MICROSOFT SECURITY INTELLIGENCE REPORT VOLUME 15 JANUARY – JUNE 2013

Tim Rains

Director, Trustworthy Computing, Microsoft

Jeff Jones

Director, Trustworthy Computing, Microsoft

RSA CONFERENCE EUROPE 2013

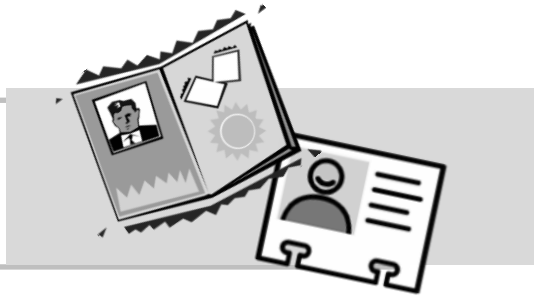
Session ID: SPO-T06

Session Classification: Intermediate

Who are these guys?

Company

- Microsoft Corporation
- Trustworthy Computing group



Jeff Jones

- Director, Trustworthy Computing
- 25-year Security Guy : DoD, TIS, McAfee, PGP, MSFT
- Microsoft Security Blog & Trustworthy Computing Blog
- @securityjones

Tim Rains

- Director, Trustworthy Computing
- Threat intel, MSRC, MMPC, MSEC, Cybersecurity, Cloud Security
- Reformed Engineer: Windows, IT
- Microsoft Security Blog, Trustworthy Computing Blog Microsoft EU blog
- @MSFTSecurity

Session Objectives

Learn

- Come up to speed on the latest threat intelligence
- Understand threat trends to better protect

Apply

- Lessons from what is working
- Guidance to help manage threats

Have Fun!

- We are data geeks
- Our idea of fun is strange, maybe yours is as well

What You Will Hear Today

- Encounter rate: a new metric for analyzing malware prevalence
- Vulnerabilities & Exploits
- Malware Trends
- Applying it
- Q&A

About SIRv15: Contents

New “Encounter Rate” metric

Worldwide Threat Assessment

- Vulnerability trends
  - O/S, Browser, and applications
- Exploit trends
- Malware
- Potentially unwanted software
- Spam trends
- Malicious websites

Regional Threat Assessment

- 100+ countries/regions

About SIRv15: Data Sources

Product name	Main customer segment		Malicious software		Spyware and potentially unwanted software		Available at no additional charge	Main distribution methods
	Consumer	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 Defender	•		•	•	•	•	•	Windows 8
Windows Safety scanner	•		•		•		•	Cloud
Microsoft Security Essentials	•		•	•	•	•	•	Cloud
Exchange Online Protection		•	•	•				Cloud
System Center Endpoint Protection		•	•	•	•	•		Volume licensing

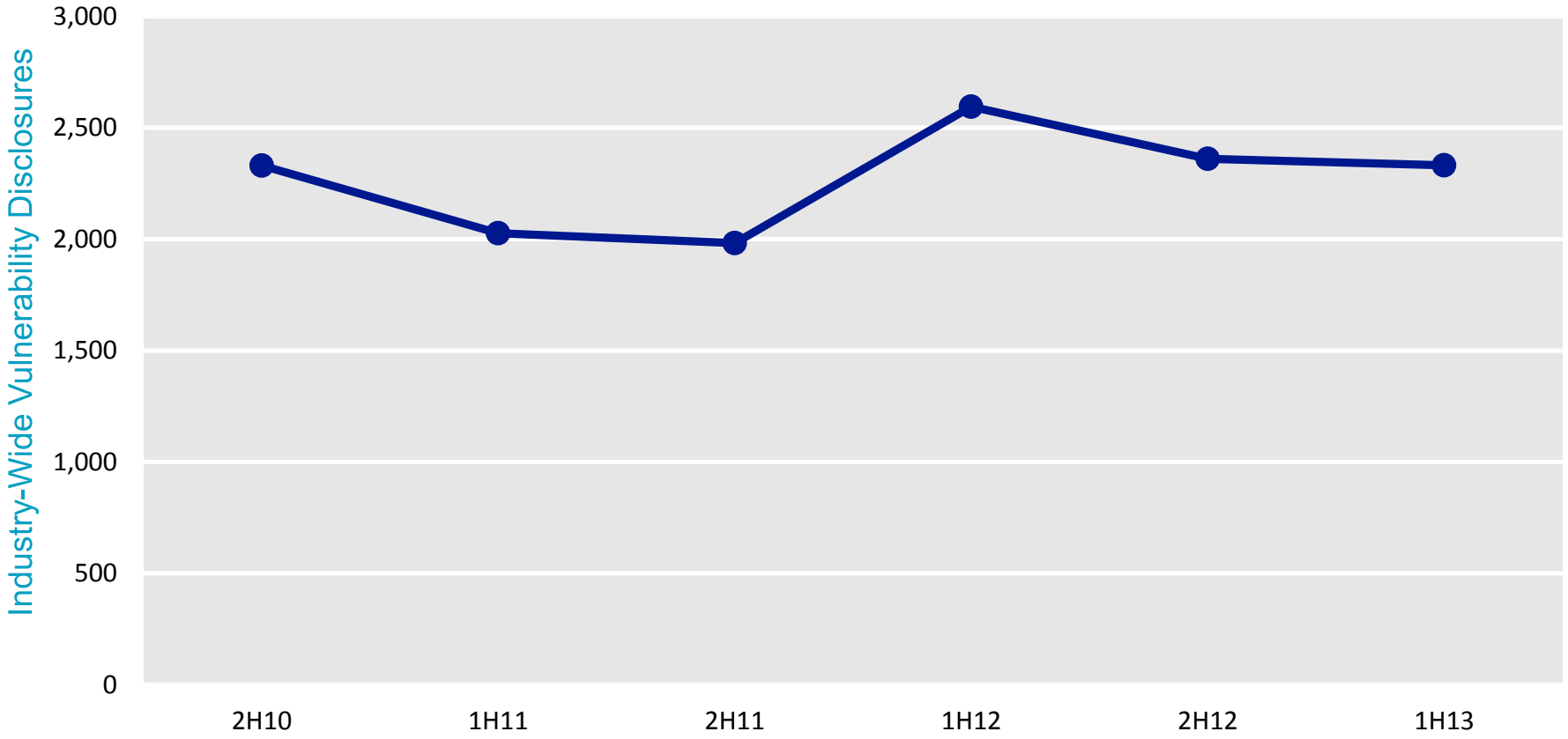
- **Outlook.com –** more than 400 million users
- **Internet Explorer –** the world's most popular browser with SmartScreen, Microsoft Phishing Filter
- **Exchange Online Protection** – scans billions of e-mail messages a year for threats
- **Windows Malicious Software Removal Tool –** users opt-in to share data from more than 600 million computers worldwide each month
- **Microsoft Security Essentials** – available in over 30 languages
- **Bing –** billions of Web-pages scanned each month

Vulnerability Trends

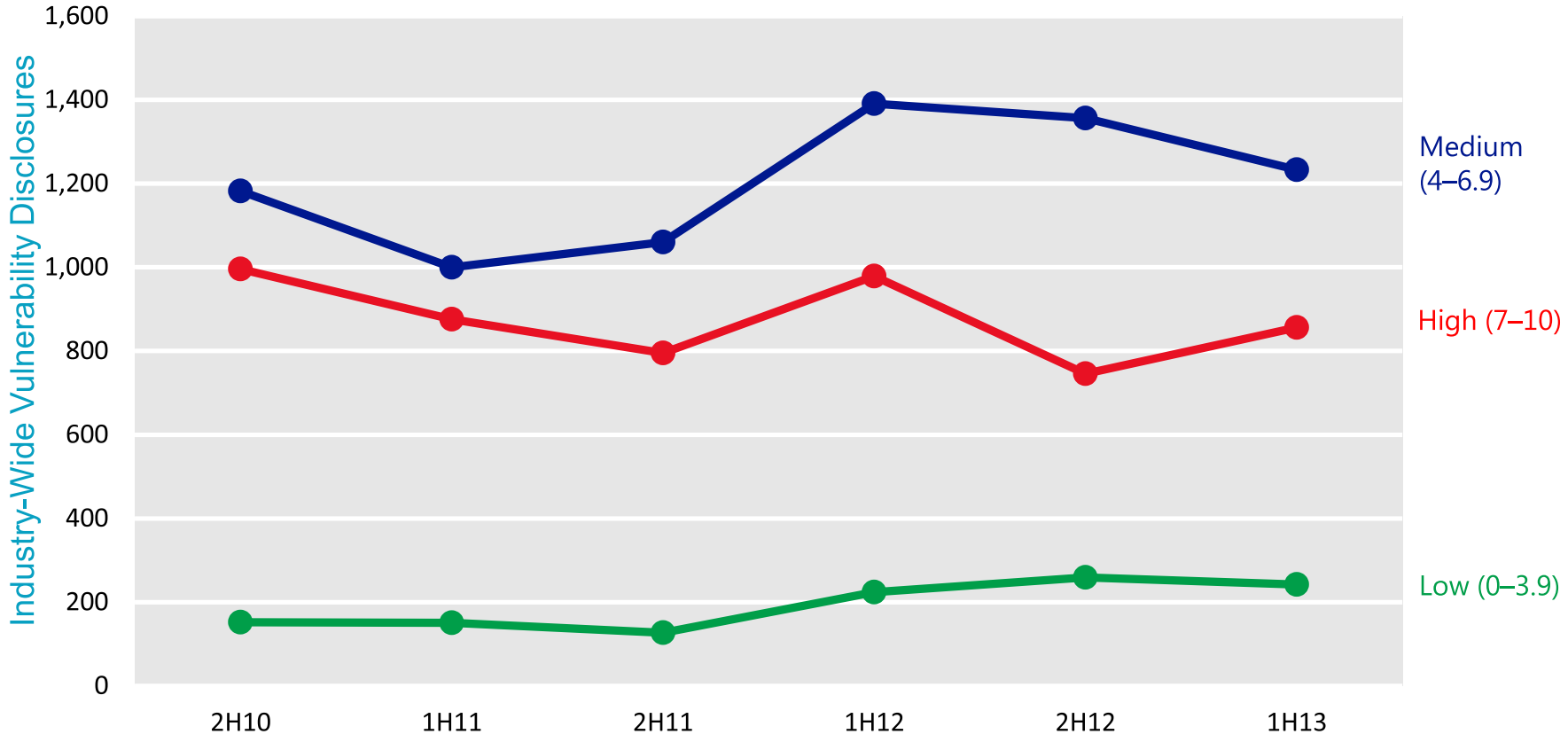
#RSAC

RSA CONFERENCE EUROPE 2013

Industry-Wide Vulnerability Disclosures

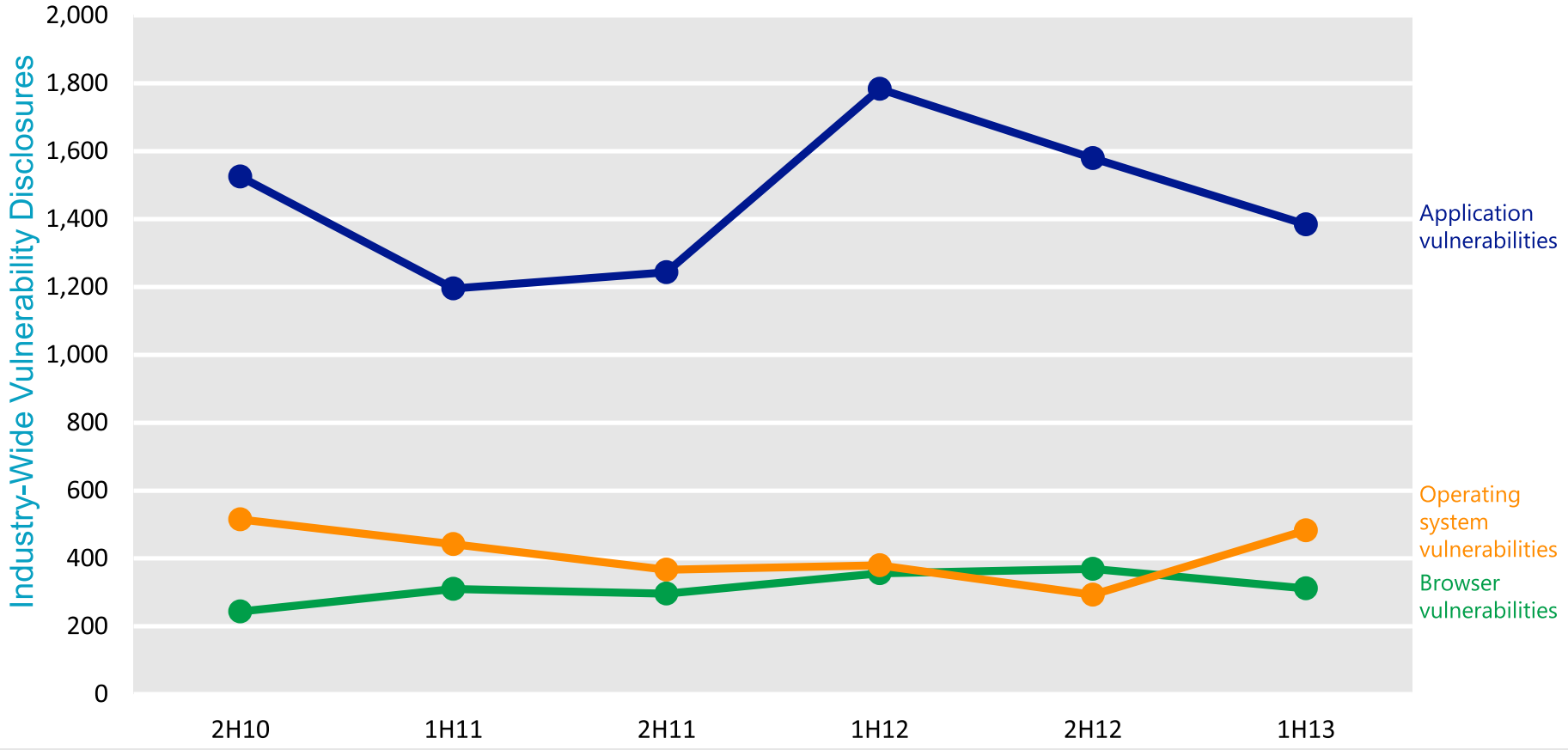


Industry-Wide Vulnerability Severity



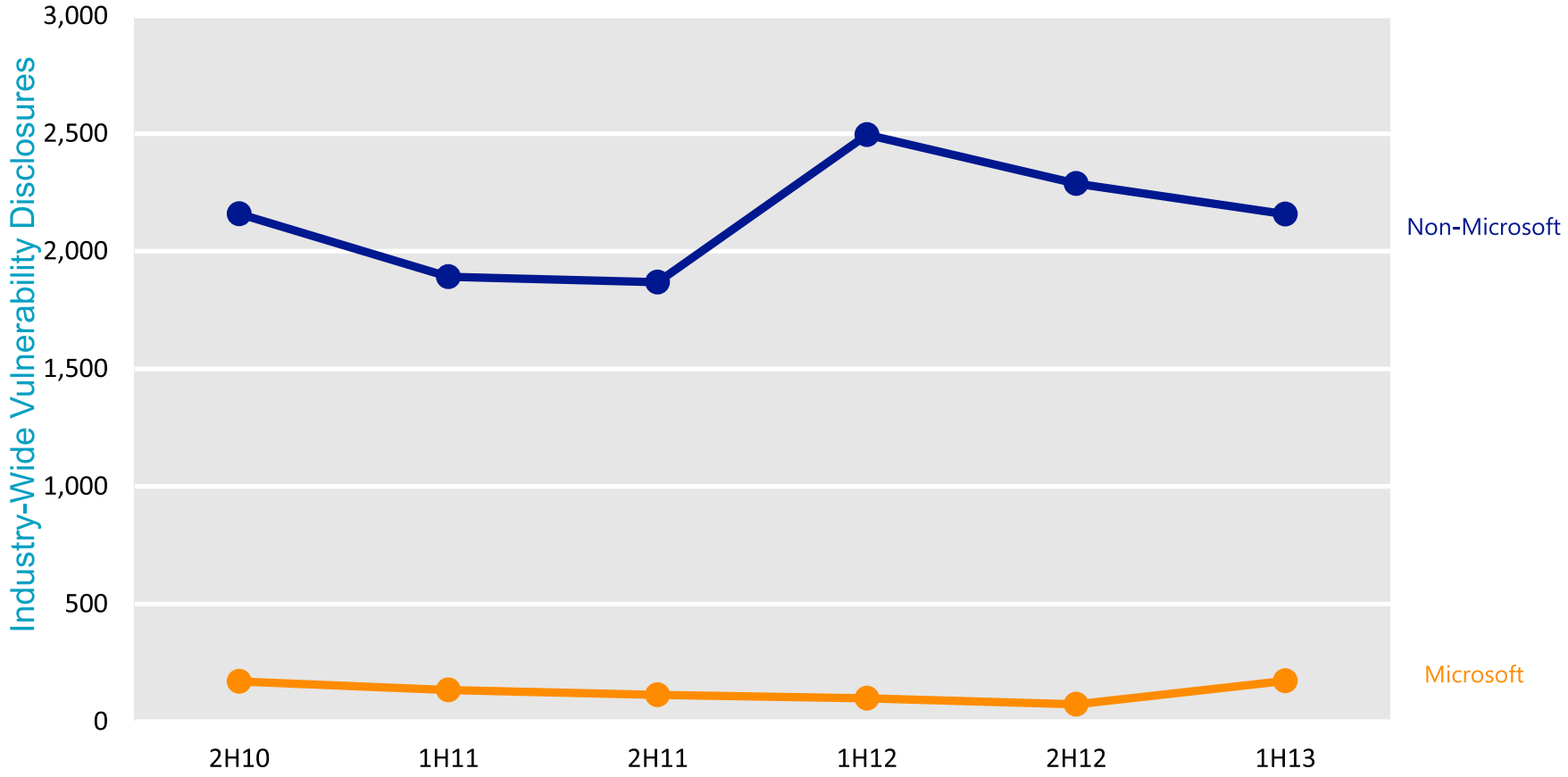
High-severity vulnerability disclosures increased 12.9 percent industrywide in 1H13. High-severity vulnerabilities accounted for 36.7 percent of total disclosures in 1H13, compared to 31.6 percent in the previous period.

Industry-Wide OS, Browser, App Vulns



Application vulnerability disclosures decreased 12.9 percent in 1H13. Operating system vulnerability disclosures increased 39.3 percent in 1H13.

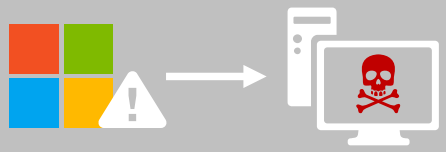
Industry-Wide Vulnerability Disclosures



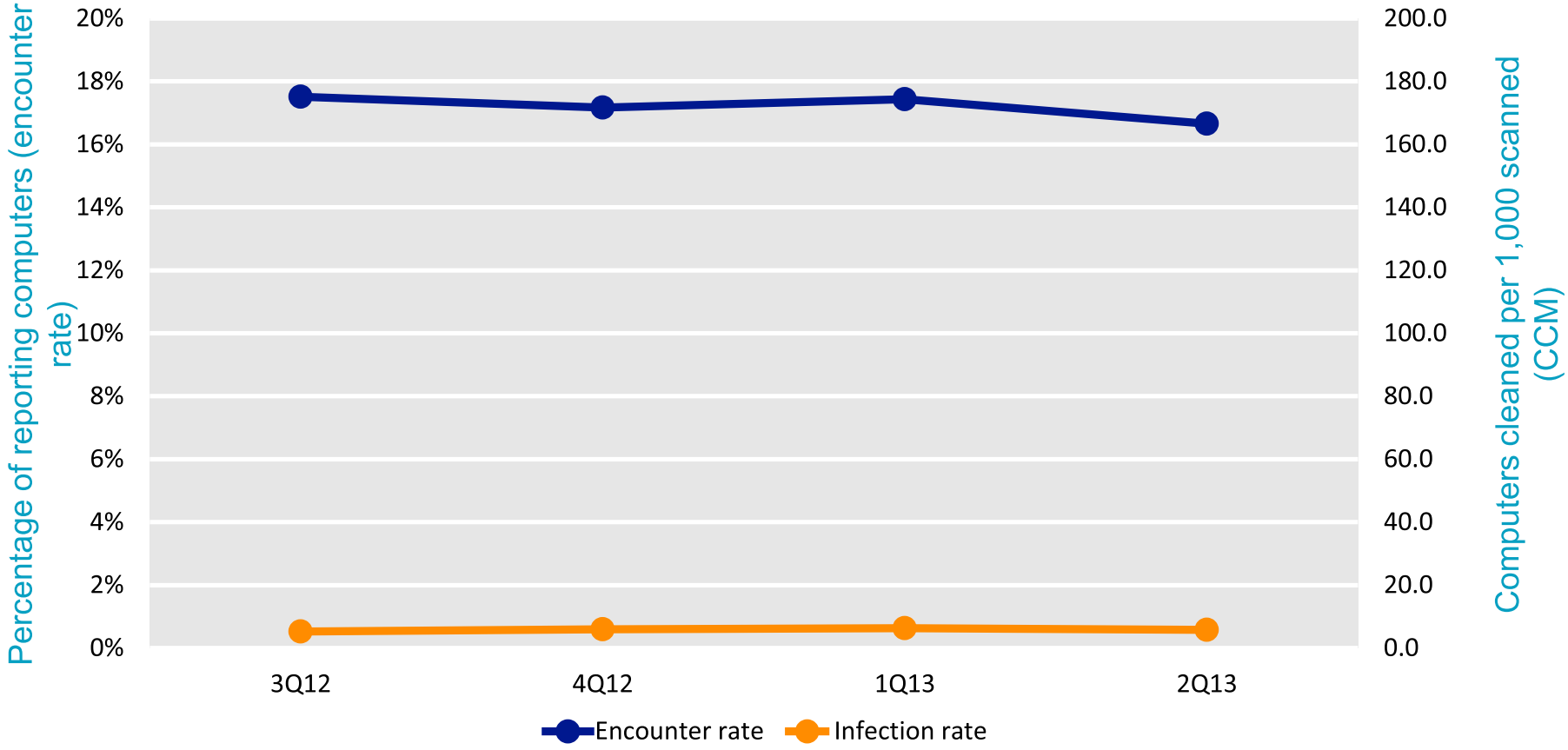
After several periods of decline, disclosures of vulnerabilities in Microsoft products increased to 7.4 percent of all disclosures across the industry, up from 3.1 percent in 2H12.

Encounter rate

Encounter Rate (ER)

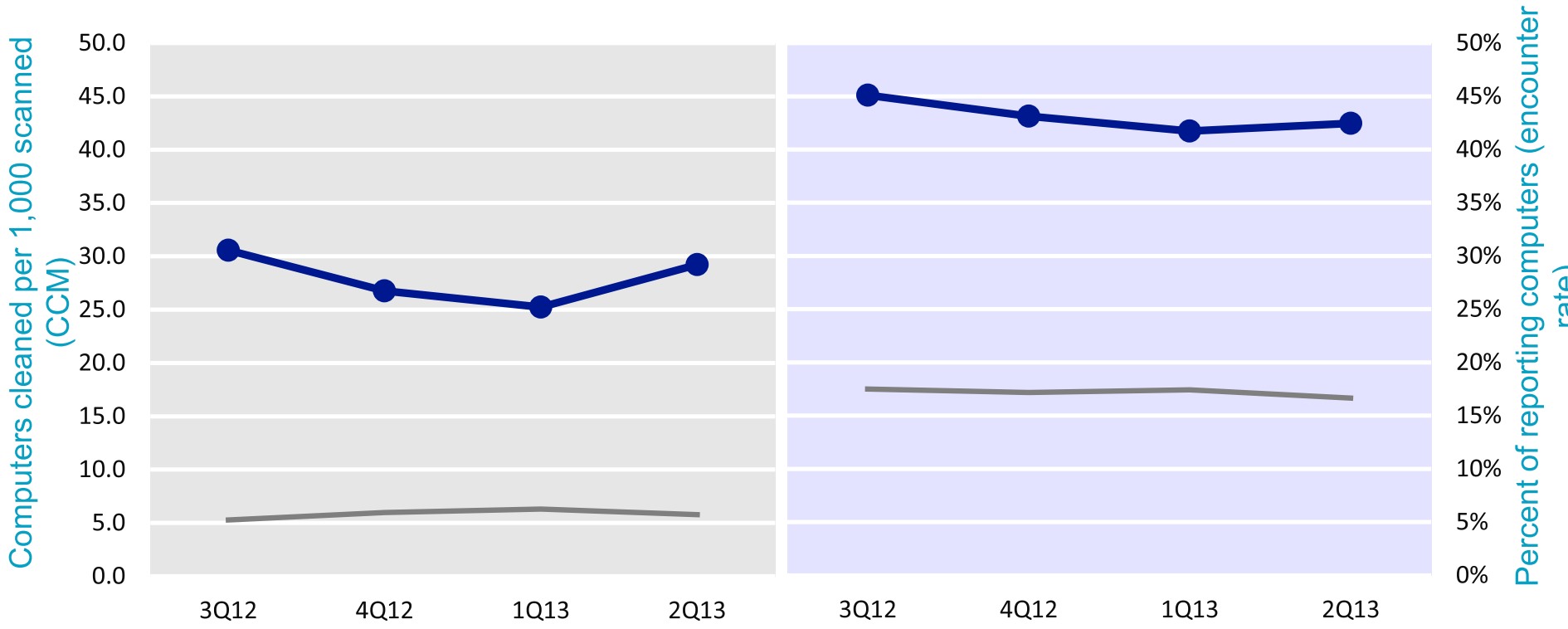
	A measure of malware prevalence
	Percent of computers encountering malware
	Microsoft antimalware products detect malware or malicious activity
	Includes blocks and infections

Worldwide Encounter and Infection Rates



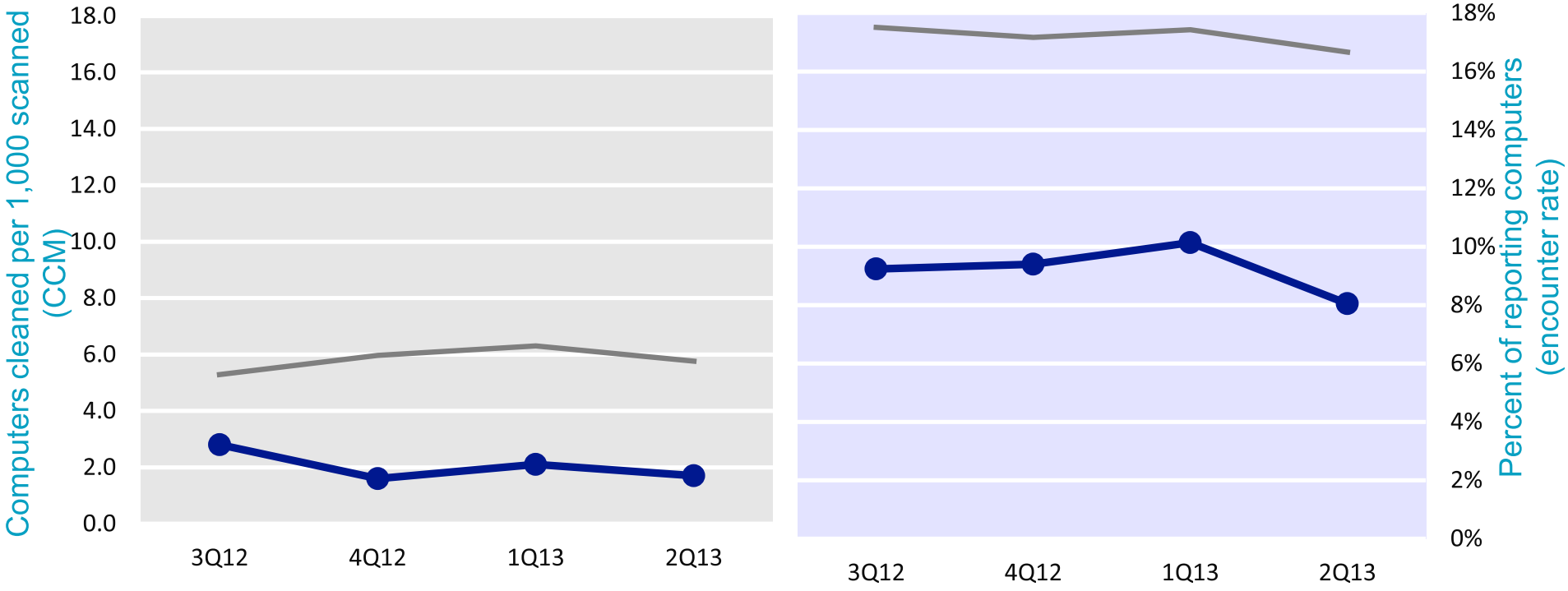
On average, about 17.0 percent of computers worldwide encountered malware each quarter in 1H12, as reported by Microsoft security products. The MSRT detected and removed specific highly prevalent or serious malware from about 6.0 out of every 1,000 computers (0.6 percent).

Infection and Encounter Rates: Pakistan



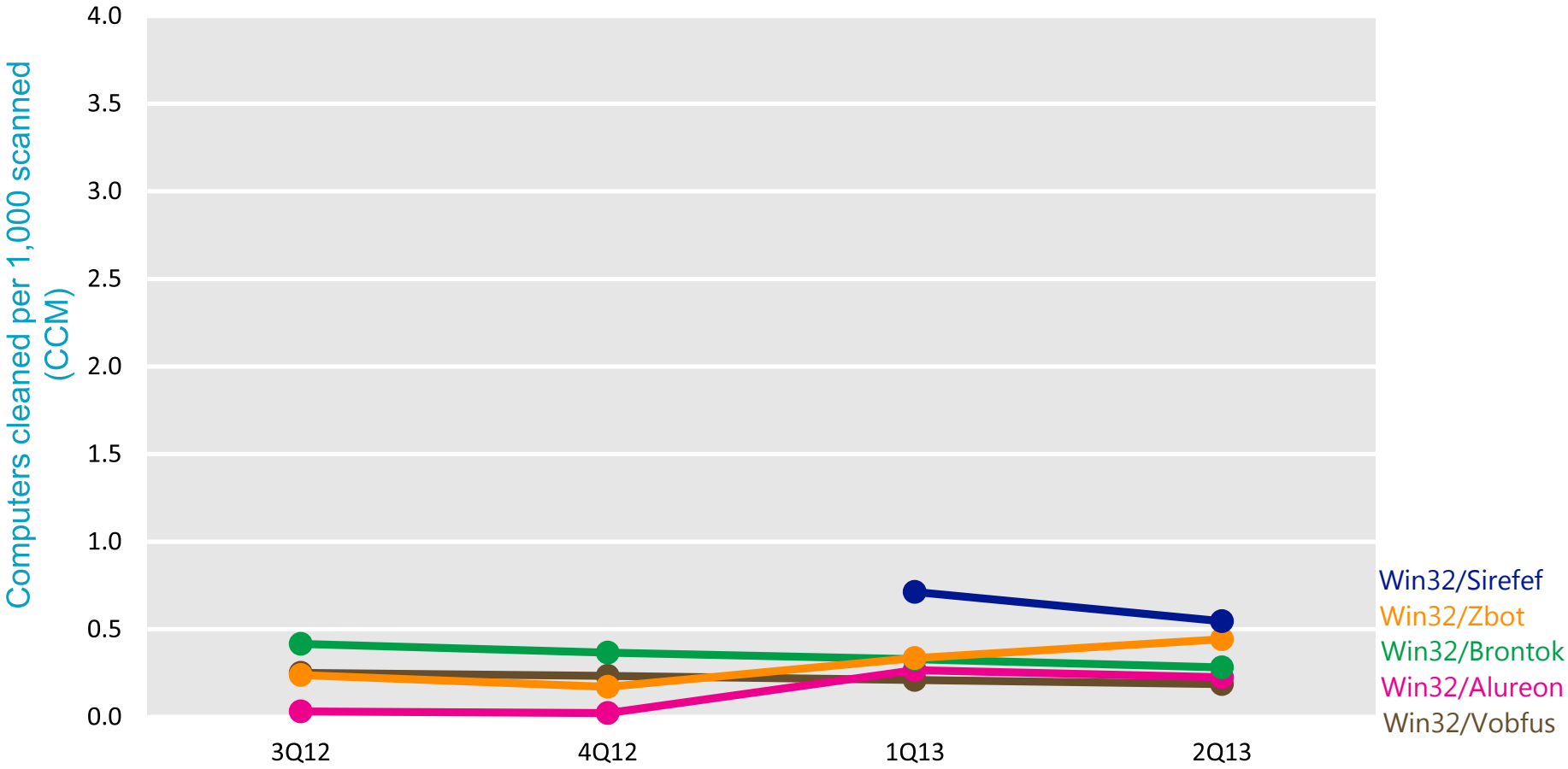
The infection rate scale on the left is magnified by a factor of 10 compared to the encounter rate scale on the right, to make the infection rate trends easier to see.

Infection and Encounter Rates: Denmark

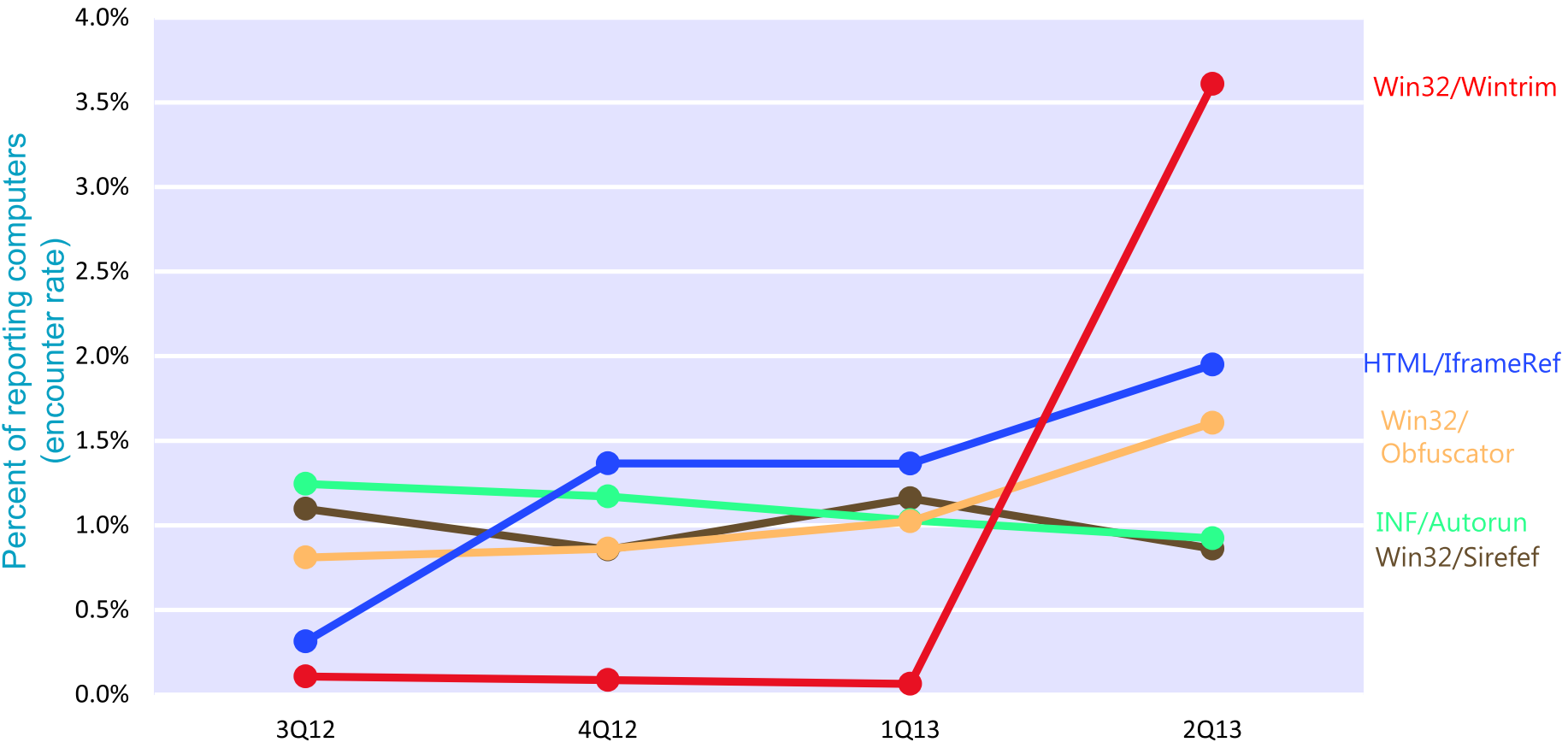


The infection rate scale on the left is magnified by a factor of 10 compared to the encounter rate scale on the right, to make the infection rate trends easier to see.

Threat Family by CCM: France



Threat Family by ER: France

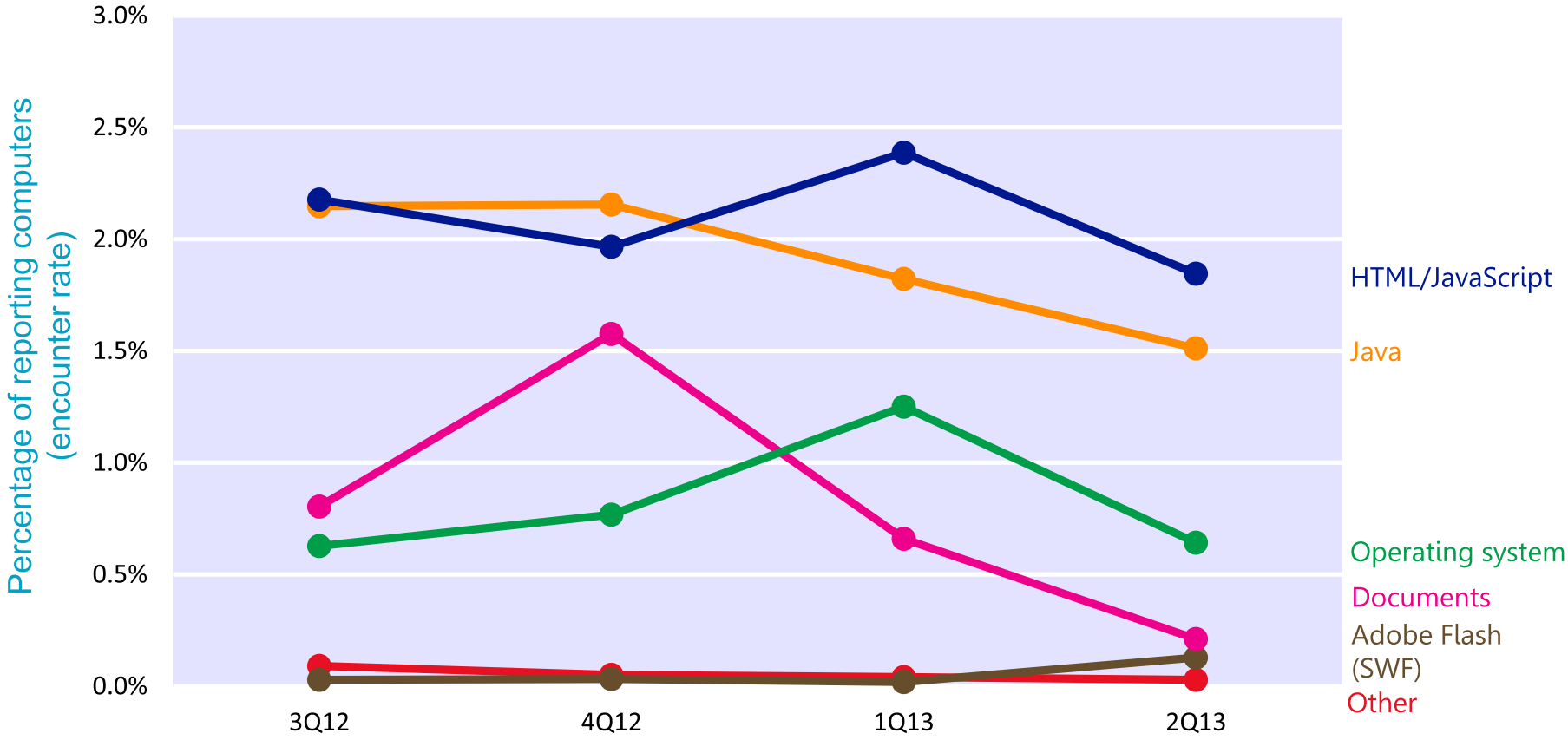


Exploit Trends

#RSAC

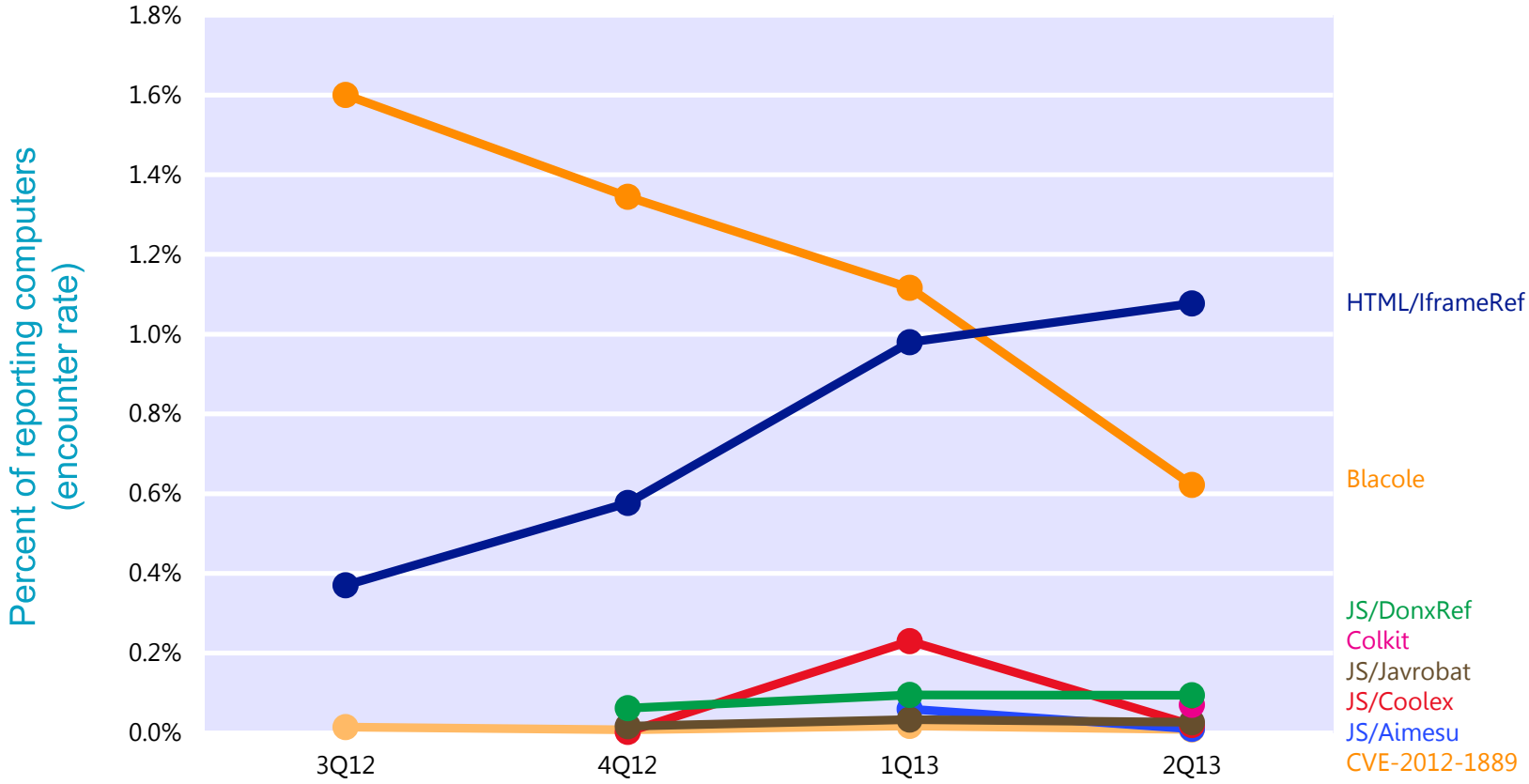
RSA CONFERENCE EUROPE 2013

Exploit Trends



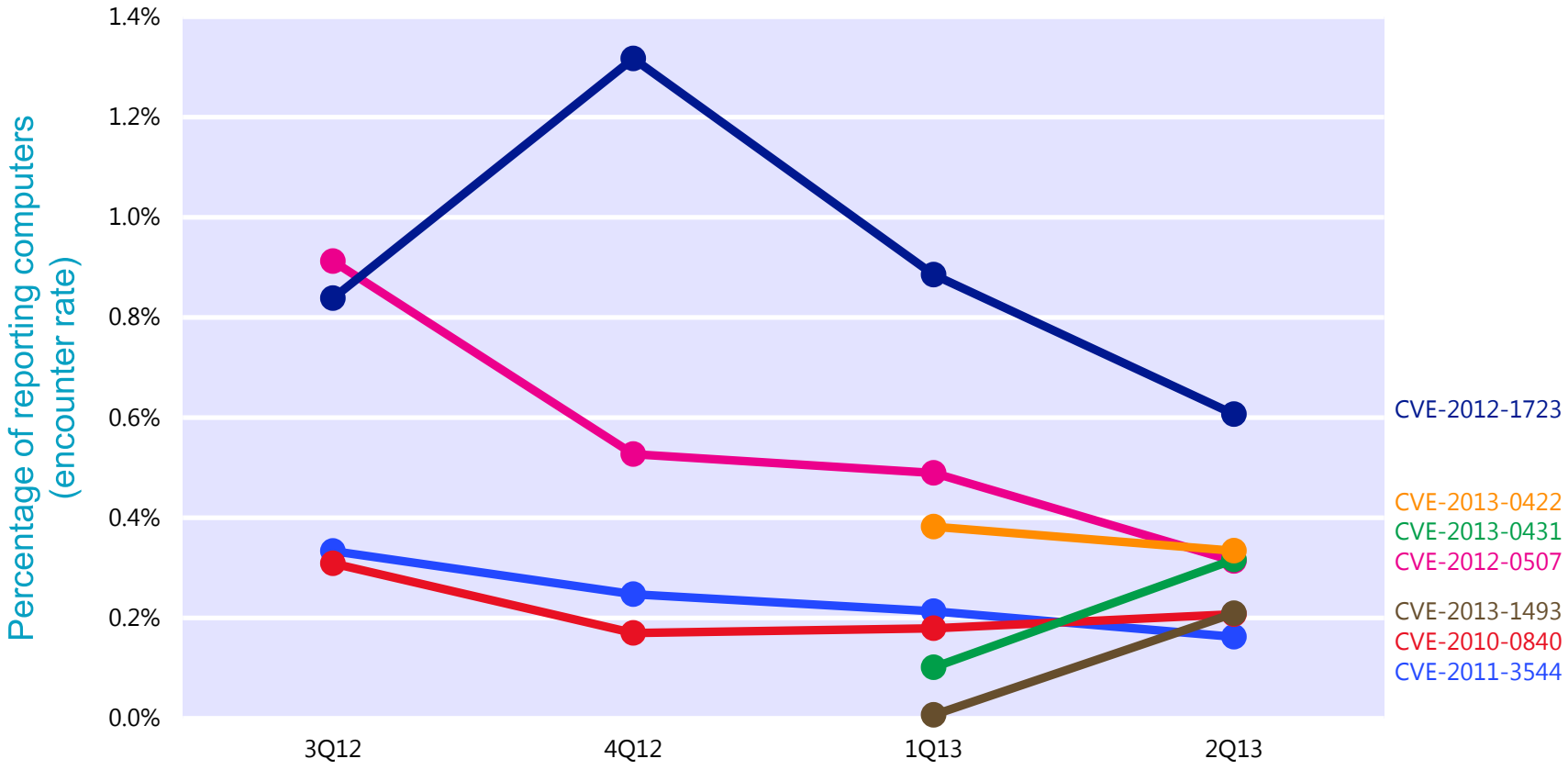
Web-based (HTML/JavaScript) threats continued to be the most commonly encountered type of exploit encountered in 2Q13, followed by Java exploits and operating system exploits.

HTML and JavaScript Exploits



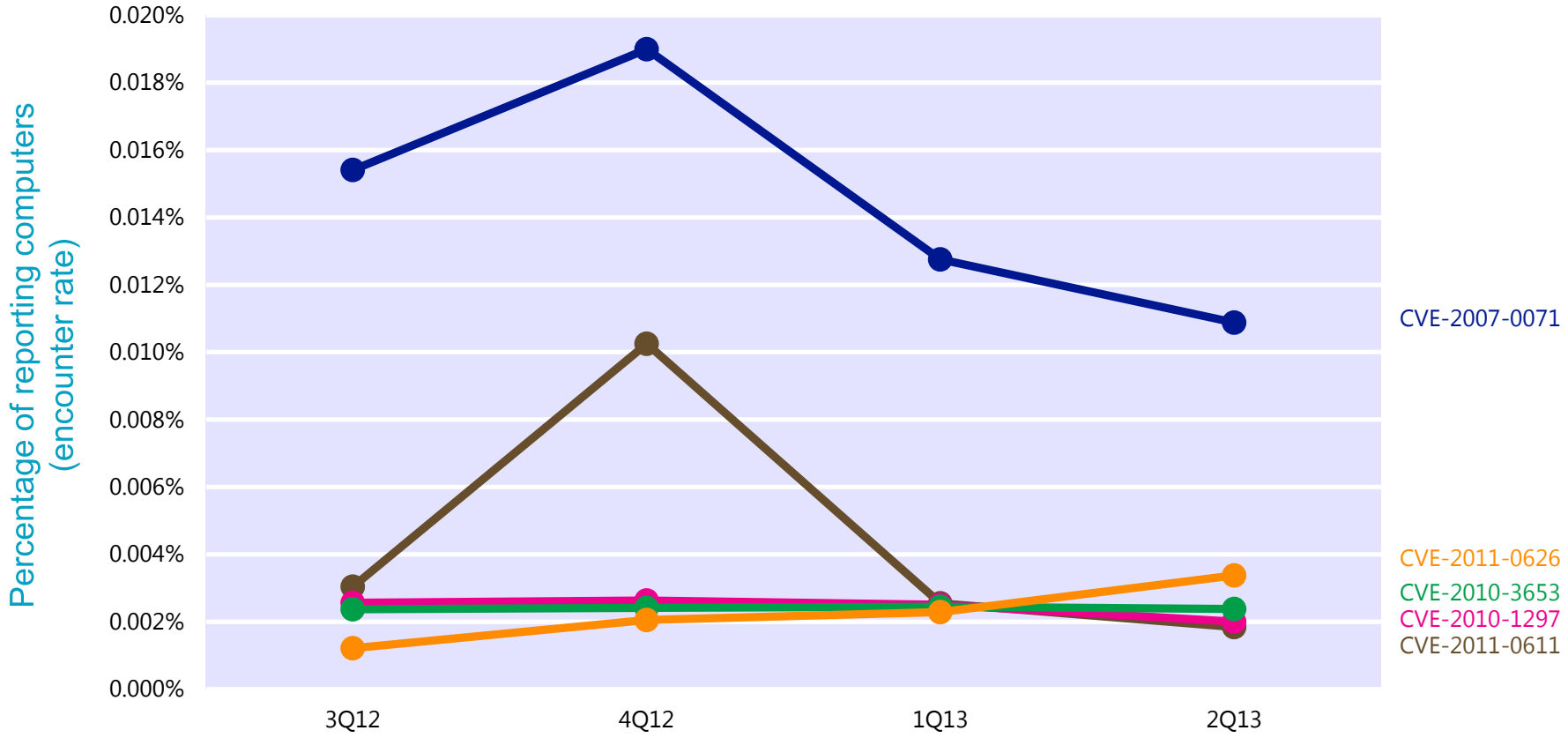
JS/Coolex is Microsoft's detection name for the so-called Cool exploit kit, which first appeared in October 2012 and is often used in ransomware schemes

Java Exploits



Several new Java exploits (notably CVE-2013-0431 and CVE-2013-1493) were first detected in 1Q13 and quickly rose in prominence during the next quarter as they began to be included in various exploit kits.

Adobe Flash Player Exploits



Attempts to exploit CVE-2007-0071 decreased significantly in 1H13, but remained the most commonly encountered exploit in both quarters.

Top Exploit Families

Exploit Family	Platform or Technology	3Q12	4Q12	1Q13	2Q13
HTML/IframeRef*	HTML/JavaScript	0.37%	0.58%	0.98%	1.08%
Blacole	HTML/JavaScript	1.60%	1.34%	1.12%	0.62%
CVE-2012-1723	Java	0.84%	1.32%	0.89%	0.61%
CVE-2010-2568 (MS10-046)	Operating system	0.51%	0.57%	0.57%	0.53%
CVE-2012-0507	Java	0.91%	0.53%	0.49%	0.31%
CVE-2013-0422	Java	—	—	0.38%	0.33%
CVE-2011-3402 (MS12-034)	Operating system	—	0.11%	0.62%	0.04%
Pdfjsc	Document	0.77%	1.56%	0.53%	0.12%
CVE-2013-0431	Java	—	—	0.10%	0.32%
CVE-2010-0840	Java	0.31%	0.17%	0.18%	0.21%

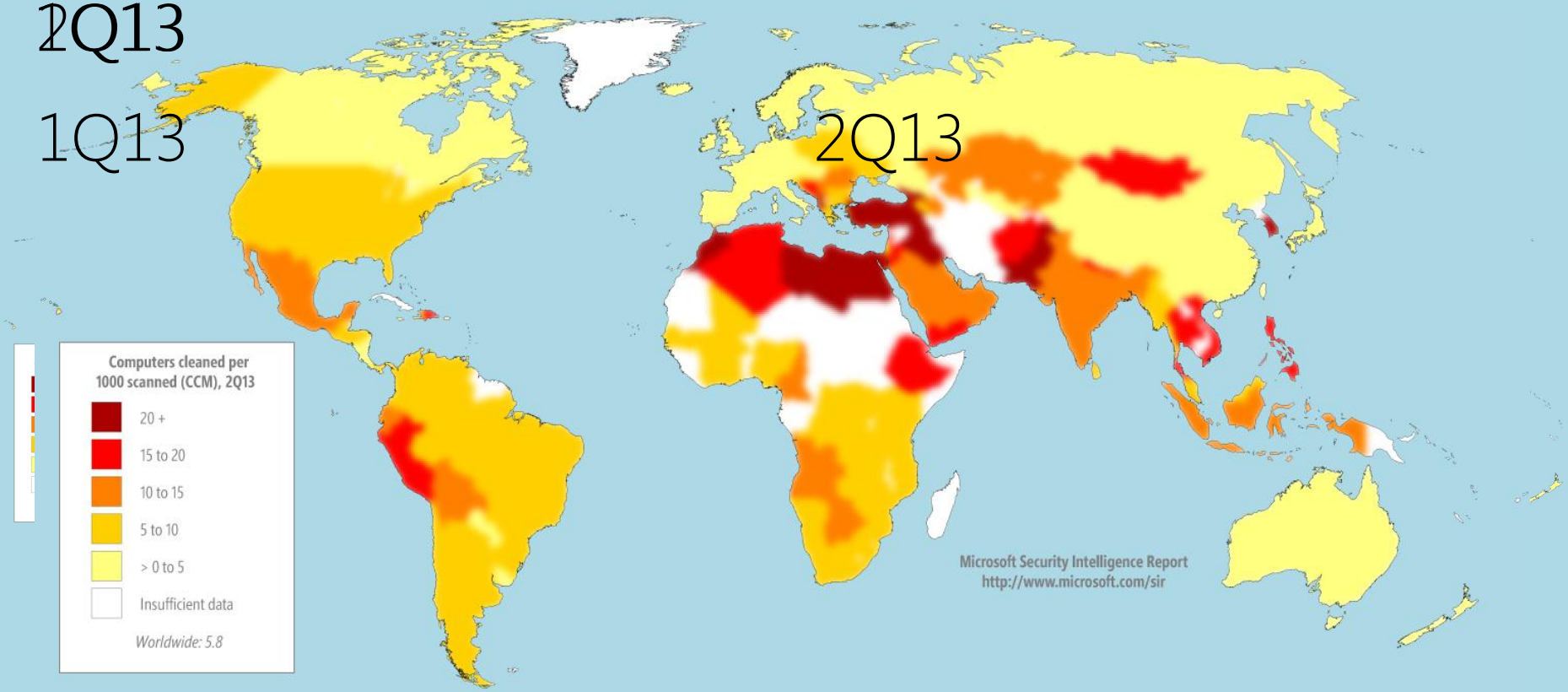
- *Totals include only IframeRef variants categorized as exploits.
- Totals do not include exploits that were detected as part of exploit kits.

Malware

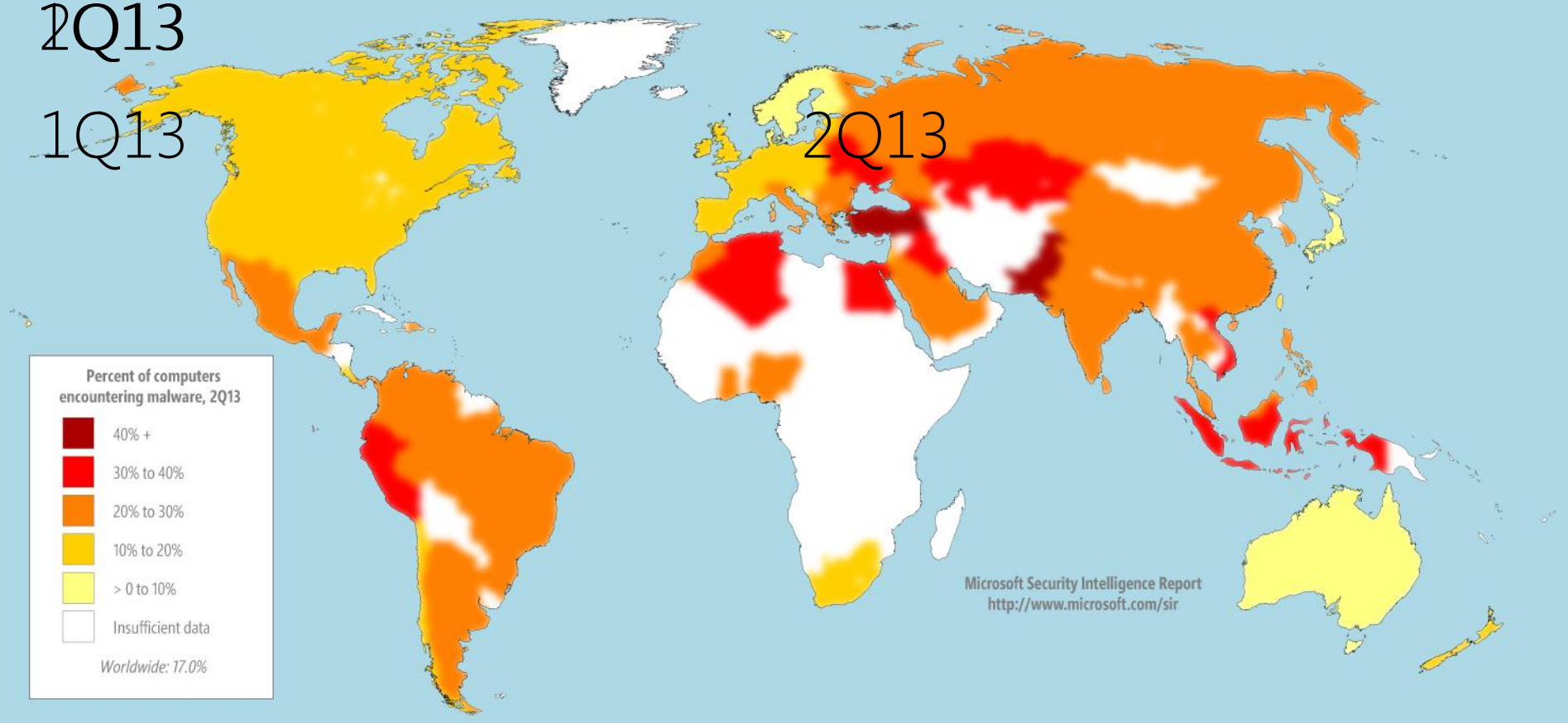
#RSAC

RSA CONFERENCE EUROPE 2013

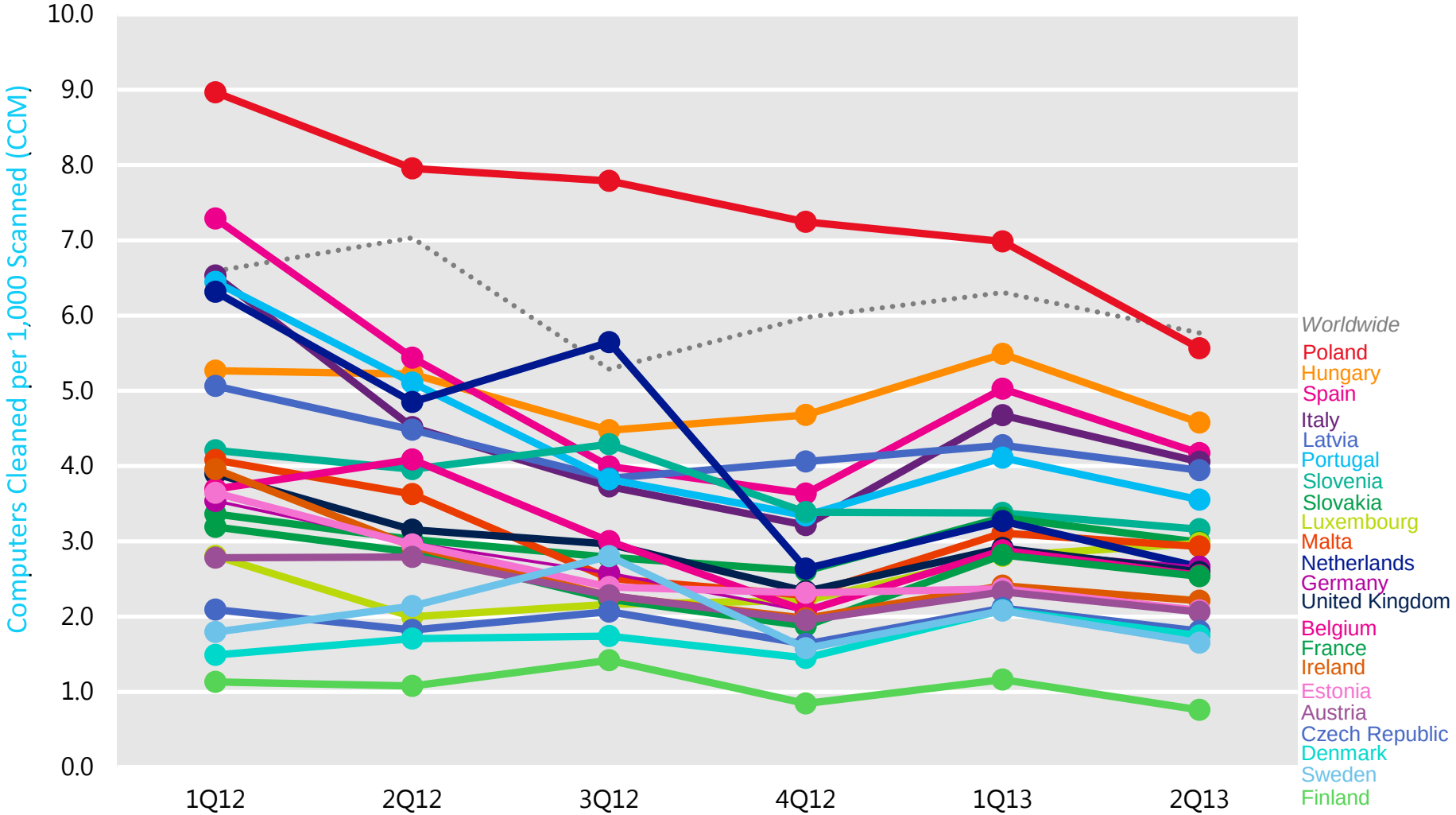
CCM by Country or Region



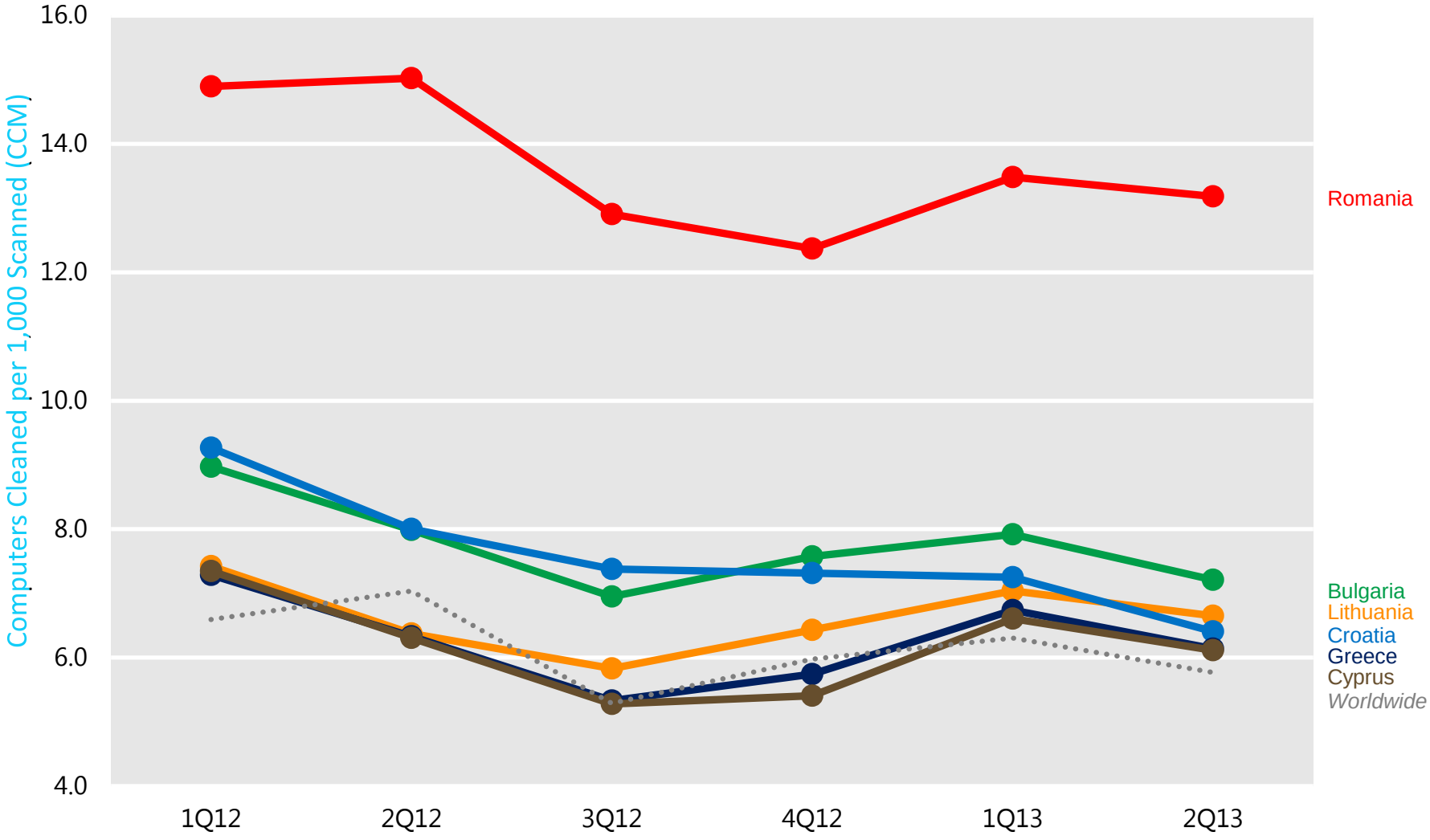
ER by Country or Region



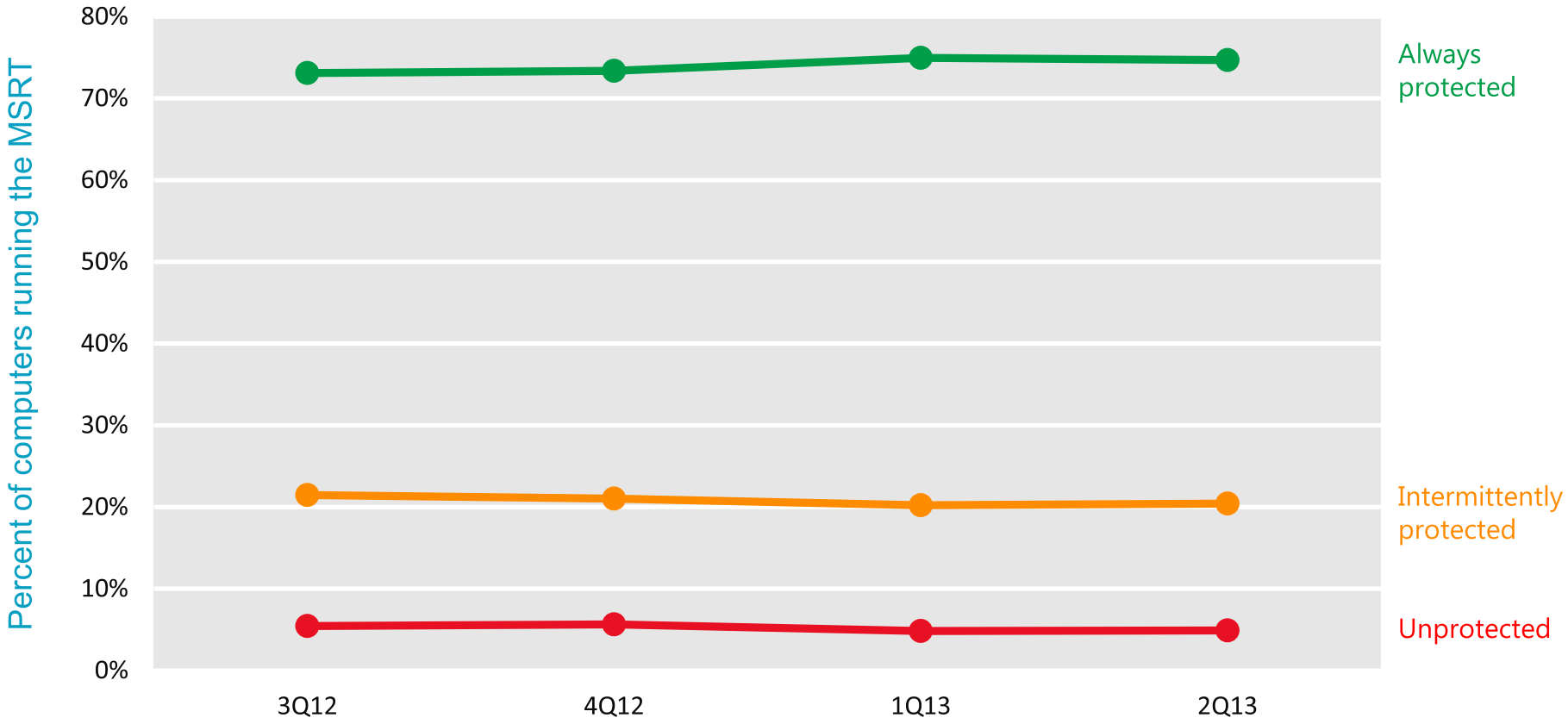
EU Infection Rate Trends



EU Infection Rate Trends

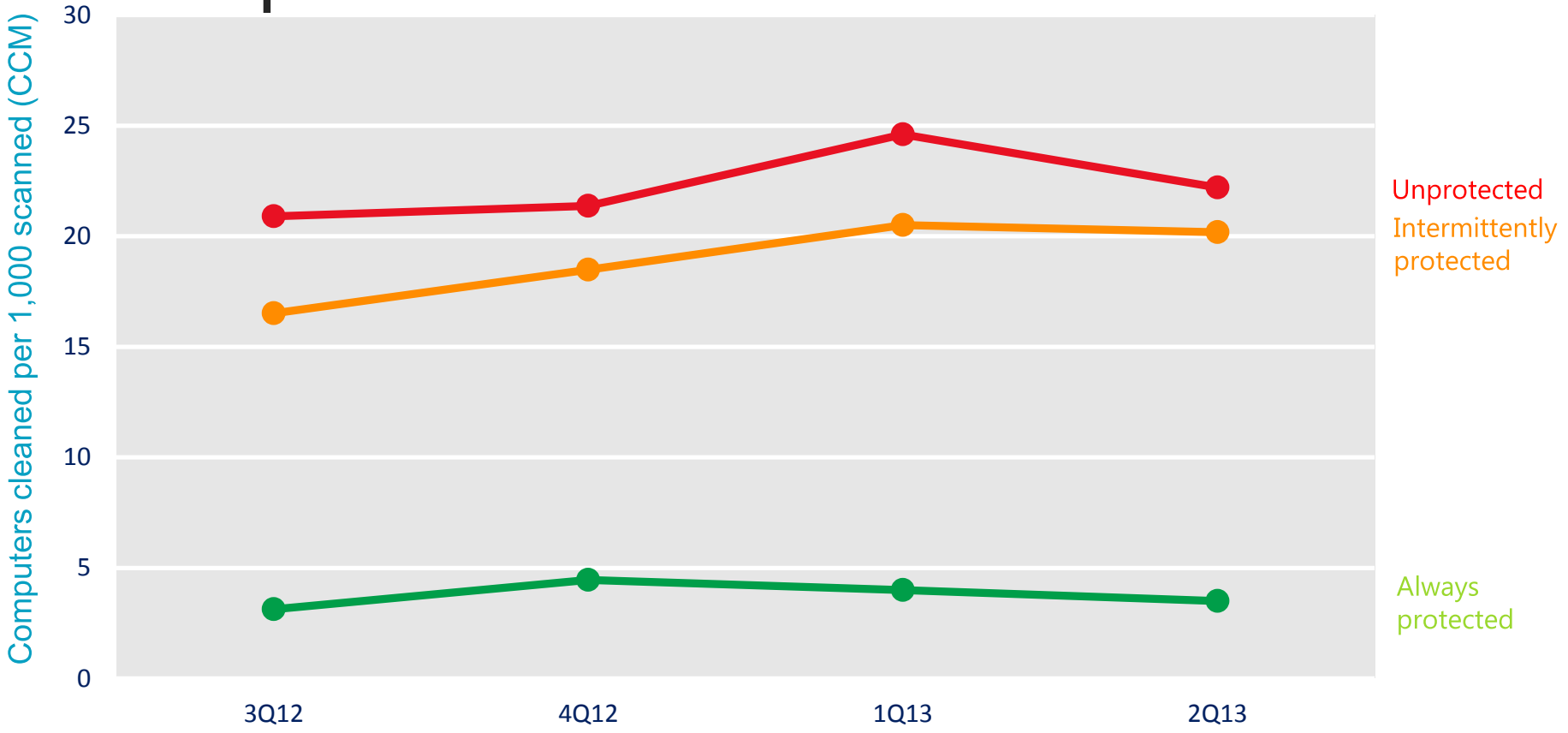


Security Software Usage



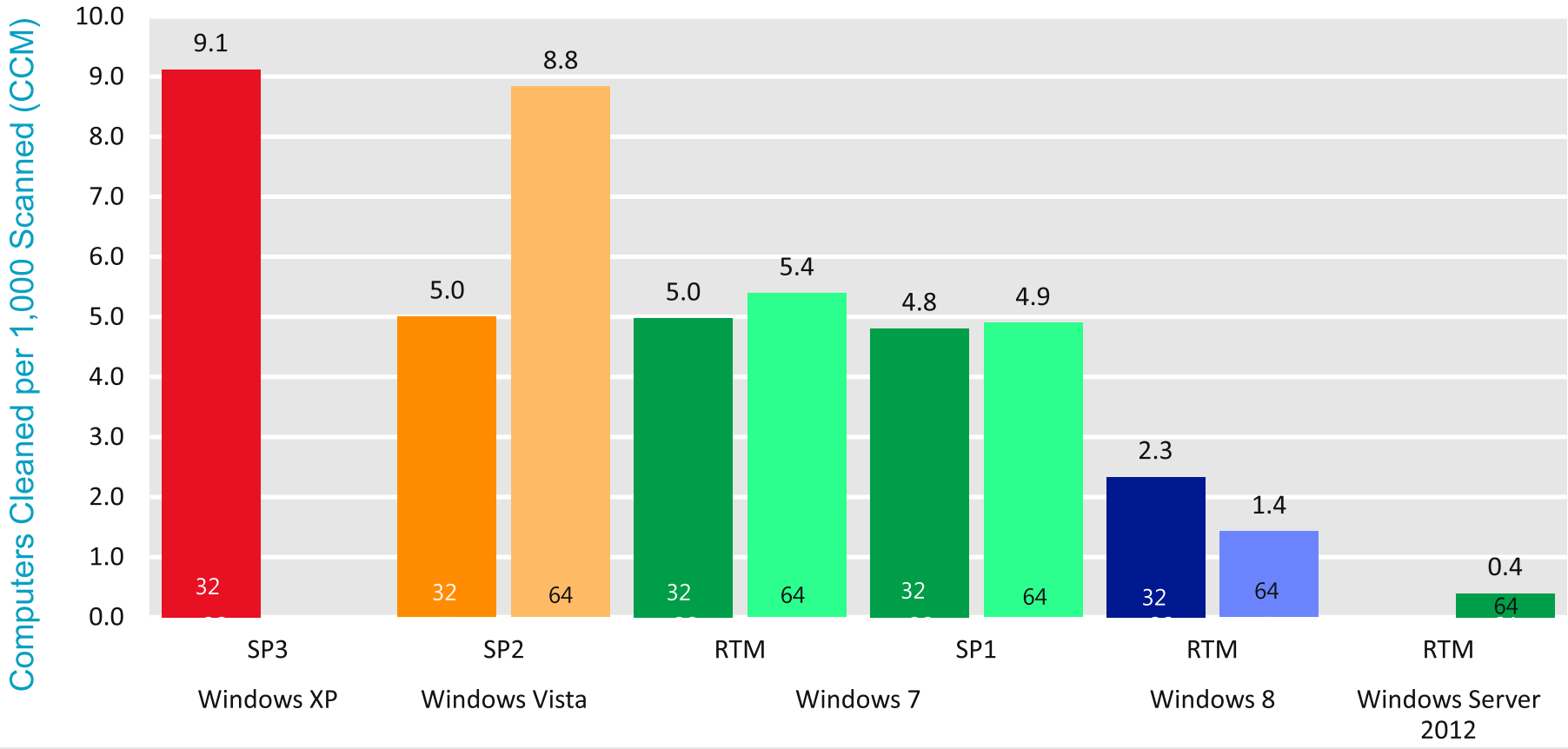
Three-quarters of computers worldwide were found to be running real-time security software during every monthly MSRT execution in each of the past four quarters.

CCM for Protected and Unprotected Computers



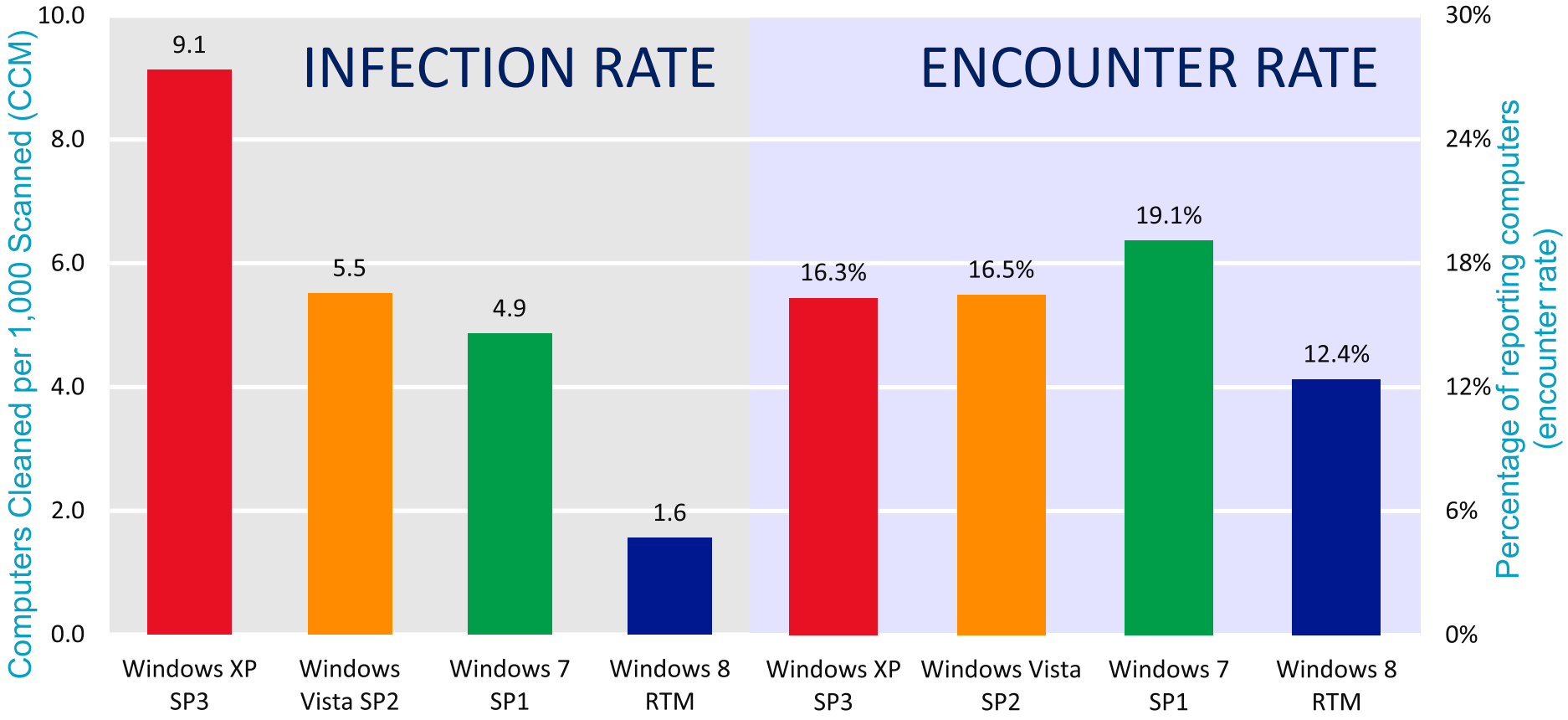
On average, the MSRT reported that computers that were never found to be running real-time security software during a quarter were 7.1 times as likely to be infected with malware as computers that were always found to be protected.

CCM by OS and Service Pack, 2Q13



- Normalized numbers
- Infection rates for more recently released operating systems and service packs are consistently lower than earlier ones.

Infection and Encounter Rates: OS, 2Q13



- The infection rate for Windows XP is significantly higher than the infection rates for both newer versions of Windows. The encounter rate differences between operating systems are significantly smaller.

Threat Category Prevalence

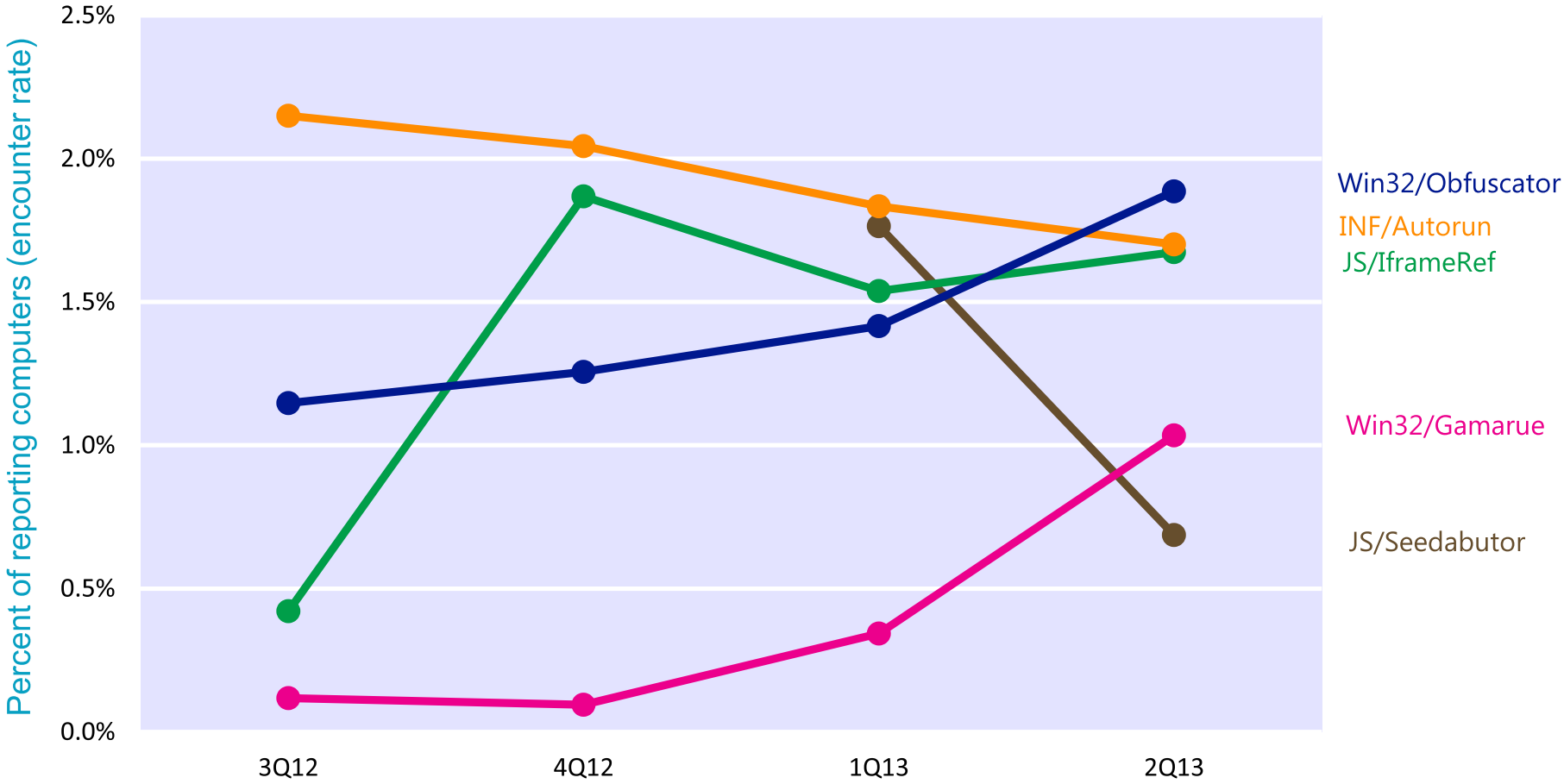
Category	Worldwide	United States	Brazil	Russia	Turkey	India	Mexico	Germany	France	China	United Kingdom
Misc. Trojans	10.3%	8.0%	15.1%	23.6%	30.2%	15.8%	14.6%	6.9%	8.9%	16.3%	8.0%
Worms	4.7%	0.7%	8.4%	5.7%	21.4%	18.0%	17.7%	1.2%	2.1%	5.8%	0.9%
Exploits	3.9%	4.0%	3.1%	3.9%	7.7%	5.4%	3.7%	4.6%	3.6%	2.7%	4.1%
Trojan downloaders and droppers	2.7%	1.8%	8.2%	3.9%	10.7%	2.1%	5.6%	0.9%	5.1%	3.6%	1.6%
Viruses	2.1%	0.3%	3.3%	2.2%	8.8%	8.8%	3.5%	0.5%	0.8%	6.2%	0.5%
Password stealers and monitoring tools	1.3%	0.8%	3.2%	2.5%	2.5%	2.8%	1.7%	1.2%	1.3%	1.1%	1.0%
Backdoors	1.2%	0.6%	1.7%	1.2%	2.8%	2.4%	2.4%	0.5%	0.9%	3.1%	0.8%

Totals for each location may exceed 100% because some computers reported threats from more than one category.

Top 10 Threat Families

	Family	Category	3Q12	4Q12	1Q13	2Q13
1	INF/Autorun	Misc. Trojans	2.15%	2.04%	1.83%	1.70%
2	Win32/Obfuscator	Misc. Trojans	1.15%	1.26%	1.42%	1.89%
3	HTML/IframeRef	Exploits	0.42%	1.87%	1.54%	1.67%
4	JS/Seedabutor	Misc. Trojans	—	—	1.76%	0.69%
5	Win32/Dorkbot	Worms	0.95%	1.01%	0.82%	0.95%
6	Win32/Sirefef	Misc. Trojans	1.03%	0.74%	0.88%	0.71%
7	Win32/Sality	Viruses	0.80%	0.81%	0.78%	0.73%
8	Win32/Conficker	Worms	0.86%	0.82%	0.72%	0.68%
9	Win32/Gamarue	Worms	0.12%	0.09%	0.34%	1.03%
10	JS/BlacoleRef	Misc. Trojans	0.87%	0.57%	0.45%	0.74%

Trends for Notable Threat Families



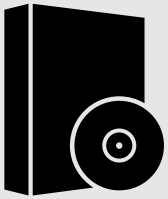
Most Commonly Encountered

Rank 2Q13	Family	Most significant category	Rank (Windows 8 RTM)	Rank (Windows 7 SP1)	Rank (Windows Vista SP2)	Rank (Windows XP SP1)
1	Win32/Obfuscator	Misc. Trojans	1	1	4	6
2	INF/Autorun	Misc. Trojans	2	3	13	1
3	HTML/IframeRef	Exploits	3	2	1	2
4	Win32/Gamarue	Worms	4	4	24	7
5	Win32/Dorkbot	Worms	8	5	25	8
6	JS/BlacoleRef	Misc. Trojans	15	6	6	9
7	Win32/Sality	Viruses	6	12	52	5
8	Win32/Sirefef	Misc. Trojans	20	7	2	12
9	JS/Seedabutor	Misc. Trojans	5	13	26	3
10	Win32/Conficker	Worms	13	10	28	4
13	Java/CVE-2012-1723	Exploits	43	9	3	20

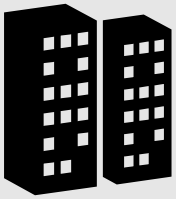
Applying It

Applying It

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

Thank you!

Tim Rains

Microsoft Corporation

Jeff Jones

Microsoft Corporation

#RSAC

RSA CONFERENCE EUROPE 2013