Microsoft

Microsoft Security Intelligence Report: Hong Kong Findings

Tim Rains
Director
Trustworthy Computing

About SIRv14

"Measuring the benefits of real-time security software"

Worldwide threat assessment

- Vulnerability trends
- Exploit trends
  - O/S, browser, and applications
- Malware and potentially unwanted software

Regional threat assessment

- 105 countries/regions

Malware Data From Over a Billion Systems Worldwide

ONE SECURITY REPORT

The Security Intelligence Report (SIR) is an analysis of the current threat landscape based on data from internet services and over a billion systems worldwide to help you protect your organization, software, and people.

View the Security Intelligence Report at **www.microsoft.com/SIR**

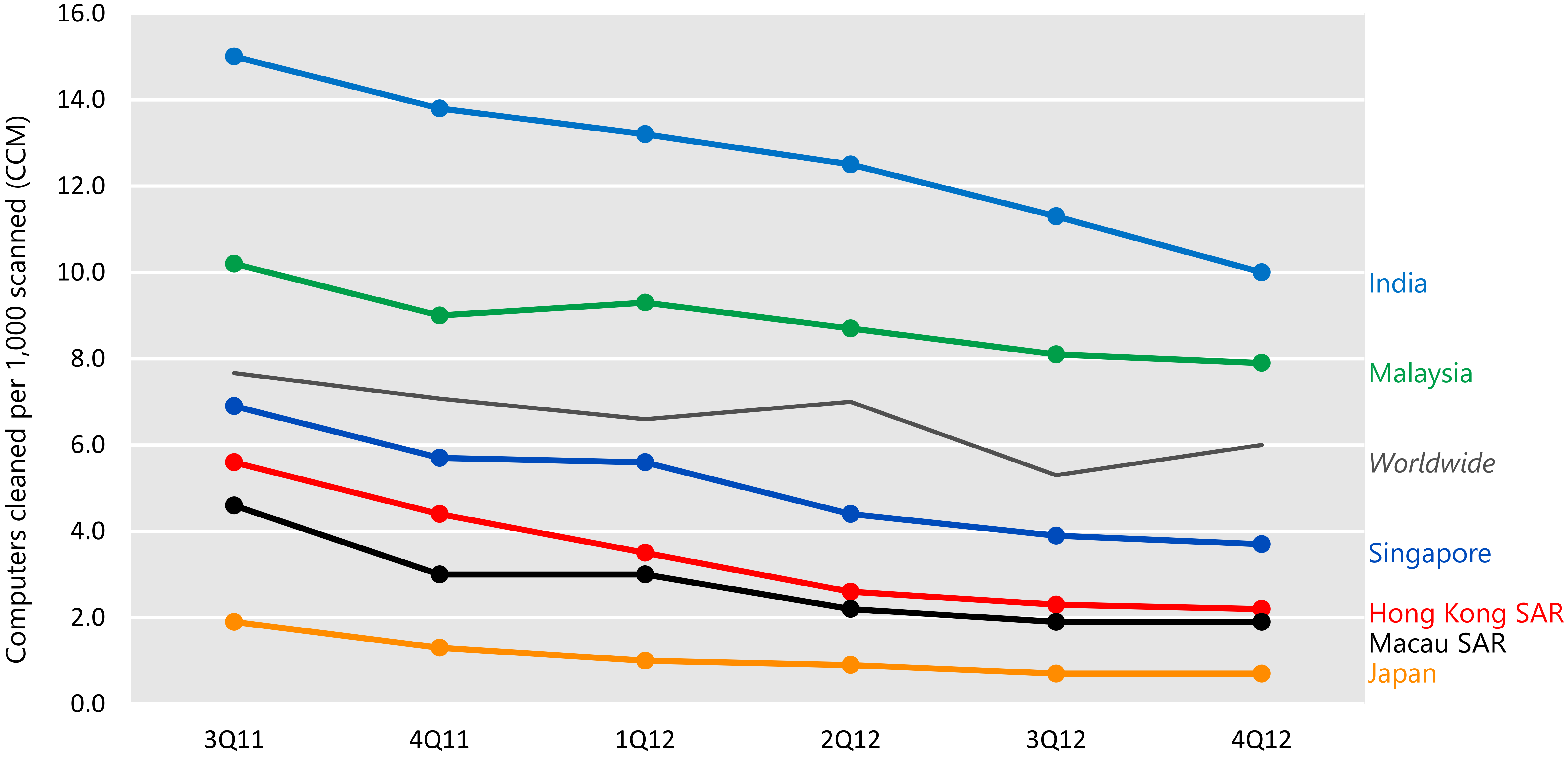
Microsoft | Security Intelligence Report

About SIRv14

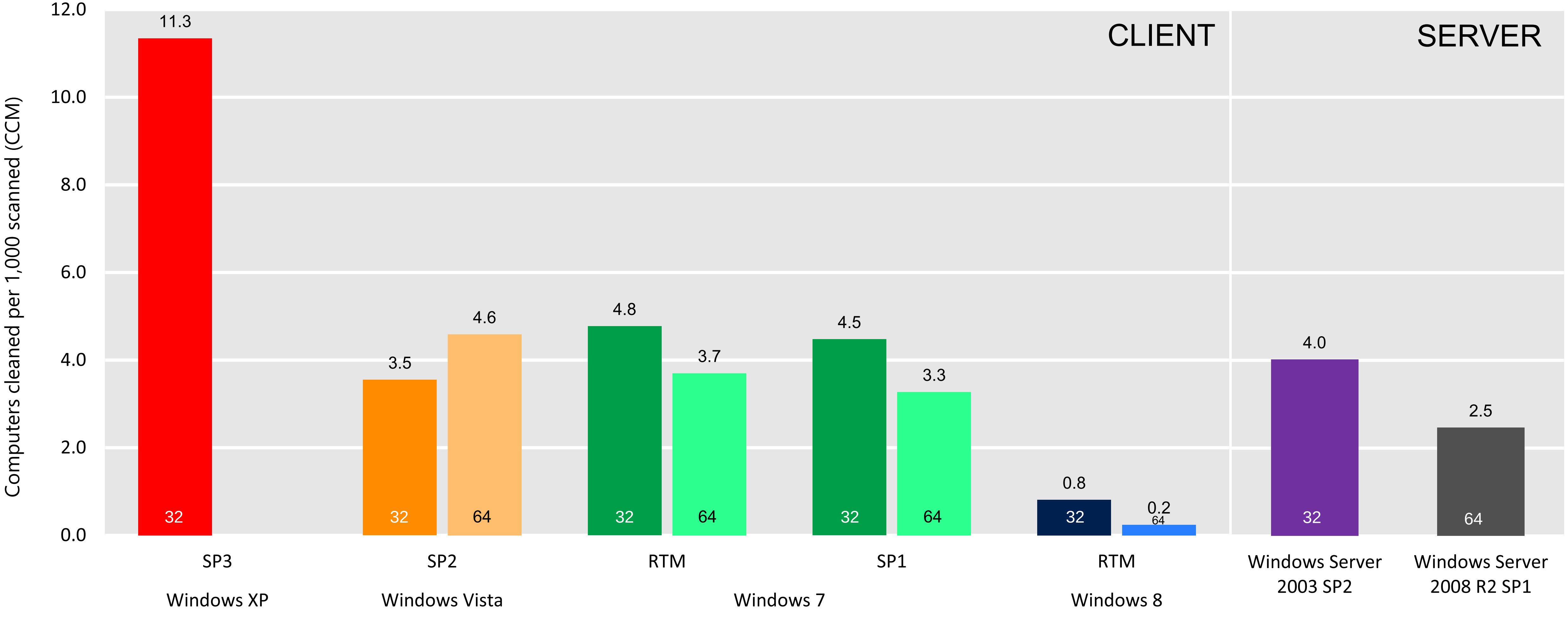
Product name	Main customer segment		Malicious software		Spyware and potentially unwanted software		Available at no additional charge	Main distribution methods
	Consumers	Business	Scan and remove	Real-time protection	Scan and remove	Real-time protection		
Windows Malicious Software Removal Tool	●		Prevalent Malware families				●	WU/AU Download Center
Windows Defender	●				●	●	●	Download Center Windows Vista/ Windows 7/Windows 8
Windows Safety Scanner	●		●		●		●	Cloud
Microsoft Security Essentials	●		●	●	●	●	●	Cloud
Exchange Online Protection		●	●	●				Cloud
System Center Endpoint Protection		●	●	●	●	●		Volume licensing

- **Hotmail**—more than 280 million active users
- **Internet Explorer**—the world’s most popular browser with SmartScreen, Microsoft Phishing filter
- **Exchange Online Protection**—scans billions of email messages a year
- **Windows Malicious Software Removal Tool**—executes on more than 600 million unique computers worldwide each month
- **Microsoft security essentials**—available in over 30 languages
- **Bing**—billions of webpages scanned each month

Malware infection trends in Asia

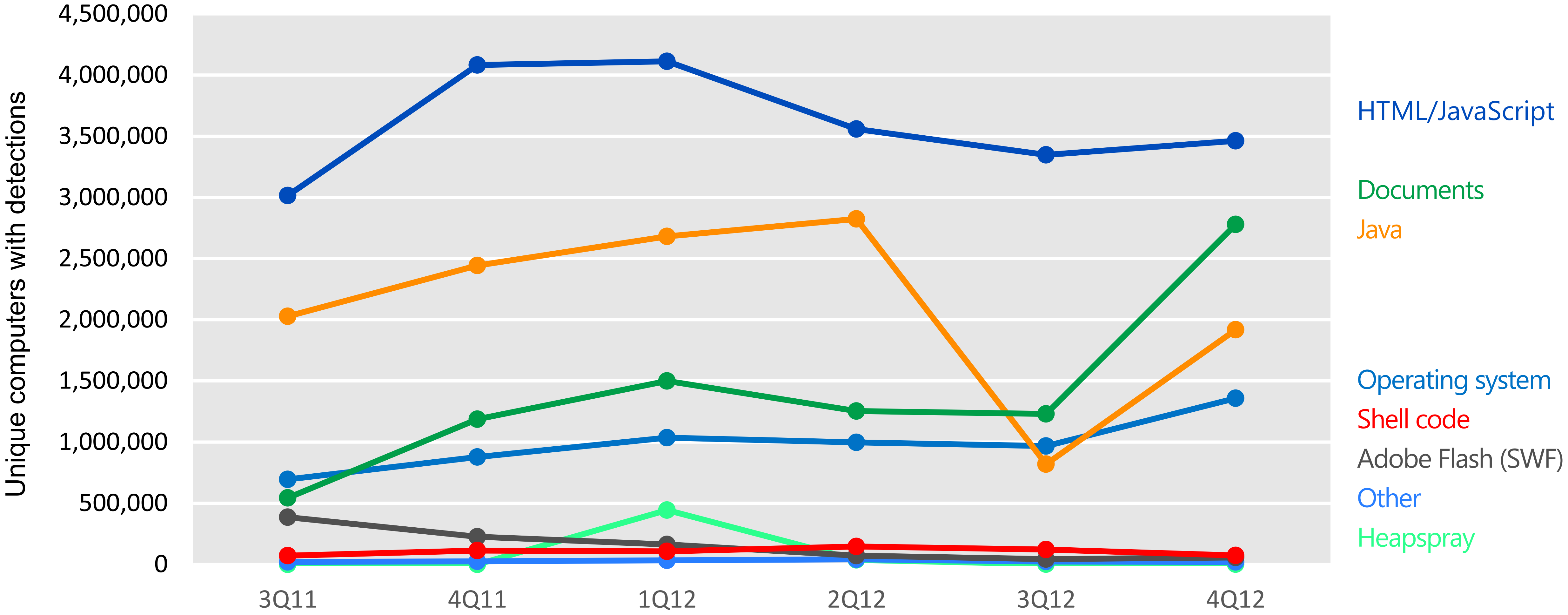


Infection rates by OS and service pack



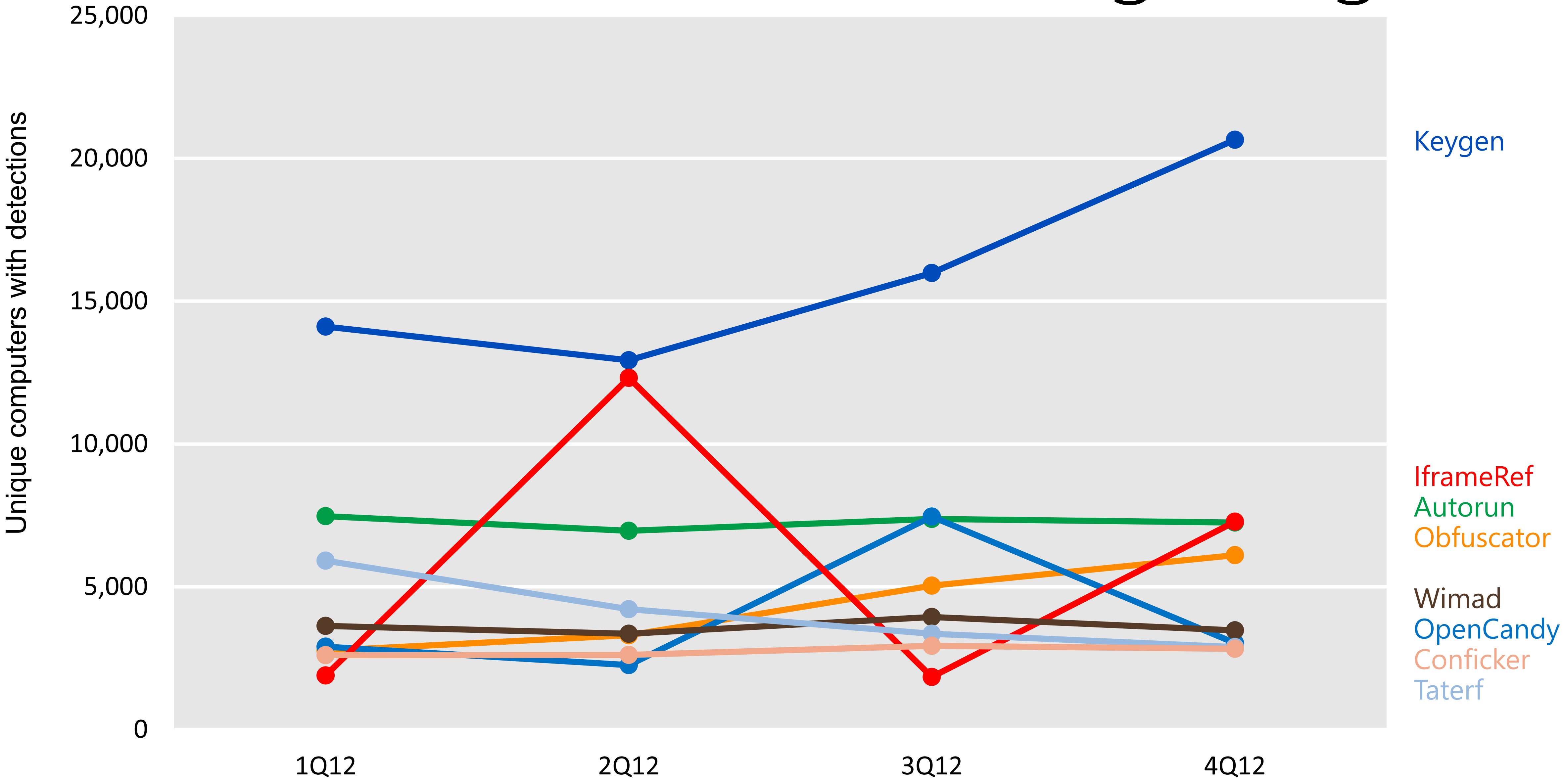
- Normalized numbers
- Infection rates for more recently released operating systems and service packs are consistently lower than earlier ones, for both client and server platforms

Exploit trends

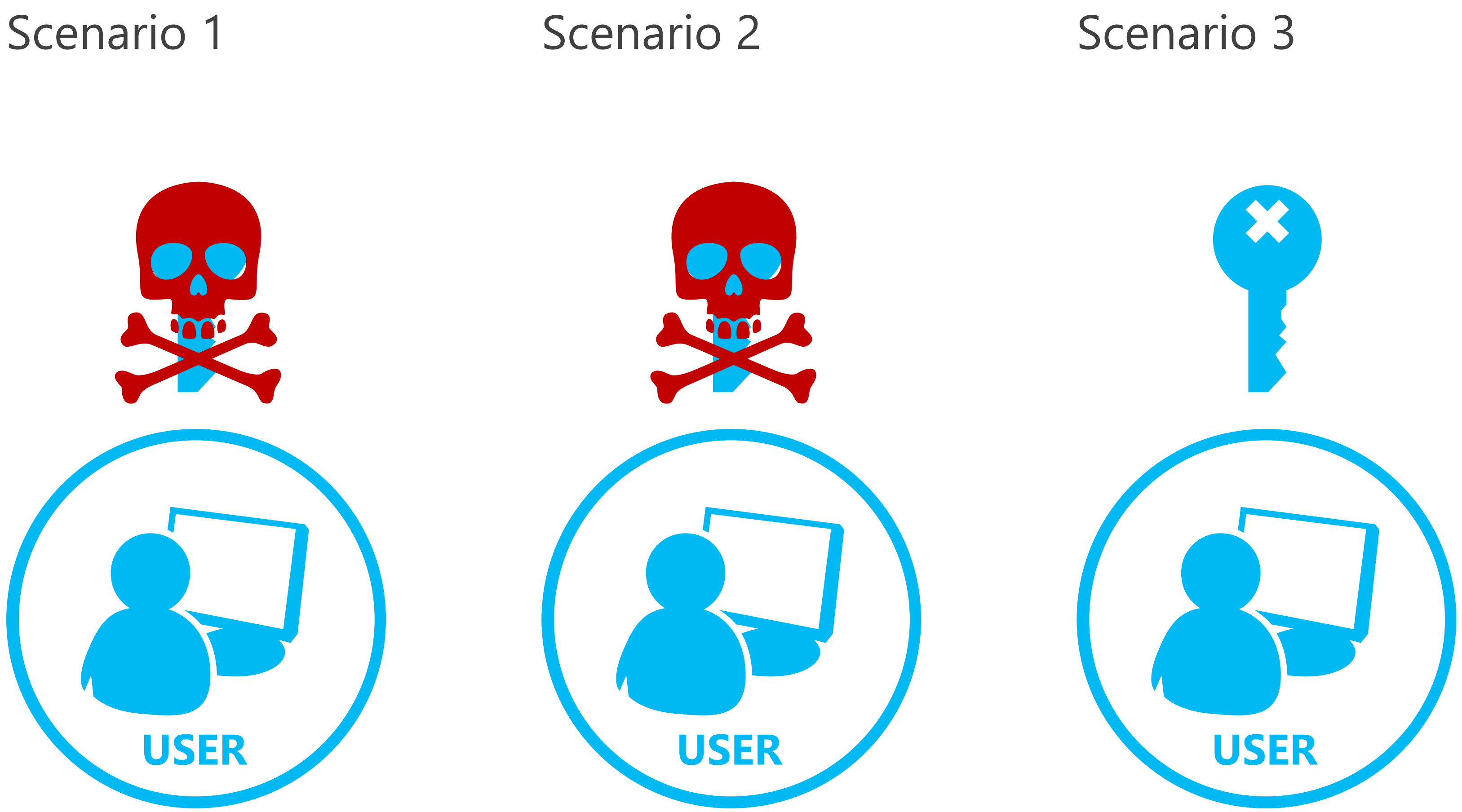


The number of computers reporting exploits delivered through HTML or JavaScript remained high during the second half of 2012, primarily driven by the continued prevalence of the multi-platform exploit family Blacole

Prevalent threat families: Hong Kong



3 scenarios

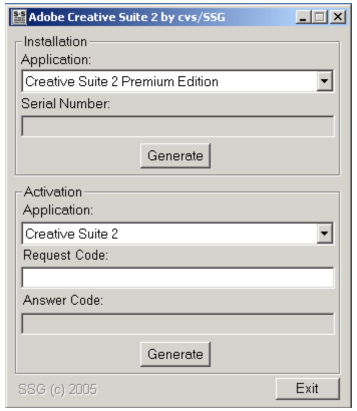


Scenario 1

Scenario 2

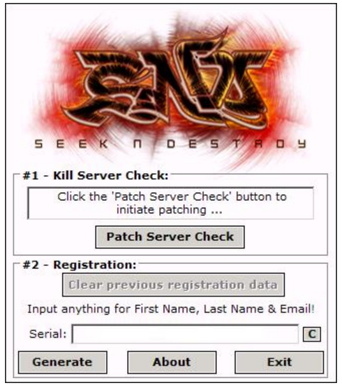
Scenario 3

Keygen examples



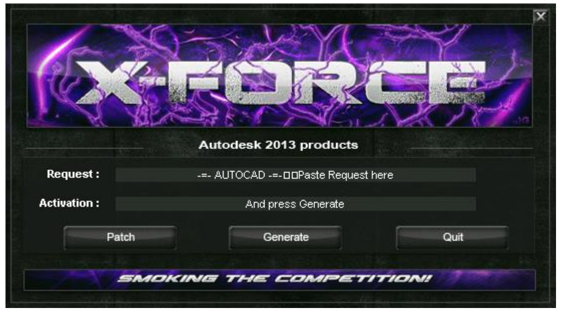
Application: Creative Suite 2 Premium Edition

Application: Creative Suite 2



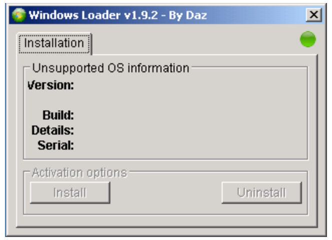
Click the 'Patch Server Check' button to initiate patching ...

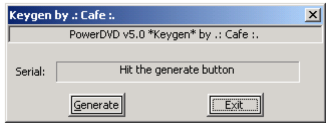
Input anything for First Name, Last Name & Email!



-=- AUTOCAD -=-□□Paste Request here

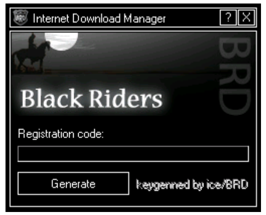
And press Generate

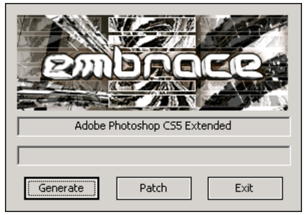




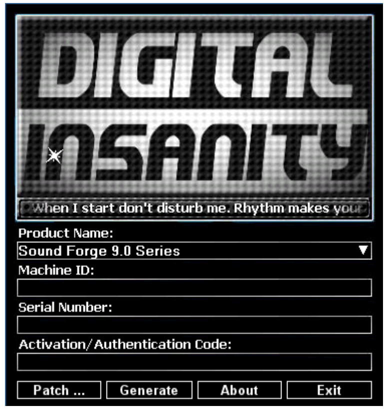
PowerDVD v5.0 *Keygen* by .: Cafe :.

Hit the generate button

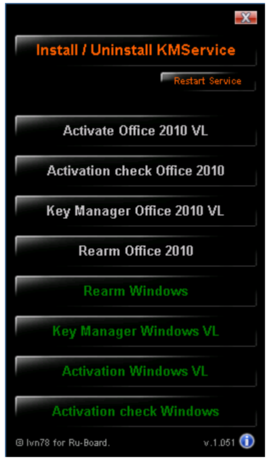


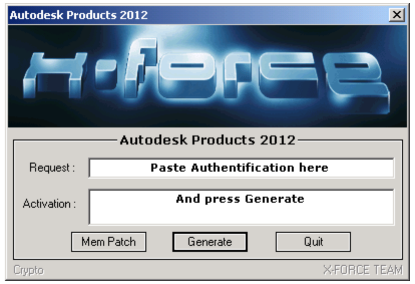


Adobe Photoshop CS5 Extended



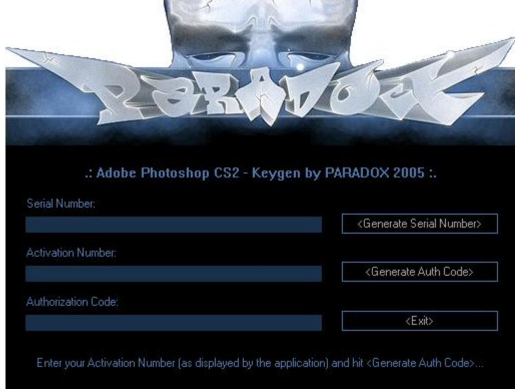
Product Name: Sound Forge 9.0 Series





Paste Authentification here

And press Generate



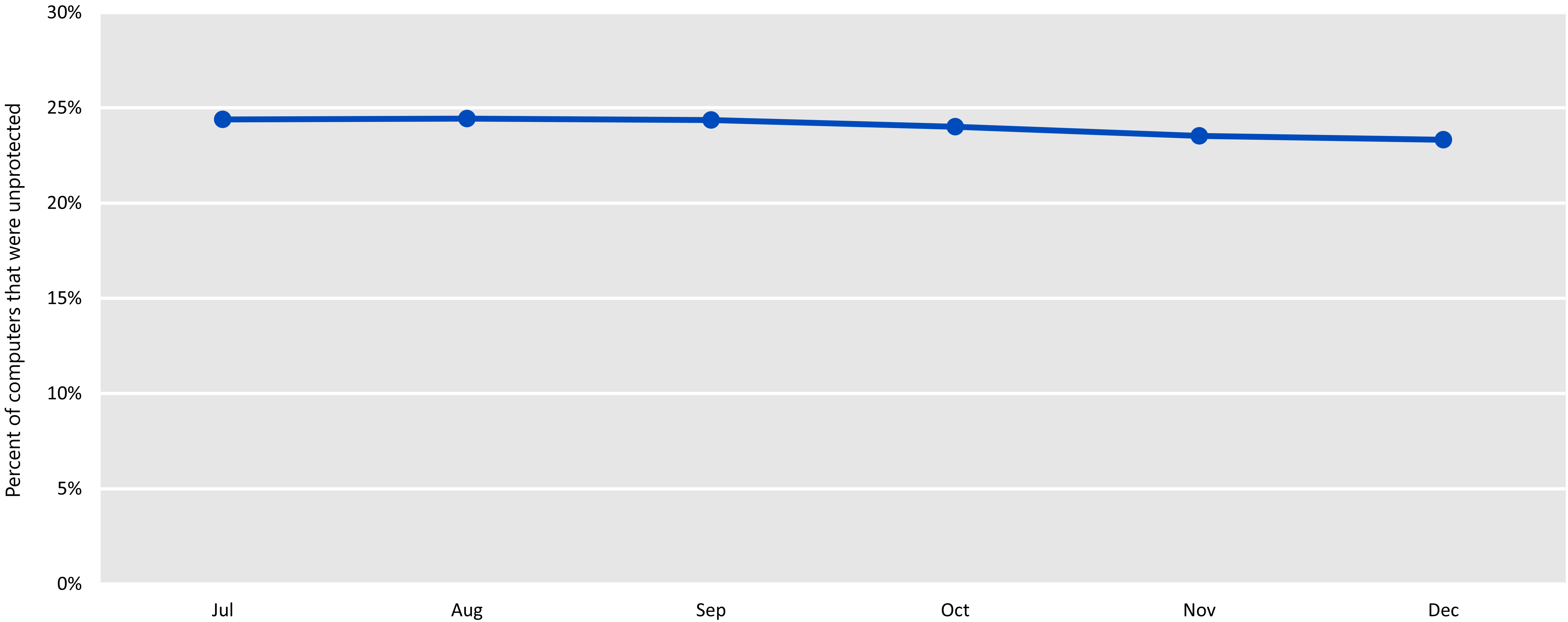
Enter your Activation Number (as displayed by the application) and hit <Generate Auth Code>...

Featured intelligence

Introduction

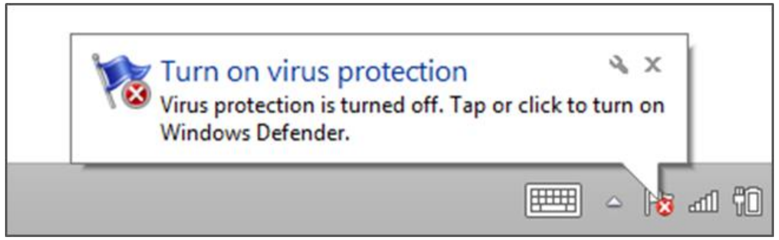
In 2H12, computers that did not have up-to-date real-time antimalware protection were more than 5 times as likely to be infected with malware as computers that did

Computers lacking real-time antimalware protection



On average, about 24 percent of computers scanned by the MSRT each month in 2H12 were not running up-to-date real-time antimalware software at the time they were scanned

Why some users are not running a real-time antimalware solution

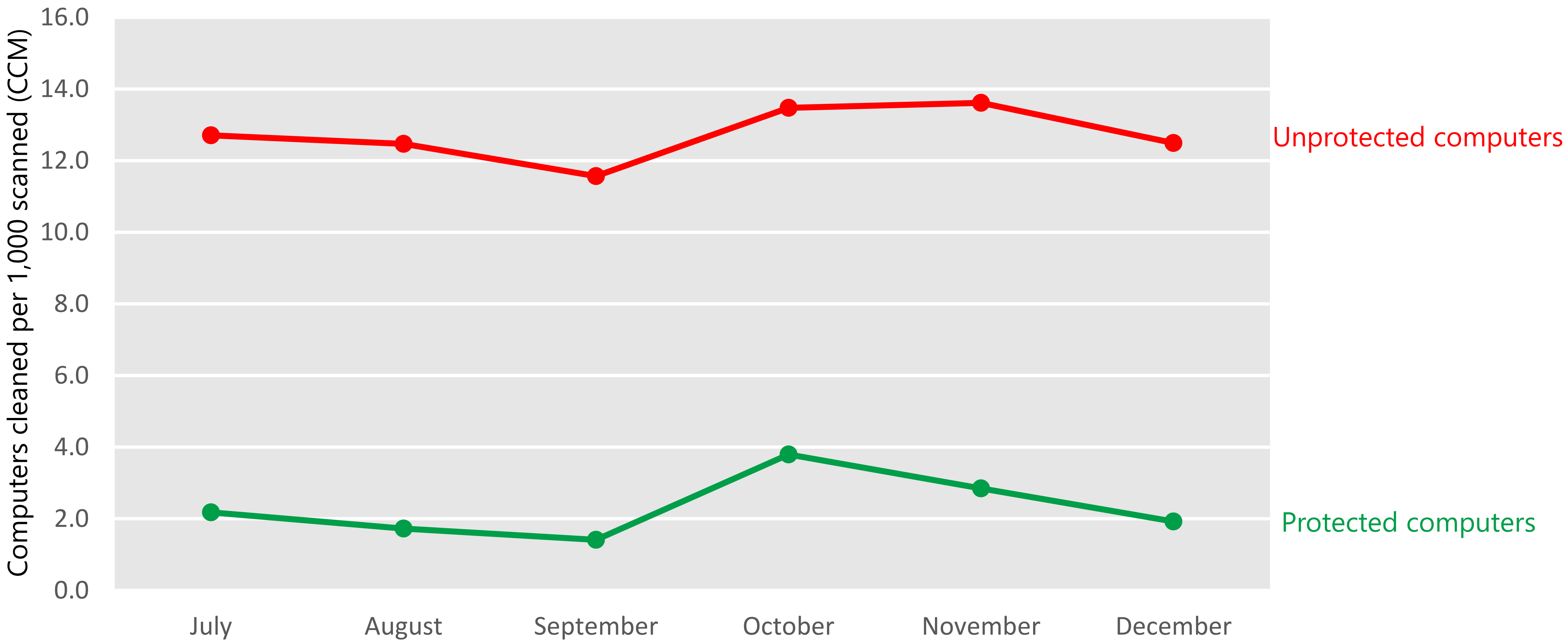


Turn on virus protection

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

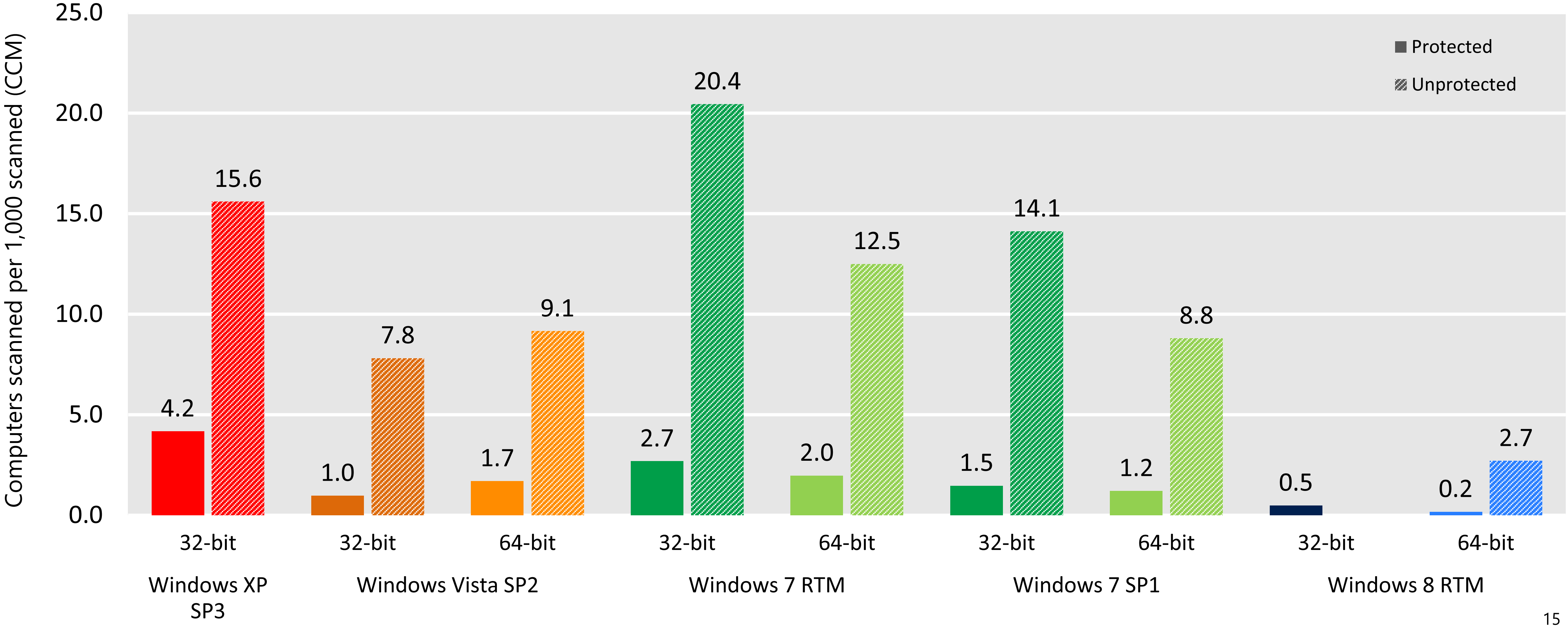
USER
USER
USER

Infection rates for protected and unprotected computers



Computers without up-to-date real-time antimalware protection were 5.5 times more likely on average to report malware infections each month than computers with protection

Infection rates for computers with and without real-time antimalware protection



Guidance

- Using up-to-date real-time security software is an important part of a defense in depth strategy
- Simply installing and using real-time antimalware software can help individuals and organizations reduce the risk they face from malware by more than 80 percent

www.microsoft.com/windows/antivirus-partners/

Protect your environment

Security Intelligence Report (SIR) helps customers protect:

Organizations
Protect your organization’s network from security threats.

Software
Protect your applications and minimize malware threats.

People
Protect workers against privacy and security threats.

Keep all software on your systems updated
Third party, as well as Microsoft

Use Microsoft Update, not Windows Update
Updates all Microsoft software

Run antivirus software from a trusted vendor
Keep it updated

Use caution when clicking on links to Web pages

Use caution with attachments and file transfers

Avoid downloading pirated software

Protect yourself from social engineering attacks

Resources

Microsoft Security Intelligence Report
www.microsoft.com/sir

Microsoft Security Blog
blogs.technet.com/b/security

Twitter
@msftsecurity

Microsoft Trustworthy Computing
www.microsoft.com/twc

Microsoft

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

Extra slides

Top Malware families blocked by SmartScreen: Hong Kong

	Family	Category	Percent of Malware impressions
1	Win32/Orsam!rts	Misc. Trojans	32.27%
2	Win32/Vobfus	Trojan downloaders and droppers	10.55%
3	Win32/Dynamer!dtc	Misc. Trojans	7.38%
4	Win32/Nitol	Misc. potentially unwanted software	6.00%
5	Win32/VB	Misc. potentially unwanted software	5.18%
6	Win32/Kuluoz	Trojan downloaders and droppers	3.80%
7	Win32/Obfuscator	Misc. potentially unwanted software	3.72%
8	Java/Boxer	Misc. Trojans	3.02%
9	Win32/Netbot	Backdoors	2.88%
10	Win32/Banker	Misc. Trojans	2.41%
11	X97M/Mailcab	Viruses	2.33%
12	Win32/Farfli	Backdoors	2.08%
13	Win32/Agent	Misc. Trojans	1.92%
14	Win32/Delfsnif	Trojan downloaders and droppers	1.74%
15	Win32/Dunik!rts	Trojan downloaders and droppers	1.61%