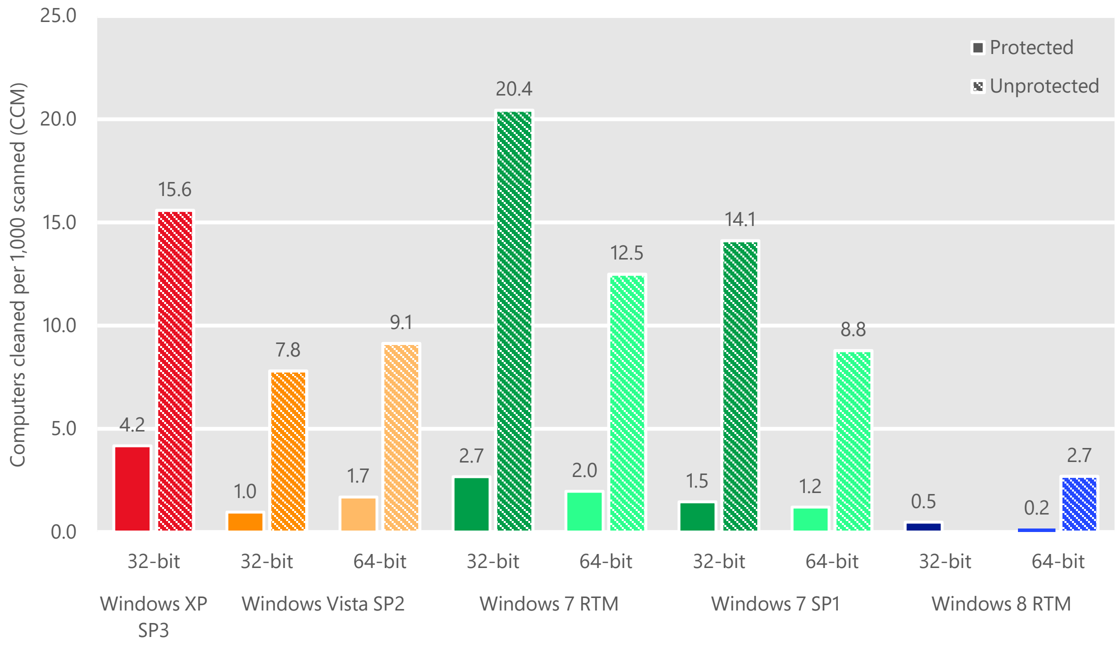
Computers running Windows 8 had the highest rate of protection, with just 8.1 percent of computers running the 32-bit edition and 7.0 percent of computers running the 64-bit edition lacking up-to-date real-time protection. Windows 8 includes real-time antimalware and antispyware protection by default,[2] which is likely a significant factor in the reduced number of Windows 8 computers not running security software; previous releases of Windows did not include real-time antimalware software by default. In addition, Windows 8 was only generally available for slightly more than two months of the half-year period, which provided less of an opportunity for real-time protection to expire or to be disabled by computer users or by malware.

Among supported releases of Windows, the lowest rate of protection was observed on computers running the RTM version of Windows 7, of which 32.3 percent of computers running the 32-bit edition and 28.2 percent of computers running the 64-bit edition lacked up-to-date real-time protection. Computers running Windows 7 SP1, the most recent service pack available for Windows 7, were significantly less likely to lack real-time protection than computers running the RTM version.

[2] See windows.microsoft.com/en-US/windows-8/windows-defender for more information about antimalware protection in Windows 8.

Although infection rates for unprotected computers were significantly higher than those for protected computers, regardless of operating system version or service pack level, platforms with greater usage of up-to-date security software also tended to have lower infection rates in general, as shown in Figure 5.

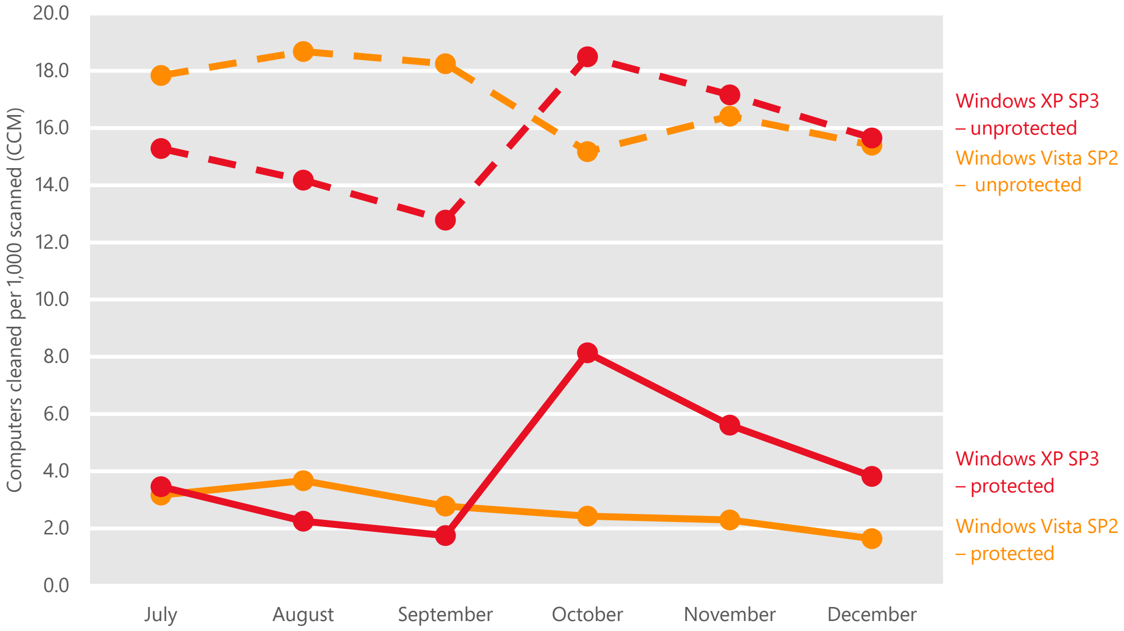
Figure 5. Infection rates for computers with and without up-to-date real-time antimalware protection in 2H12, by operating system version and service pack level



32 = 32-bit edition; 64 = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.05 percent of total MSRT executions in 2Q12 shown.

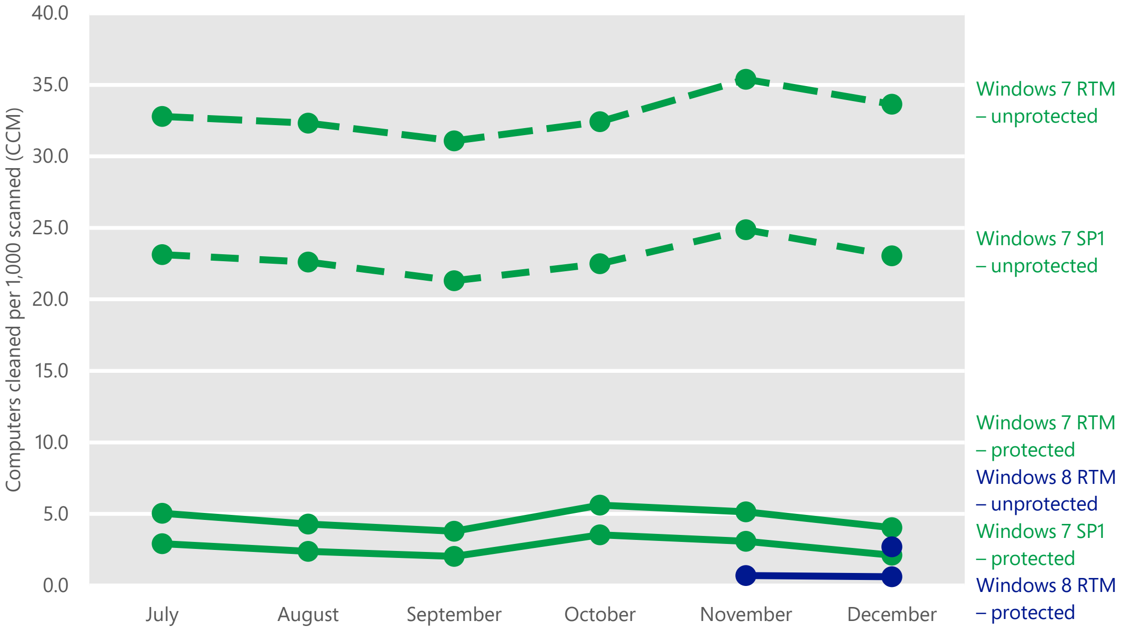
Of all the currently supported Windows client operating system and service pack combinations, Windows XP SP3 had the smallest relative difference between the infection rates of protected and unprotected computers, with protected computers reporting an infection rate 3.7 times greater than unprotected computers. More recently released versions of Windows feature a number of security improvements that are not included in Windows XP, which means that even protected computers running Windows XP face risks from exploitation and malware infection that don’t apply to more recent versions of Windows.

Figure 6. Infection rates for computers running Windows XP and Windows Vista with and without up-to-date real-time antimalware protection in 2H12, by month



The RTM version of Windows 7, which had the highest percentage of unprotected computers of any platform (shown in Figure 4), also displayed the highest infection rates for unprotected computers, with a CCM of 20.4 for the 32-bit edition and 12.5 for the 64-bit edition. This correlation suggests that a larger population of unprotected users within a platform creates an attractive target for attackers.

Figure 7. Infection rates for computers running Windows 7 and Windows 8 with and without up-to-date real-time antimalware protection in 2H12, by month



On Windows 8, which had the lowest infection rate overall, unprotected computers have an infection rate (CCM) that is 16.2 times greater than the infection rate for protected users. This difference is much higher than average, and suggests that protected users benefit far more from their protection than protected users on other platforms. Because Windows 8 includes real-time antimalware protection by default,[3] many or most unprotected Windows 8 computers may lack protection because their users have chosen to disable it.[4]

The threat family most commonly detected by Microsoft security products on Windows 8 computers in 2H12 was Win32/Keygen, a detection for tools that generate keys for various software products that are often distributed by software pirates to enable users to run software illegally. Such tools are typically detected as malware or potentially unwanted software by most antimalware scanners, so some users may choose to disable their security software to use the tools.[5] As the analysis presented here demonstrates, such users face significantly

[3] See blogs.msdn.com/b/b8/archive/2011/09/15/protecting-you-from-malware.aspx for more information about this change and other security improvements in Windows 8.

[4] As with other Windows releases, many computer vendors ship Windows 8 with a preinstalled trial version of a different antivirus product. The MMPC will continue to monitor MSRT telemetry to determine whether Windows 8 computers tend to become unprotected due to license expiration or for other reasons.

[5] Microsoft classifies Win32/Keygen as potentially unwanted software rather than malware, and therefore does not include detection signatures for the family in the MSRT.

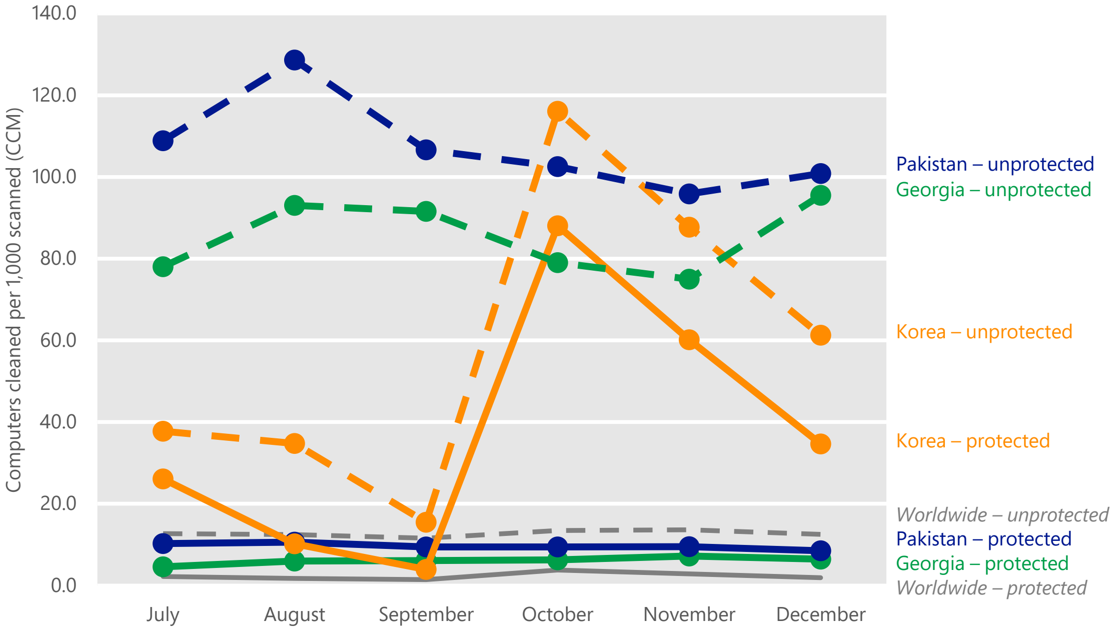
greater risk from malware than do users who leave real-time protection enabled.[6]

See “Operating system infection rates” on page 43 for more information and statistics about infection rates by operating system.

Geographic statistics

Figure 8 and Figure 9 show the infection rate differences for protected and unprotected computers in locations around the world with particularly high and low infection rates overall.

Figure 8. Infection rates for protected and unprotected computers in three locations with high CCM



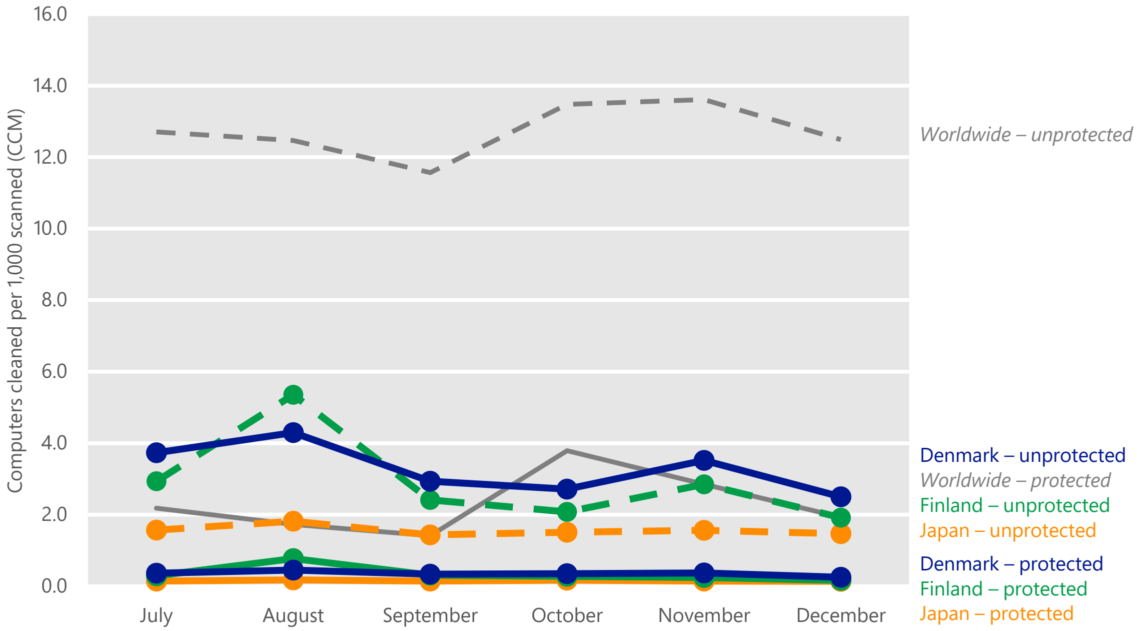
Pakistan and Georgia, which both had significantly more computers without up-to-date real-time protection than the world as a whole (38.6 percent in Pakistan, 33.5 percent in Georgia) also displayed a larger infection rate gap between protected and unprotected computers than the world overall. In Pakistan, unprotected computers were 11.7 times more likely to be infected than protected computers, which translates to a CCM over 100.0 in 5 out of the 6 months in 2H12—in other words, the MSRT found that more than 1 of every 10 unprotected computers in Pakistan was infected with malware. In Georgia,

[6] See “Deceptive downloads: Software, music, and movies” on page 1 of *Microsoft Security Intelligence Report, Volume 13 (January–June 2012)* for more information about Keygen and the threats users face from unsecure software distribution channels.

unprotected computers were 14.0 times more likely to be infected than protected computers, with CCM figures between 75.0 and 95.5 each month, compared to a range of 4.6 to 6.4 for protected computers in Georgia.

In Korea, infection rates for both protected and unprotected computers were heavily influenced by a steep increase in detections of the rogue security software family Win32/Onescan and the Trojan downloader family Win32/Pluzoks, which affected both protected and unprotected computers in similar proportions. Overall, the infection rate for unprotected computers in Korea in 2H12 was 1.6 times higher than the infection rate for protected computers there. See "Rogue security software" on page 52 for more information.

Figure 9. Infection rates for protected and unprotected computers in three locations with low CCM



Unprotected computers in Japan have an infection rate that is 10.4 times higher than the infection rate for protected computers. The overall infection rate in Japan for protected users is very low, at 0.2 on average. Unprotected users make up 23.2 percent of computers in Japan, which is slightly lower than the worldwide average.

The infection rate for unprotected computers in Finland is 8.6 times higher than the infection rate for protected computers there. Finland also has a significantly higher adoption rate for real-time security software than the world as a whole, with only 14.6 percent of computers in Finland lacking up-to-date real-time protection.

In Denmark, unprotected computers have an infection rate that is 9.3 times higher than that of protected computers. The adoption rate for real-time security software in Denmark is slightly higher than for the world as a whole, with 19.8 percent of computers lacking up-to-date real-time protection, about 4 percentage points lower than the global average.

Guidance: Fighting infection with real-time protection

Although there is no such thing as a perfect security product, the findings in this section clearly show that using real-time security software from a reputable vendor and keeping it up to date are two of the most important steps individuals and organizations can take to reduce the risk they face from malware and potentially unwanted software. With attackers becoming ever more proficient at exploiting software vulnerabilities and trusted relationships to spread malware in unexpected ways, it is dangerous for even expert users to assume that they will be able to detect threats on their own without the help of real-time protection before being affected by them. Simply installing and using real-time antimalware software can help individuals and organizations reduce malware infection by more than 80 percent. See www.microsoft.com/windows/antivirus-partners for a list of vendors that provide consumer security software solutions for Windows.

Users who believe their security software may have been disabled by malware should take advantage of a tool like the Microsoft Safety Scanner (www.microsoft.com/security/scanner/) or Windows Defender Offline (windows.microsoft.com/en-US/windows/what-is-windows-defender-offline) to scan their computers for malware and remove any threats that are found.

Microsoft

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security