

Microsoft Security Intelligence Report Volume 13

Tim Rains

Director, Trustworthy Computing, Microsoft

Jeff Jones

Director, Trustworthy Computing, Microsoft

Session ID: DSP-R33

Session Classification: Intermediate

Security in
knowledge



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
- Security intelligence, MSRC, MMPC, MSEC, Cybersecurity, Cloud Security
- Reformed Engineer: Windows, IT
- [Microsoft Security Blog](#) & [Trustworthy Computing Blog](#)
- @MSFTSecurity

A graphic for the Microsoft Security Intelligence Report (SIR). It features a central cluster of icons representing various devices and people, with a downward arrow pointing to a document icon. The text reads: "Malware Data From Over 600 Million Systems Worldwide", "ONE SECURITY REPORT", and "The Security Intelligence Report (SIR) is an analysis of the current threat landscape based on data from internet service providers and over 600 million systems worldwide to help you protect your organization, software, and people." At the bottom, it says "View the Security Intelligence Report at www.microsoft.com/SIR" and "Microsoft | Security Intelligence Report".

Malware Data From Over 600 Million Systems Worldwide

ONE SECURITY REPORT

The Security Intelligence Report (SIR) is an analysis of the current threat landscape based on data from internet service providers and over 600 million 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

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

Featured Intelligence: Deceptive Downloads

Vulnerabilities & Exploits

Malware Trends

Applying it

Q&A

About SIRv13: Contents

“Deceptive downloads”

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
600 Million 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 600 million 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 SIRv13: Data Sources

Product name	Main customer segment		Malicious software		Spyware and potentially unwanted software		Available at no additional charge	Main distribution methods
	Consumer s	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 Safety scanner	•		•		•		•	Cloud
Microsoft Security Essentials	•		•	•	•	•	•	Cloud
Forefront Online Protection for Exchange		•	•	•				Cloud
Microsoft Forefront Client Security		•	•	•	•	•		Volume licensing

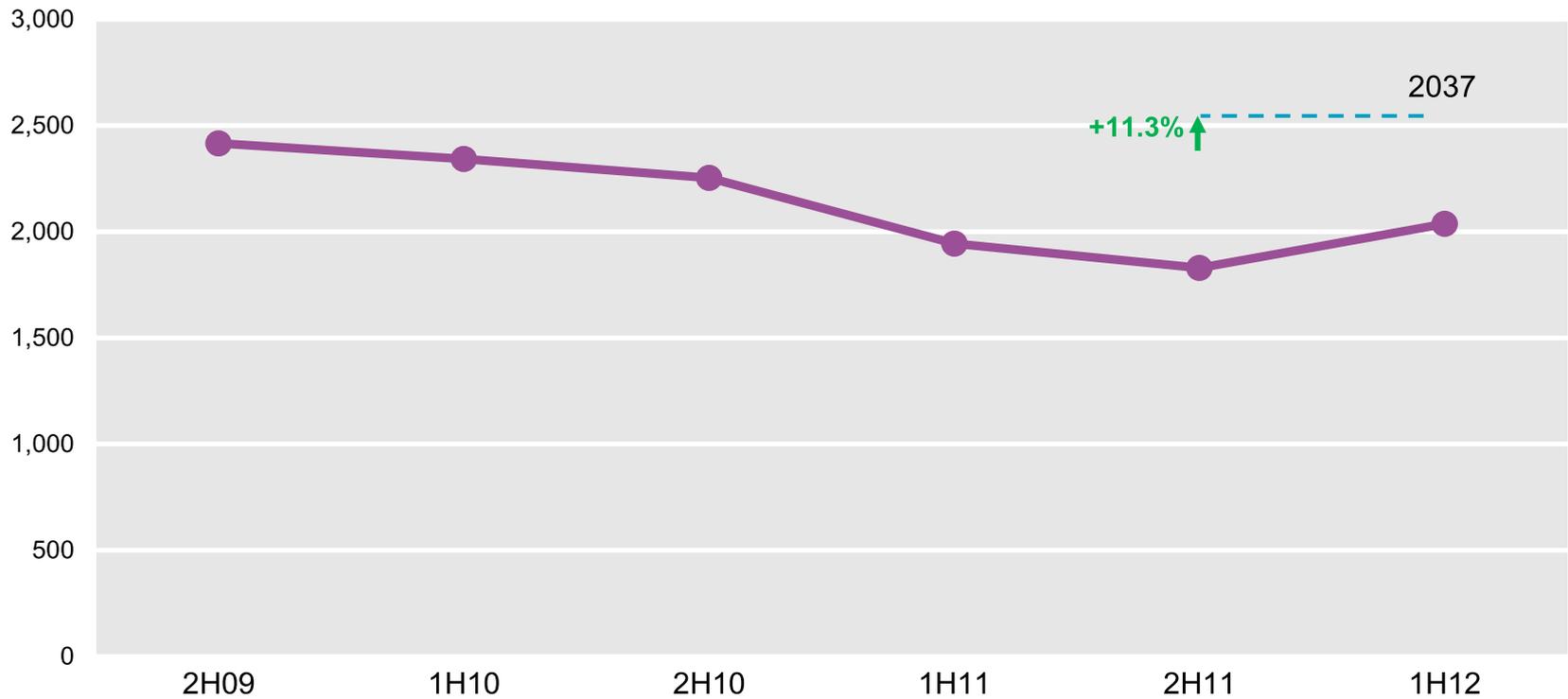
- **Hotmail** – more than 280 million active users
- **Internet Explorer** – the world’s most popular browser with SmartScreen, Microsoft Phishing Filter
- **Exchange Online Protection** – scans billions of e-mail messages a year
- **Windows Malicious Software Removal Tool** – has a user base of more than 600 million unique computers worldwide
- **Microsoft Security Essentials** – available in over 30 languages
- **Bing** – billions of Web-pages scanned each month

Vulnerability Trends



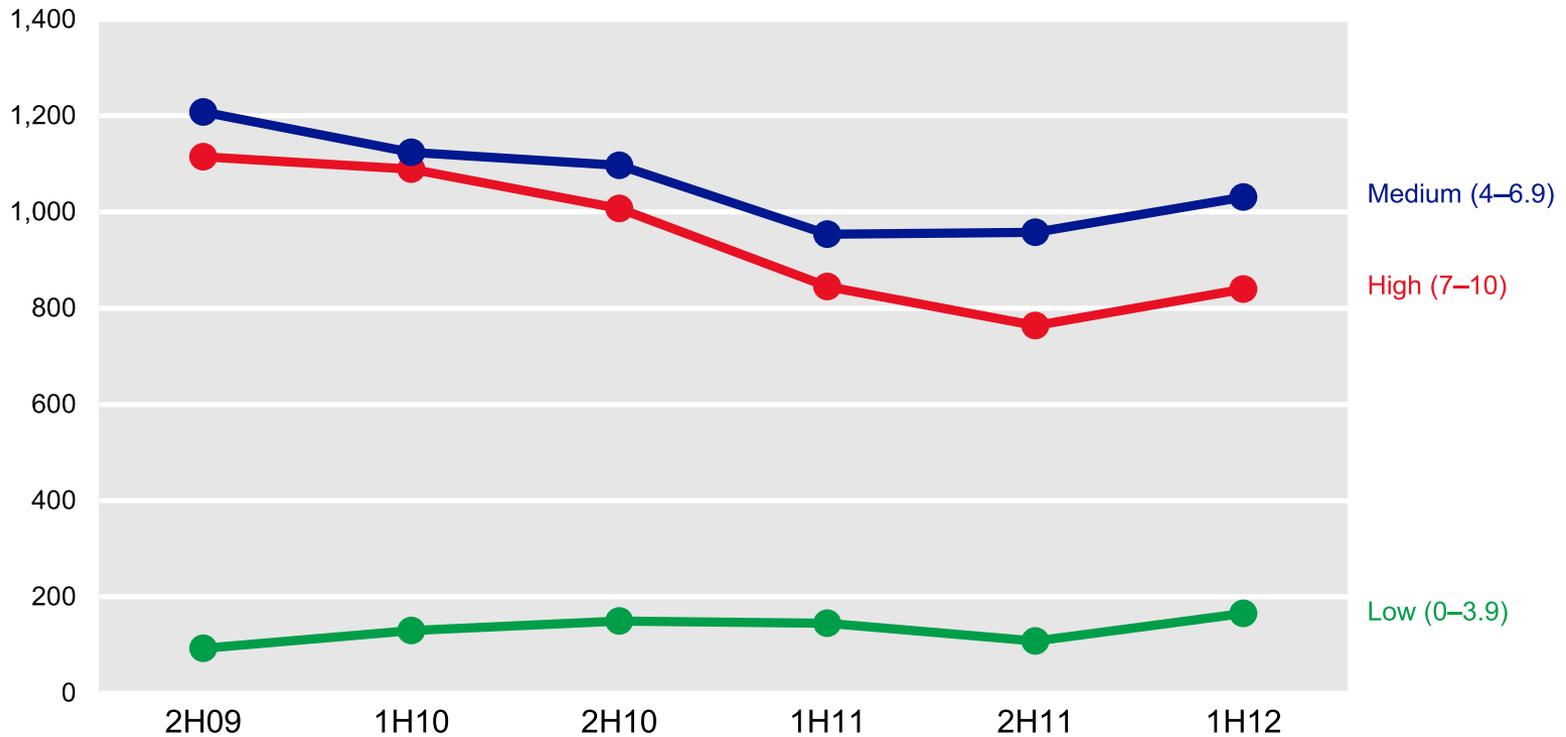
Industry-Wide Vulnerability Disclosures

Industry-Wide Vulnerability Disclosures



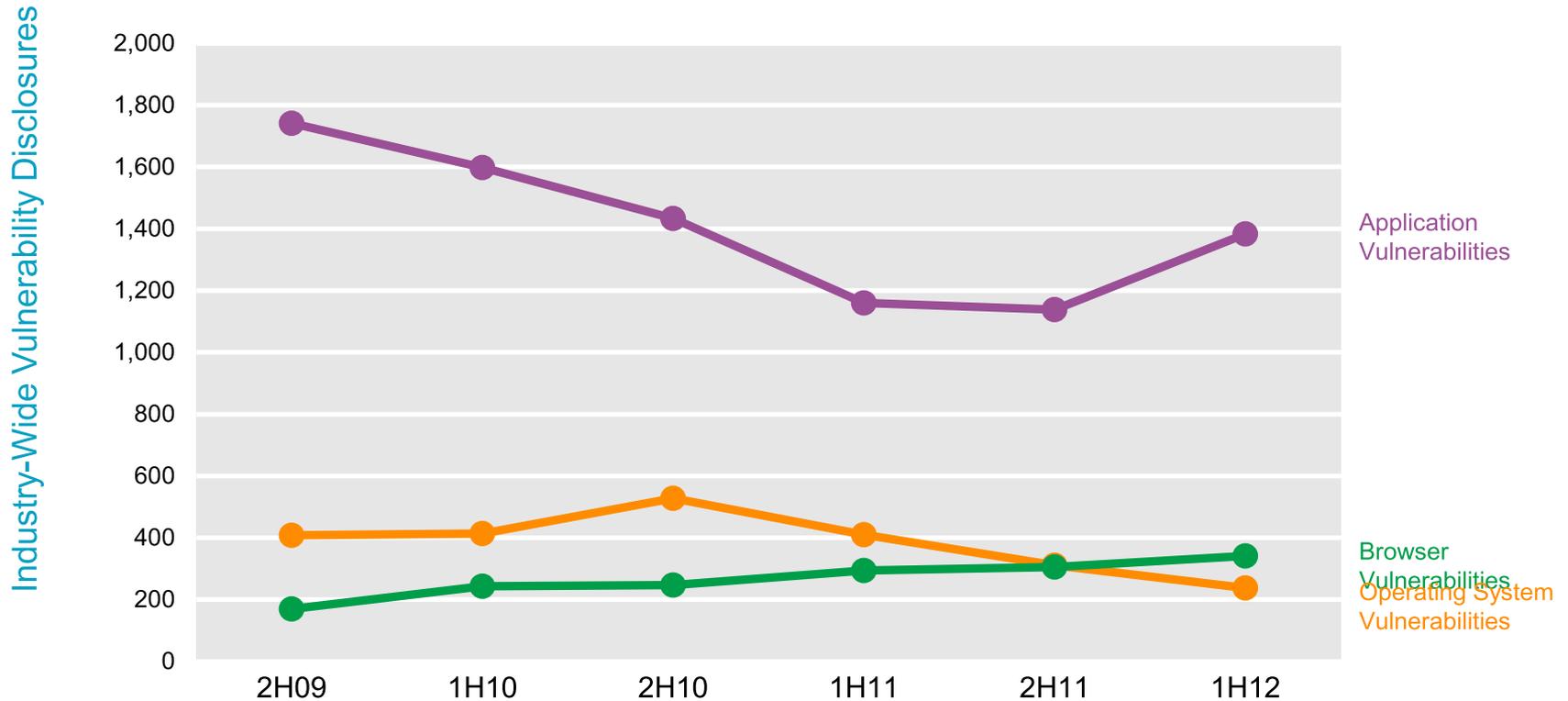
Industry-Wide Vulnerability Severity

Industry-Wide Vulnerability Disclosures



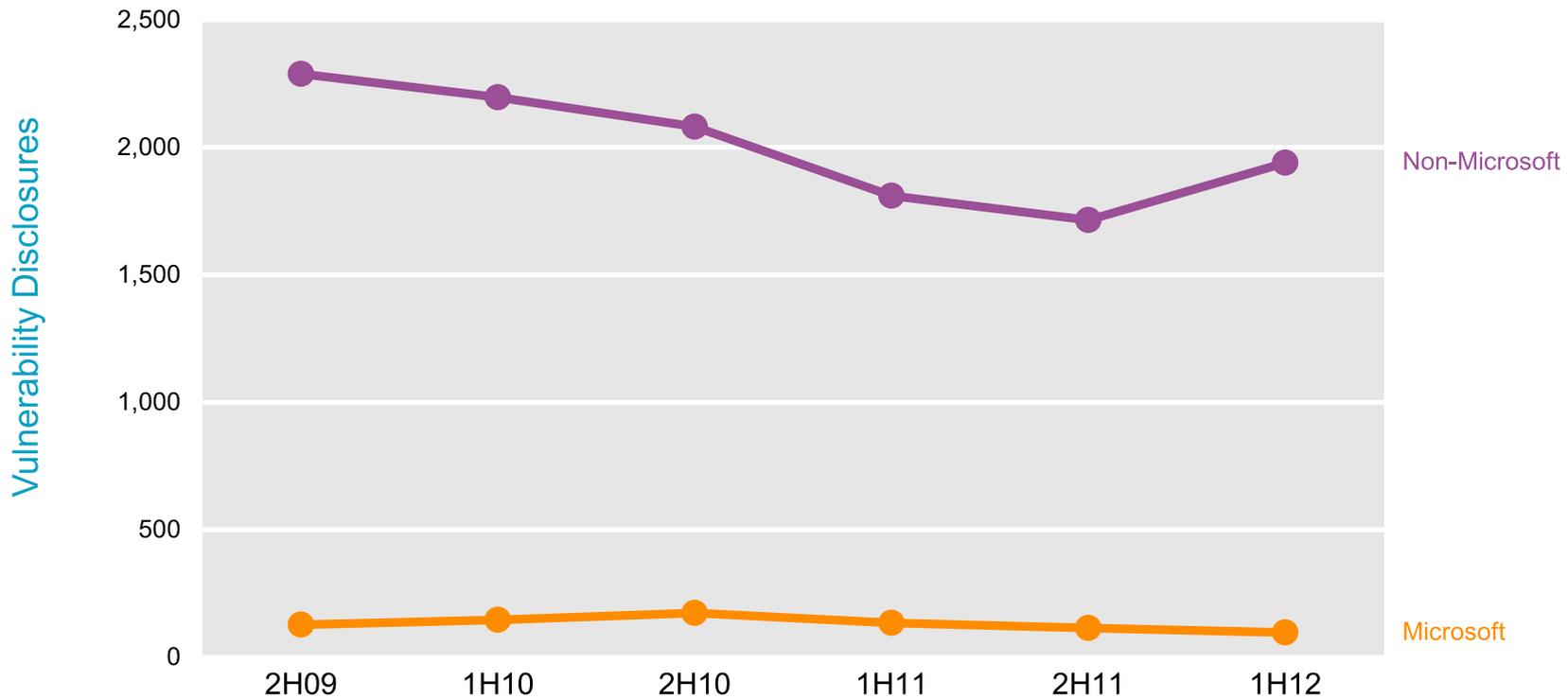
Vulnerability disclosures in each of the three CVSS severity classifications rose by a roughly similar amount.

Industry-Wide OS, Browser, App Vulns



- Application vulnerabilities accounted for 71.2% of all vulnerability disclosures
- Operating system vulnerabilities dropped to the lowest level since 2H03

Industry-Wide Vulnerability Disclosures

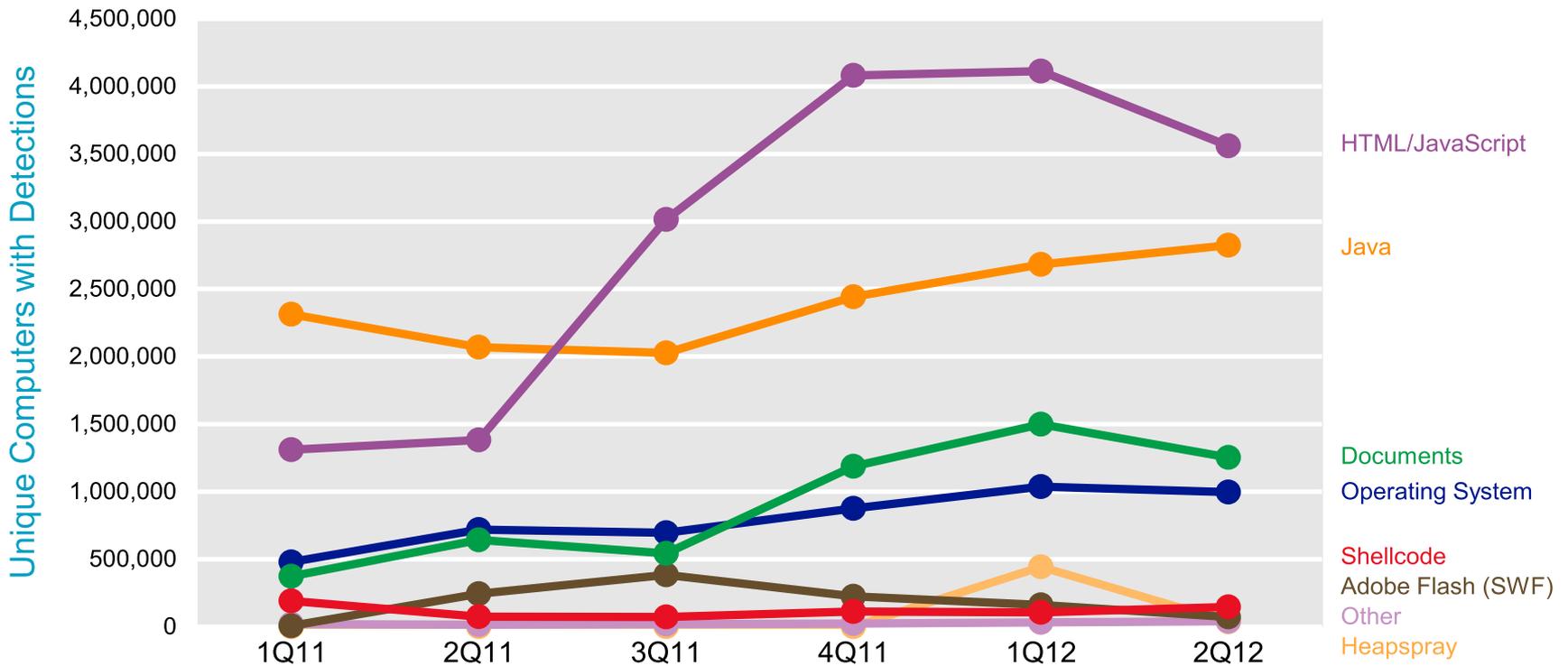


- Industry-wide vulnerability disclosures increased in 1H12
- Disclosures of vulnerabilities in Microsoft products continued to decrease slightly, accounting for 4.8% of all disclosures during the period, down from 6.3% in 2H11

Exploit Trends

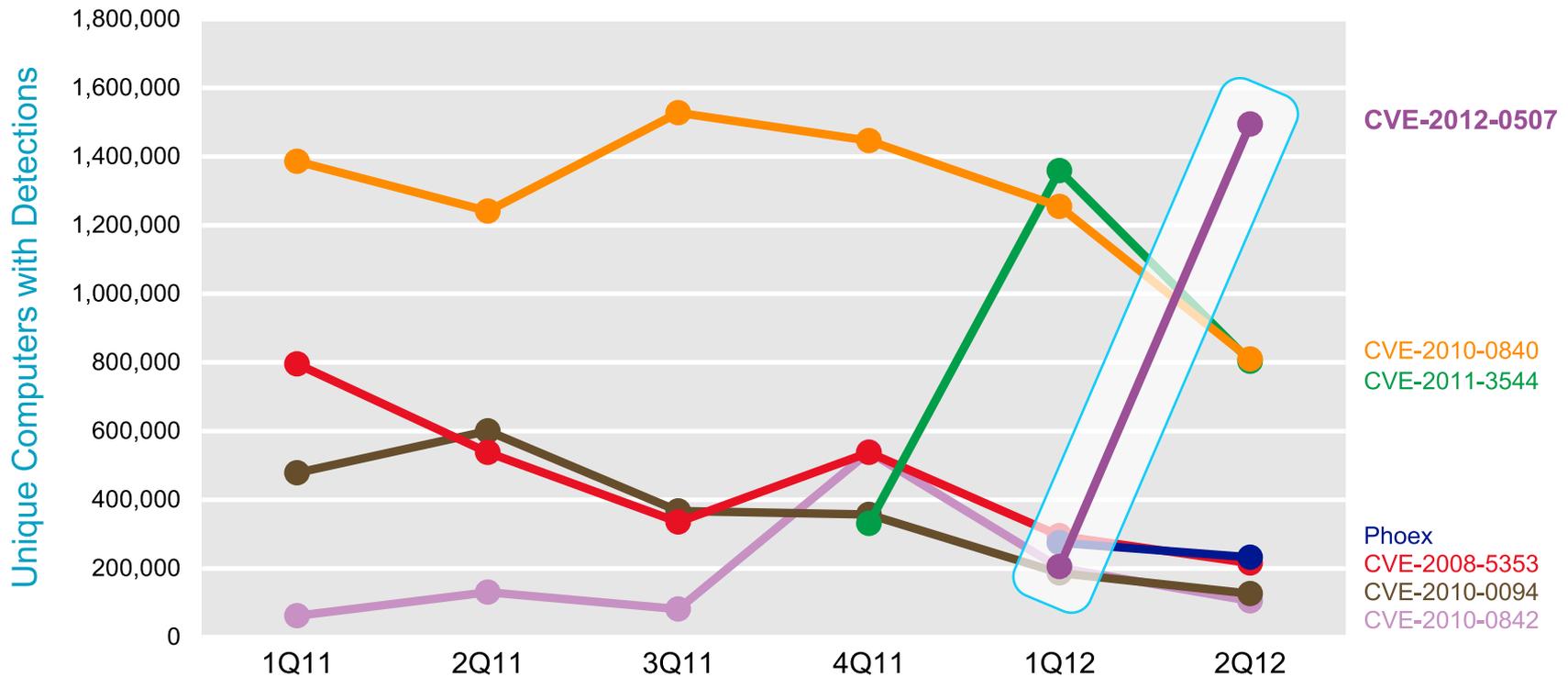


Exploit Trends



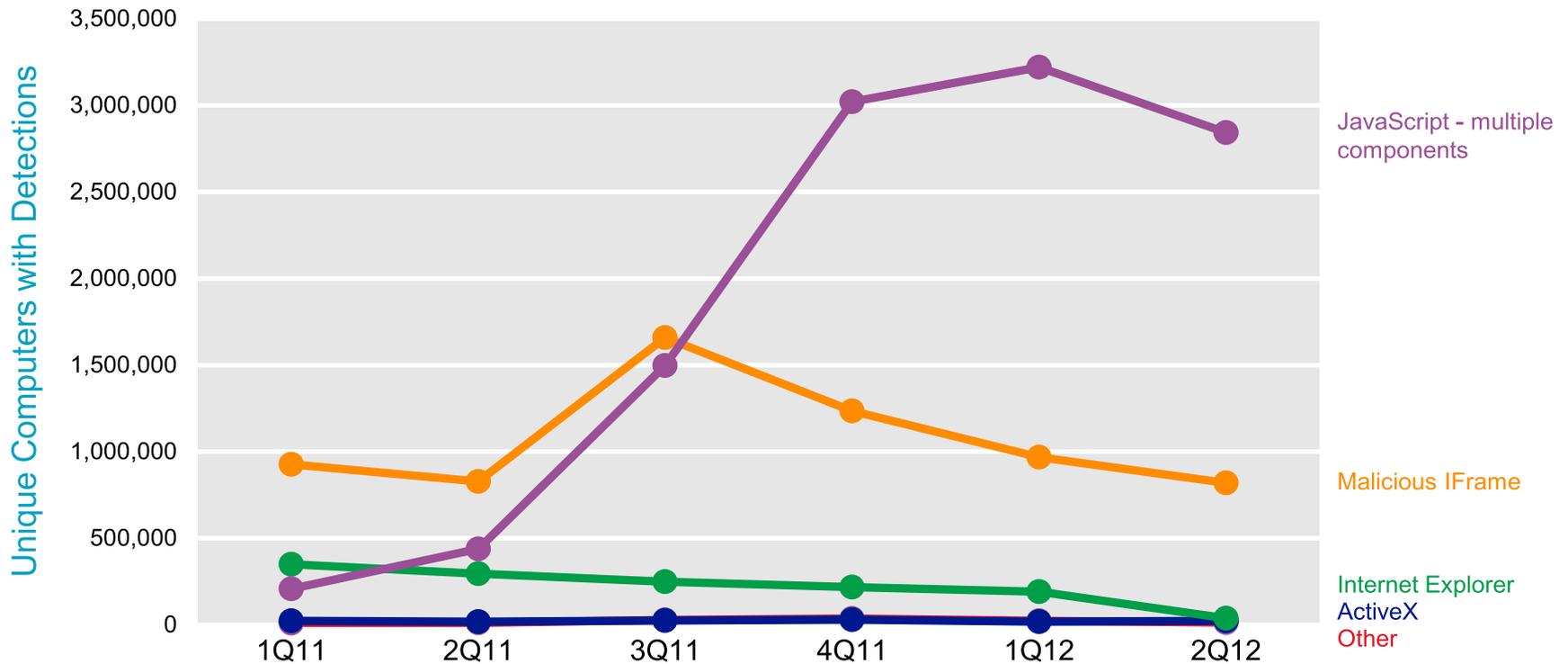
The number of systems reporting exploits delivered through HTML or JavaScript remained high during the first half of 2012, due primarily to the continued prevalence of Blacole.

Java Exploits



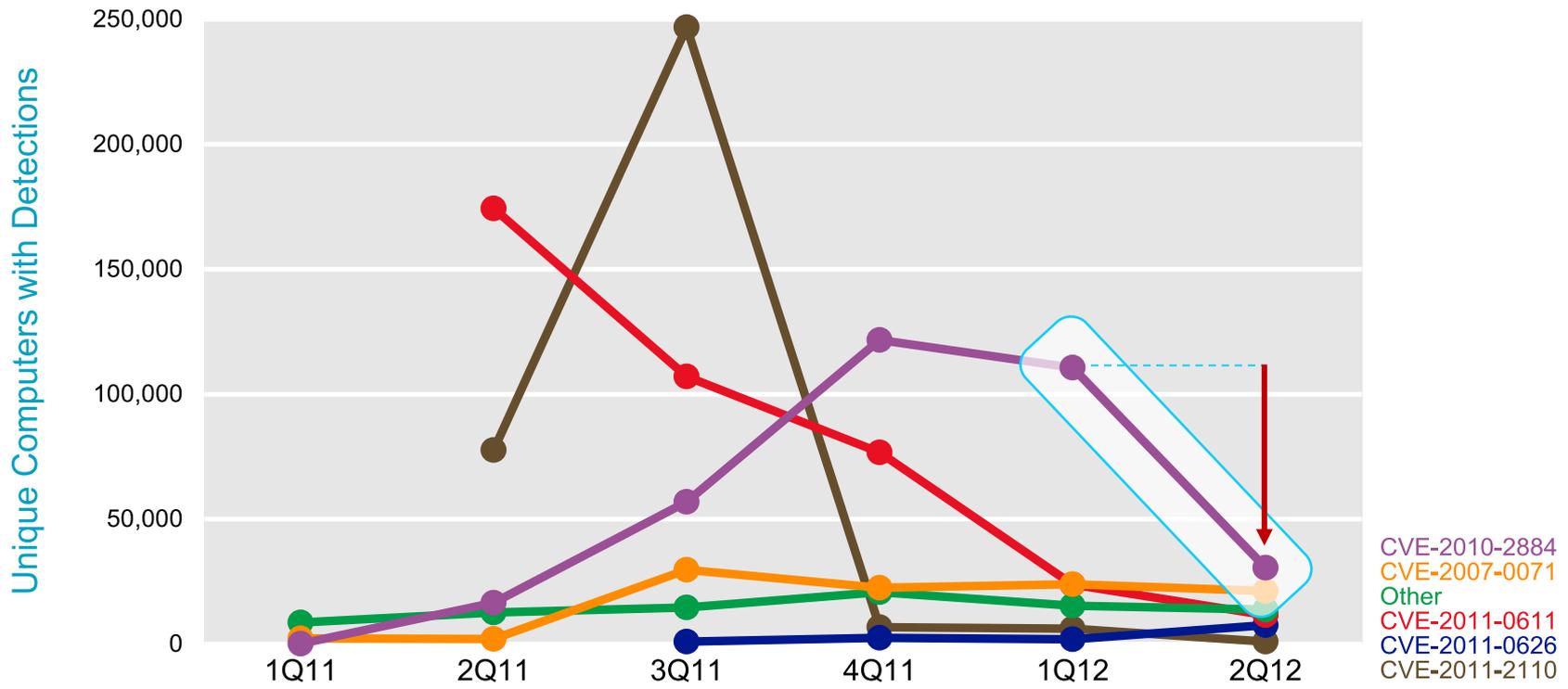
CVE-2012-0507, the multiplatform JRE vulnerability added to the Blacole exploit kit in March 2012, accounted for the largest number of Java exploits detected and blocked in 2Q12.

HTML and JavaScript Exploits



The use of malicious JavaScript code designed to exploit one or more web-enabled technologies accounted for nearly three-fourths of HTML and JavaScript exploits detected in the first half of 2012, primarily because of the Blacole exploit kit.

Adobe Flash Player Exploits



Following a surge in detections that peaked in 3Q11, detections of exploits targeting vulnerabilities in Adobe Flash Player have decreased significantly in every subsequent quarter, with no single vulnerability accounting for more than 35,000 computers with detections by 2Q12.

Top Exploit Families

Exploit Family	Platform or Technology	3Q11	4Q11	1Q12	2Q12
Blacole	HTML/JavaScript	1,054,045	2,535,171	3,154,826	2,793,451
CVE-2012-0507*	Java	—	—	205,613	1,494,074
Win32/Pdfjsc	Documents	491,036	921,325	1,430,448	1,217,348
Malicious IFrame	HTML/JavaScript	1,610,177	1,191,316	950,347	812,470
CVE-2010-0840*	Java	1,527,000	1,446,271	1,254,553	810,254
CVE-2011-3544	Java	—	331,231	1,358,266	803,053
CVE-2010-2568 (MS10-046)	Operating System	517,322	656,922	726,797	783,013
JS/Phoex	Java	—	—	274,811	232,773
CVE-2008-5353	Java	335,259	537,807	295,515	215,593
ShellCode	Shell code	71,729	112,399	105,479	145,352

* This vulnerability is also used by the Blacole kit.
The totals given here for this vulnerability exclude Blacole detections.

Security Update Adoption Rates

Using data gathered from thousands of computers that opted in to data collection, Microsoft has analyzed the distribution of missing security updates across a variety of dimensions.

Security Update Status	Microsoft Windows	Microsoft Word	Adobe Reader	Oracle Java	Adobe Flash Player
Missing latest update*	34%	39%	60%	94%	70%
Missing three latest updates	16%	35%	46%	51%	44%

* As of October 2011: At the time, the most recent updates to Adobe Flash Player, Adobe Reader, and Java had been released within one month. The most recent Windows kernel update had been released 9 months prior, and the most recent update to Word had been released one year prior.

Malware and Potentially Unwanted Software

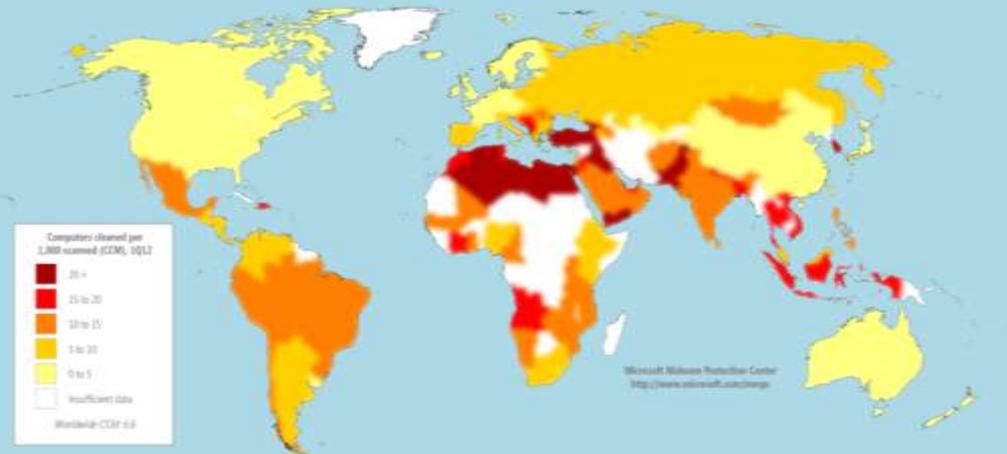


Most Computers Reporting Detections and Removals, by Location

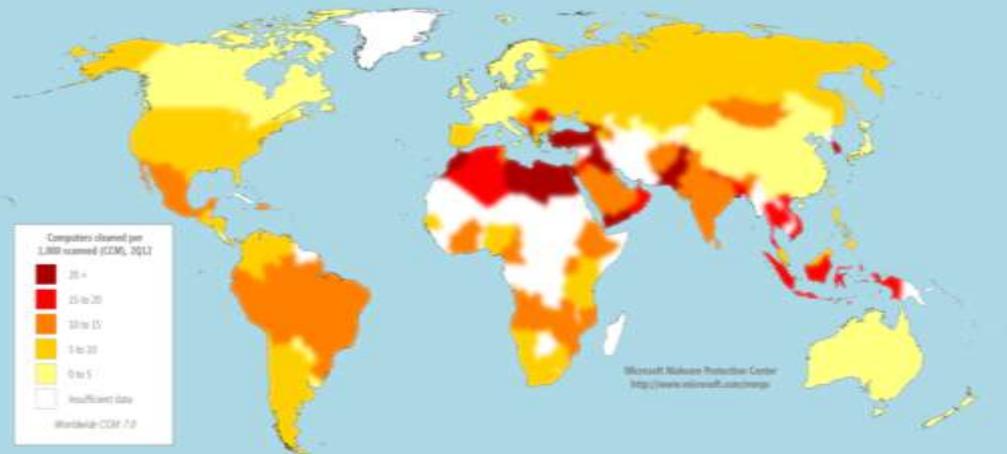
	Country/Region	1Q12	2Q12	Change 1Q to 2Q
1	United States	9,407,423	12,474,127	32.6% ▲
2	Brazil	3,715,163	3,333,429	-10.3% ▼
3	South Korea	2,137,136	2,820,641	32.0% ▲
4	Russia	2,580,673	2,510,591	-2.7% ▼
5	China	1,889,392	2,000,576	5.9% ▲
6	Turkey	1,924,387	1,911,837	-0.7% ▼
7	France	1,677,242	1,555,522	-7.3% ▼
8	United Kingdom	1,648,801	1,509,488	-8.4% ▼
9	Germany	1,544,774	1,486,309	-3.8% ▼
10	Italy	1,361,043	1,341,317	-1.4% ▼

Malware Detections by Country/Region

1Q12

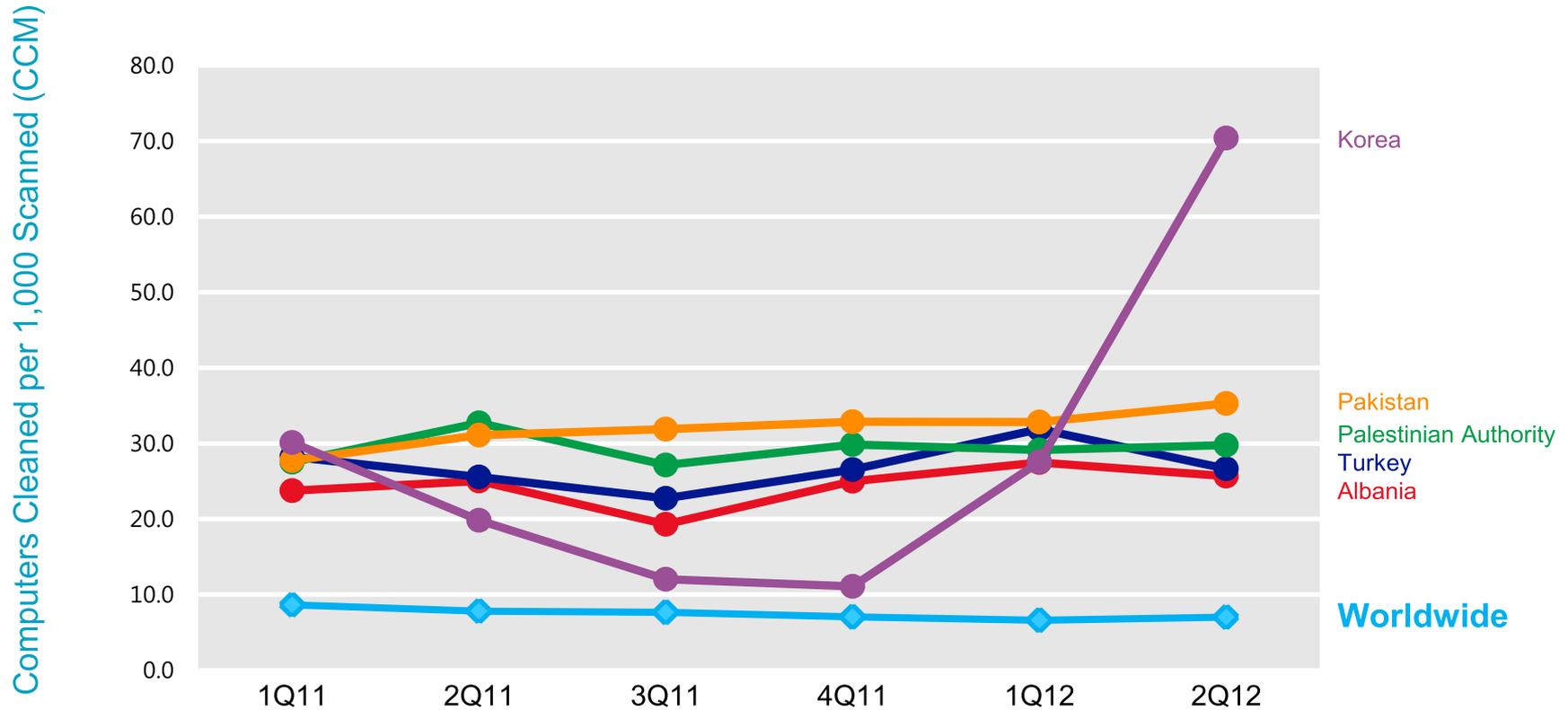


2Q12



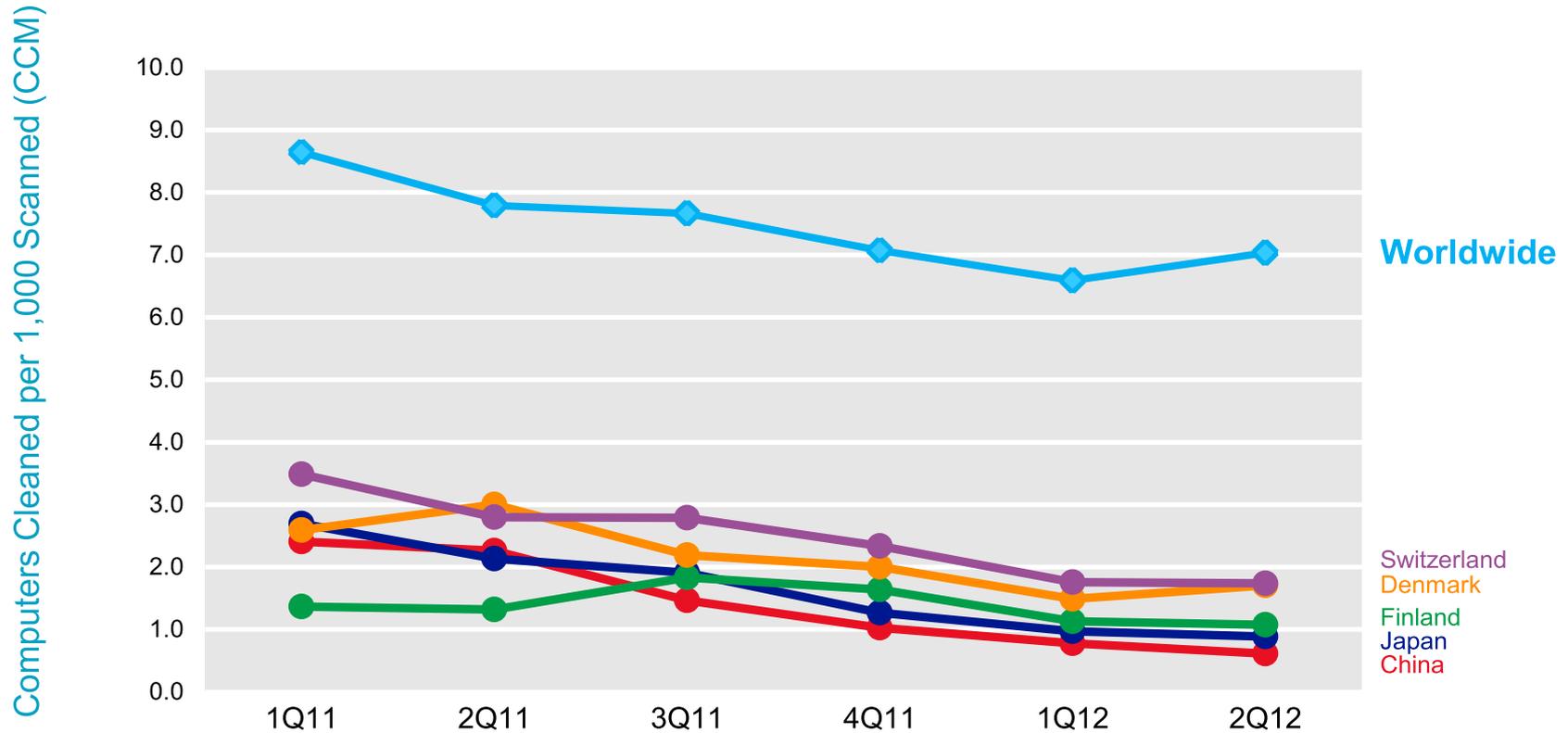
Top 5 Locations

High infection rates



Top 5 Locations

Lowest infection rates



Threat Category Prevalence by Location

Category	World	U.S.	Brazil	Russia	France	Germany	China	Korea	Turkey	U.K.	Italy
Misc. Trojans	37.9%	43.6%	32.6%	41.8%	28.8%	35.0%	29.9%	23.6%	35.9%	43.2%	31.8%
Misc. Potentially Unwanted Software	32.2%	22.7%	38.1%	57.1%	29.3%	26.6%	45.0%	11.0%	31.2%	23.3%	29.4%
Worms	19.3%	12.3%	23.3%	16.4%	12.6%	8.8%	11.1%	4.9%	34.5%	6.6%	13.6%
Adware	18.5%	19.1%	7.5%	4.9%	31.5%	19.0%	22.4%	38.0%	24.6%	26.1%	24.1%
Trojan Downloaders and Droppers	16.4%	13.1%	22.4%	13.0%	16.1%	10.8%	12.6%	53.8%	13.0%	13.3%	23.2%
Exploits	14.8%	18.7%	5.8%	17.8%	16.2%	28.2%	10.3%	3.5%	6.4%	24.0%	19.7%
Viruses	7.8%	4.4%	9.1%	5.1%	2.2%	2.2%	10.6%	2.0%	15.0%	3.1%	2.5%
Password Stealers and Monitoring Tools	6.3%	4.6%	15.7%	4.1%	4.6%	10.7%	3.2%	2.6%	6.2%	4.8%	7.6%
Backdoors	4.2%	3.4%	3.9%	3.2%	2.8%	3.2%	5.9%	2.0%	4.2%	3.0%	2.9%
Spyware	0.2%	0.3%	0.1%	0.2%	0.1%	0.2%	1.3%	0.1%	0.0%	0.2%	0.1%

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

Top 10 Threat Families

Family	Most Significant Category	3Q11	4Q11	1Q12	2Q12
Win32/Keygen	Misc. Potentially Unwanted Software	3,424,213	4,187,586	4,775,464	4,775,243
Win32/Autorun	Worms	3,292,378	3,438,745	3,316,107	3,510,816
JS/Pornpop	Adware	3,944,489	3,906,625	3,994,634	2,838,713
Blacole	Exploits	1,056,595	2,535,968	3,157,580	2,794,300
HTML/IframeRef	Misc. Trojans	1,612,828	1,191,929	952,111	2,493,830
Win32/Sality	Viruses	1,728,966	1,951,118	2,101,968	2,097,663
Win32/Hotbar	Adware	2,870,465	2,226,173	3,008,677	2,073,789
Win32/Dorkbot	Worms	1,107,300	1,713,962	1,883,642	2,055,244
ASX/Wimad	Trojan Downloader	748,716	1,825,291	1,487,334	1,890,806
Win32/Obfuscator	Misc. Potentially Unwanted Software	1,521,959	1,623,137	1,393,148	1,851,304

Popular Keygen Targets

Keygen.exe

Windows Loader.exe

Mini-KMS_Activator_v1.1_Office.2010.VL.ENG.exe

AutoCAD-2008-keygen.exe

SonyVegasPro Patch.exe

Nero Multimedia Suite 10 – Keygen.exe

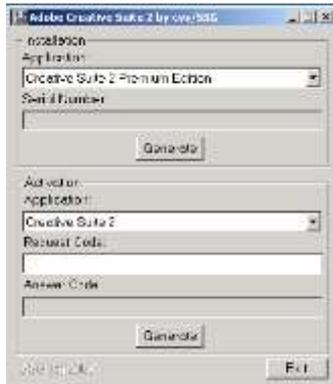
Adobe.Photoshop.CS5.Extended.v12.0.Keymaker-EMBRACE.exe

Call.of.Duty.4.Modern.Warfare.Full-Rip.Skullptura.7z

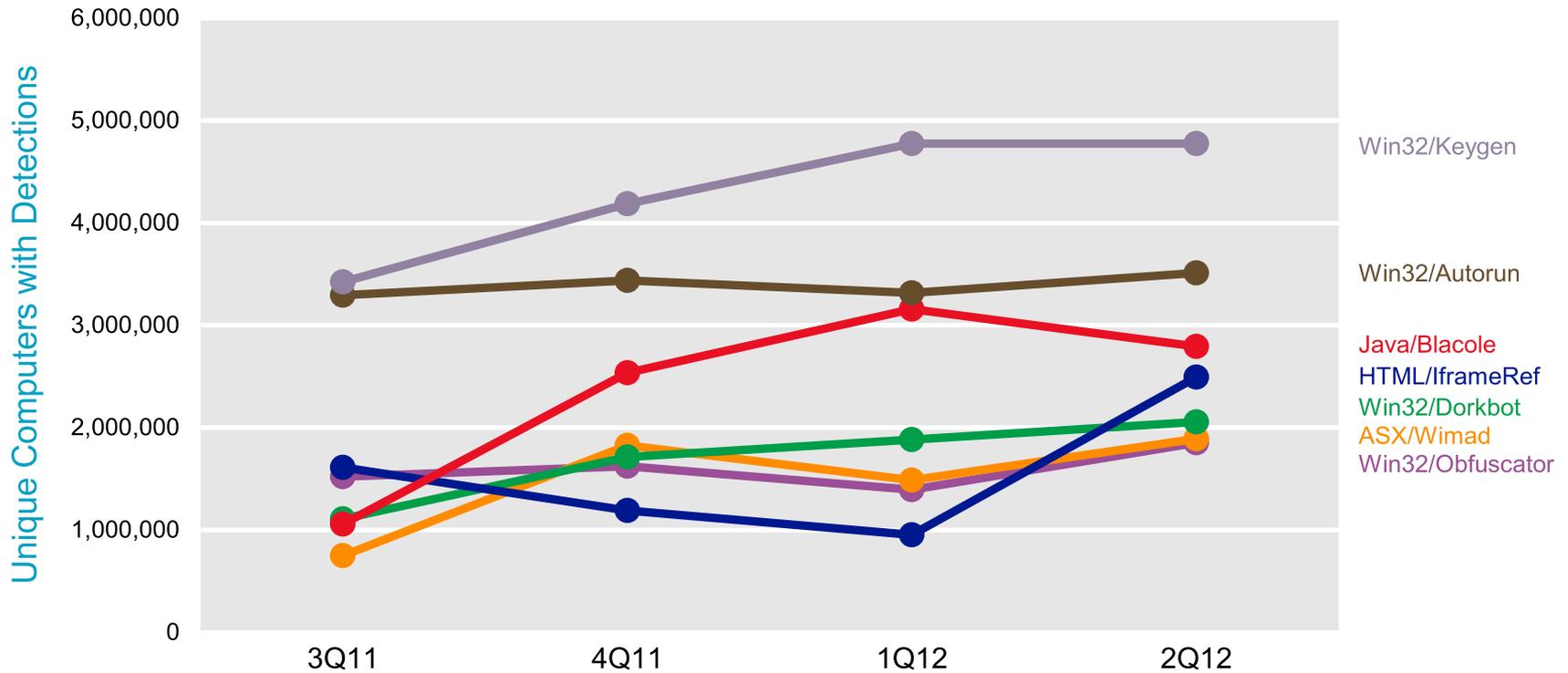
Guitar Pro v6.0.7+Soundbanks+Keygen(Registered) [kk].rar

Half Life CDkeygen.exe

Keygen Examples

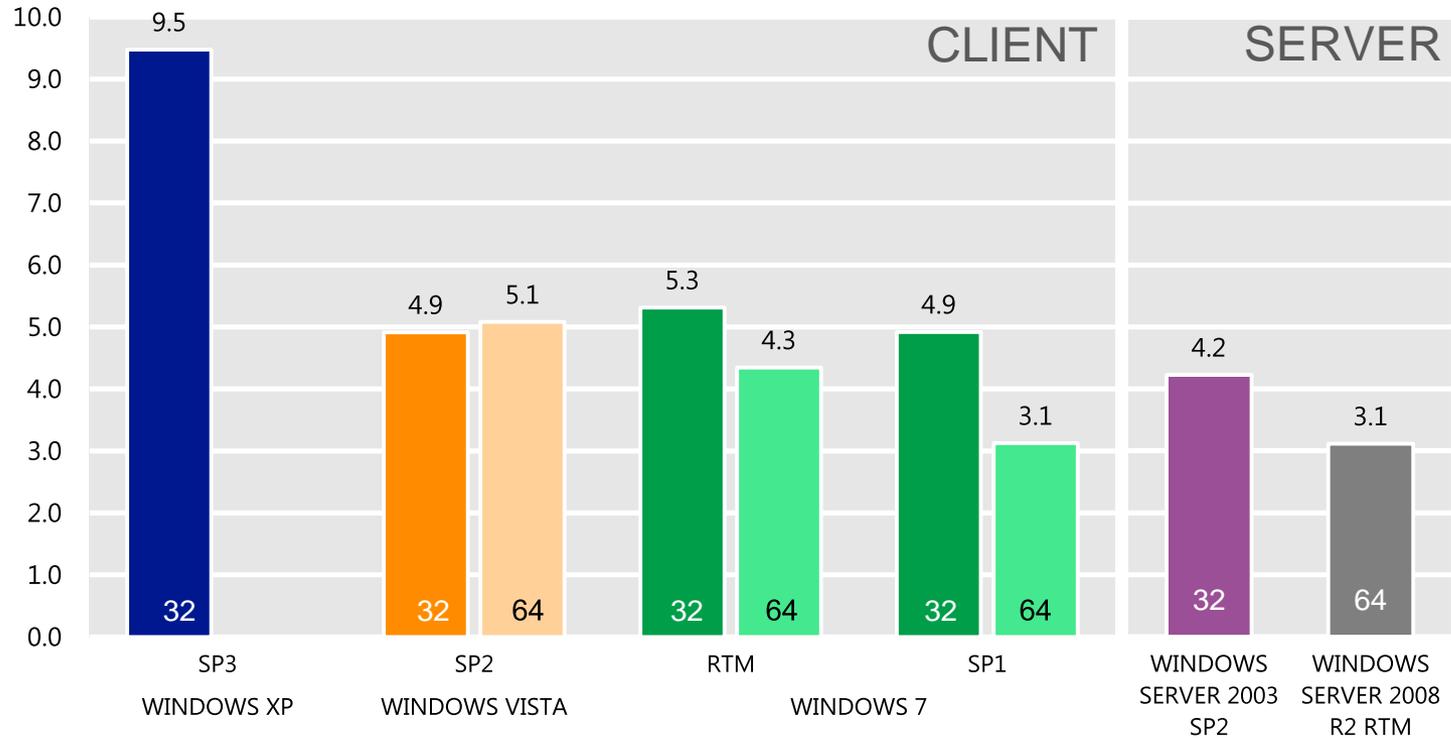


Trends for Notable Threat Families



Infection Rates by OS and Service Pack

Computers Cleaned per 1,000 Scanned (CCM)



- 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

Most Commonly Detected Malware, by Platform

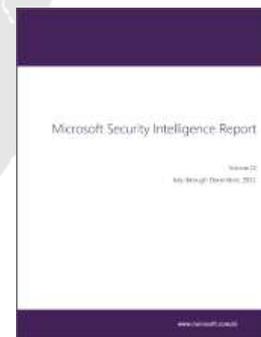
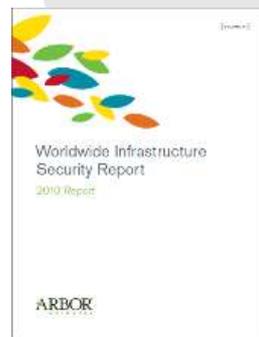
Family	Most Significant Category	Rank (Windows 7 SP1)	Rank (Windows 7 RTM)	Rank (Windows Vista SP2)	Rank (Windows XP SP3)
Win32/Keygen	Misc. Potentially Unwanted Software	1	1	11	6
Win32/Autorun	Worms	3	2	15	3
JS/Pornpop	Adware	2	6	2	7
Blacole	Exploits	4	11	1	5
JS/IframeRef	Misc. Trojans	10	7	10	1
Win32/Sality	Viruses	16	4	35	4
Win32/Hotbar	Adware	6	5	3	21
Win32/Dorkbot	Worms	9	3	21	9
ASX/Wimad	Trojan Downloaders and Droppers	8	9	5	13
Win32/Obfuscator	Misc. Potentially Unwanted Software	5	12	14	11
Win32/FakePAV	Misc. Trojans	7	19	4	10
Win32/Conficker	Worms	15	10	26	8
Win32/Sirefef	Misc. Trojans	12	13	7	15
Java/CVE-2012-0507	Exploits	11	34	6	12
Win32/Pluzoks	Trojan Downloaders and Droppers	40	56	56	2

Socio-economic Factors & Malware Infection Rates



Global Cybersecurity Outlook

What are the measures and indicators that policy makers can leverage to advance their understanding of cybersecurity at the national level?



Broader Impact of Cybersecurity Requires Broader Assessment of Metrics

Technical



280m active users



Extremely popular browser, with SmartScreen, Microsoft Phishing Filter



Billions of web pages scanned each month



Available in over 30 languages



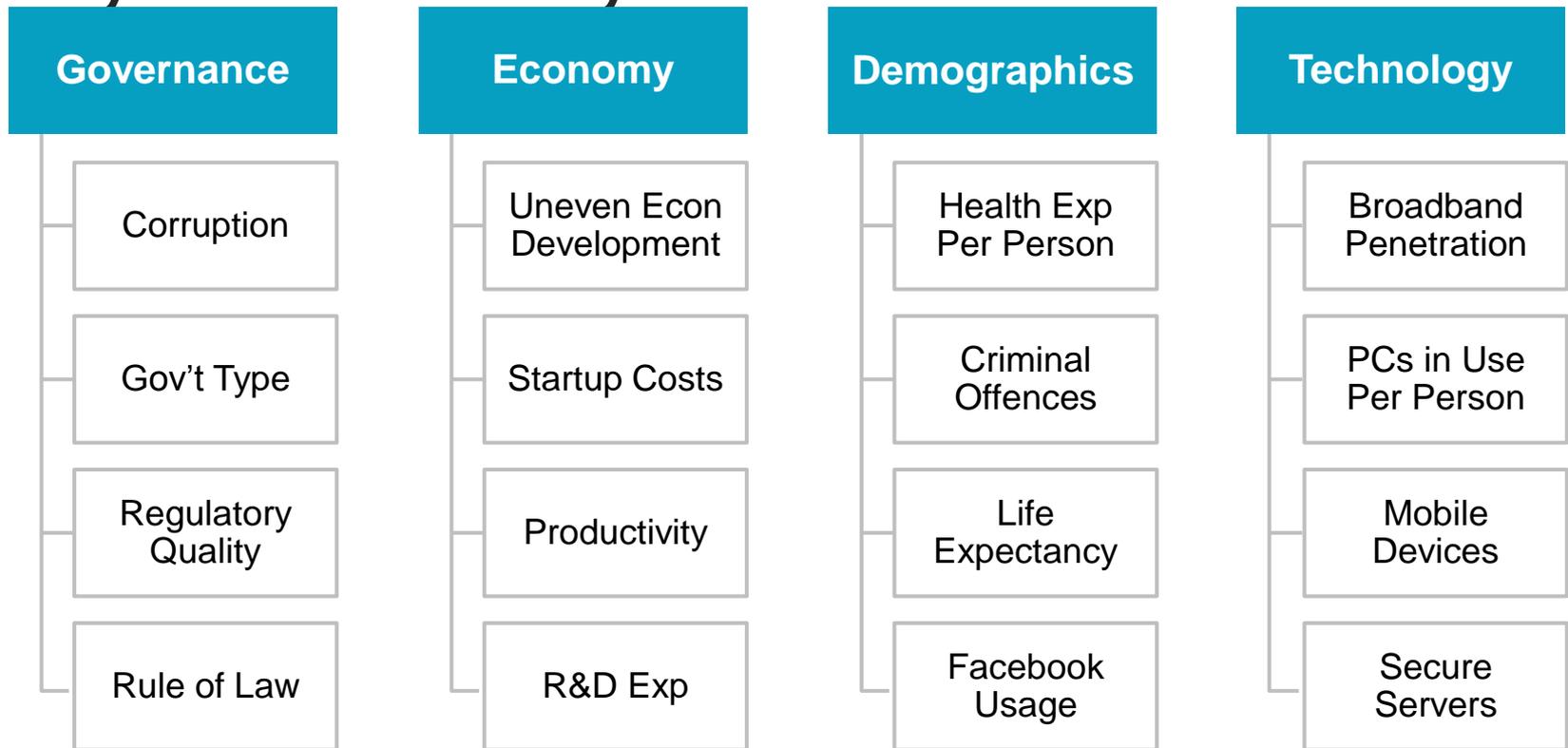
Runs security scans on billions of email messages annually

Social, Economic, Political

- Governance
- Economy
- Demographics
- Technological Advancement



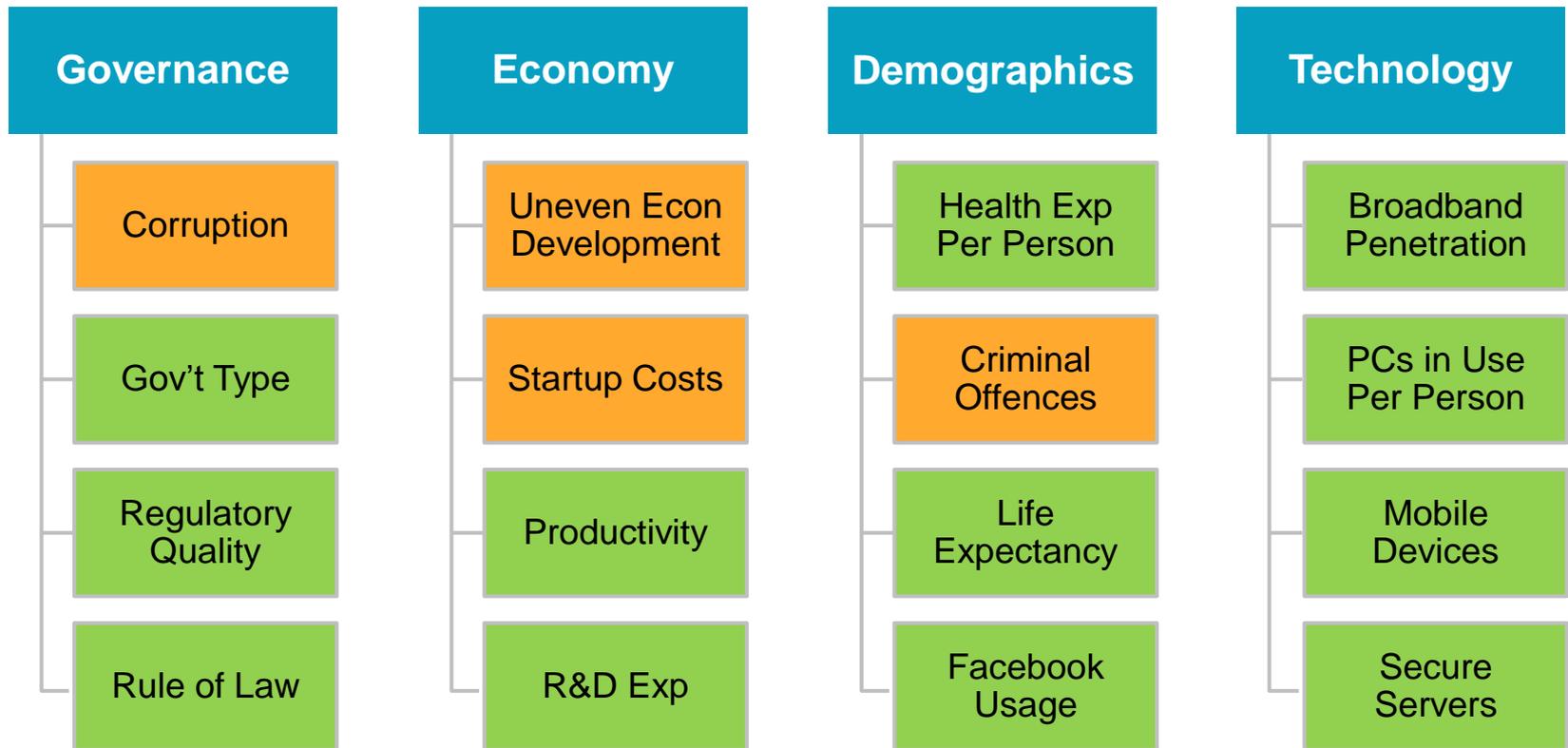
80 Quantitative Measures Predicting National Cybersecurity



Correlative Relationships with

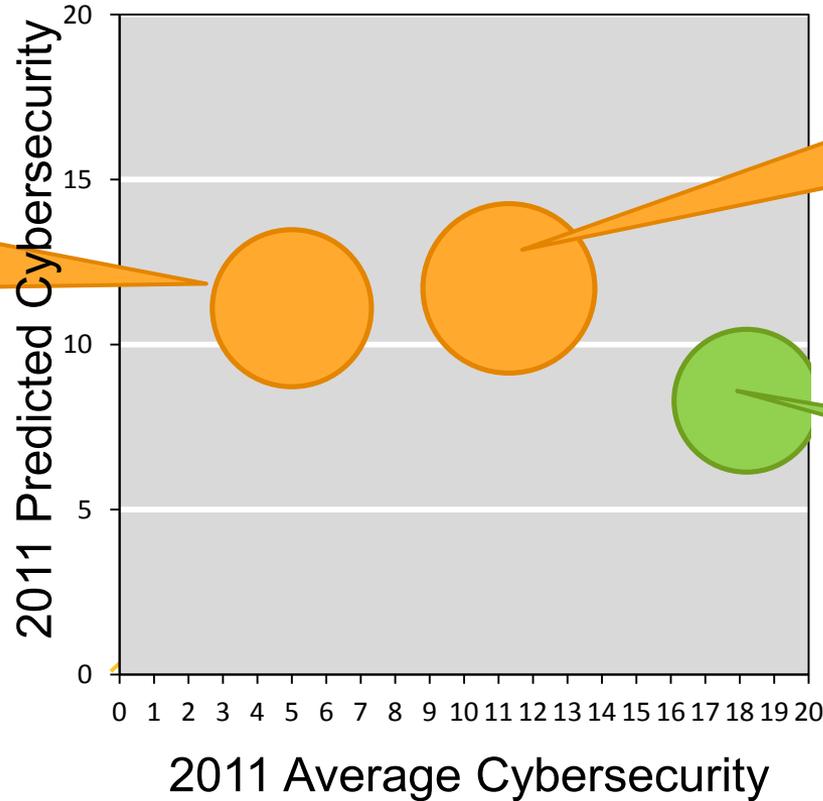
Increase in yellow boxes correlates with lower performance in cybersecurity

Increase in green boxes correlates with higher performance in cybersecurity.



Within the Model, Clusters Emerge

Maximizers
Countries with more effective cybersecurity capabilities and outperform the model



Aspirants
Countries who are on par with model and still developing cybersecurity capabilities

Seekers
Countries with higher cybersecurity risk who underperform model expectations

Applying It



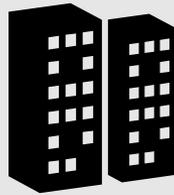
Apply

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

— In the first three months following this presentation you should:

Determine if you are using WU or MU

Evaluate 3rd party software patching

Look for Keygen in your environment

— Within six months you should:

Upgrade older software

Educate your people on threats & risks

Resources

- ▶ SIR volumes, special editions, videos, guidance:
<http://microsoft.com/sir>
- ▶ Microsoft Malware Protection Center:
<http://microsoft.com/mmpc>
- ▶ Official Microsoft Security blog:
<http://blogs.technet.com/b/security/>
- ▶ Twitter: @MSFTSecurity

