RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

A deep dive into the security threat landscape of the Middle East/Southwest Asia

SESSION ID: HT-W01

Tim Rains

Director, Trustworthy Computing
Microsoft Corporation

About Tim Rains

- Director, Trustworthy Computing
  - Threat intelligence, MSRC, MMPC, MSEC, cybersecurity public policy, Cloud security
- Reformed Engineer: Windows, Consulting, IT
- Microsoft Security Blog, Trustworthy Computing Blog, Microsoft EU blog, Microsoft on the Issues, the Official Microsoft Blog
- Twitter: @MSFTSecurity

Data from Middle East/Southwest Asia

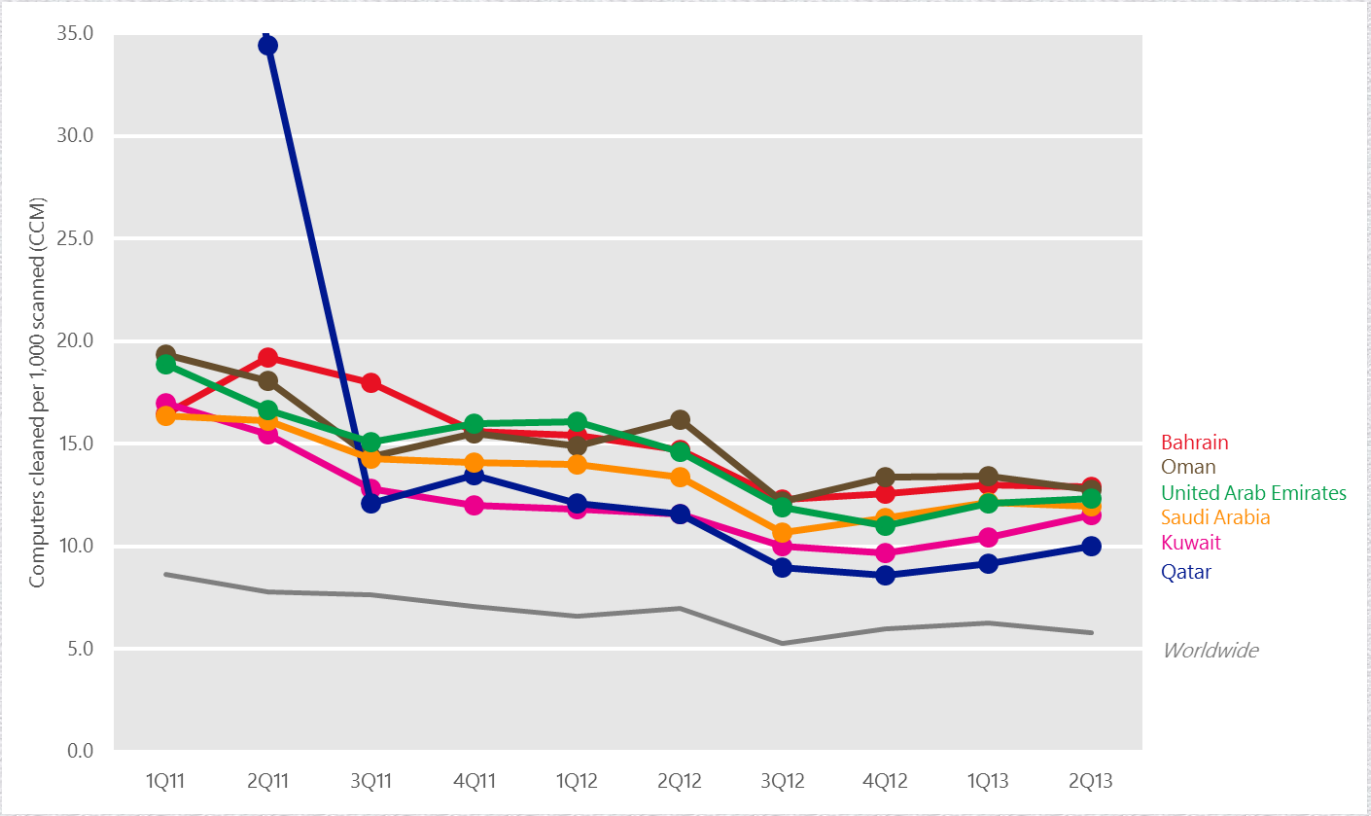
- Bahrain, Egypt, Israel, Iraq, Jordan, Kuwait, Lebanon, Oman, Pakistan, Palestinian Authority, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates
- “The Gulf” includes members of the Gulf Cooperation Council: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, United Arab Emirates

Recent history

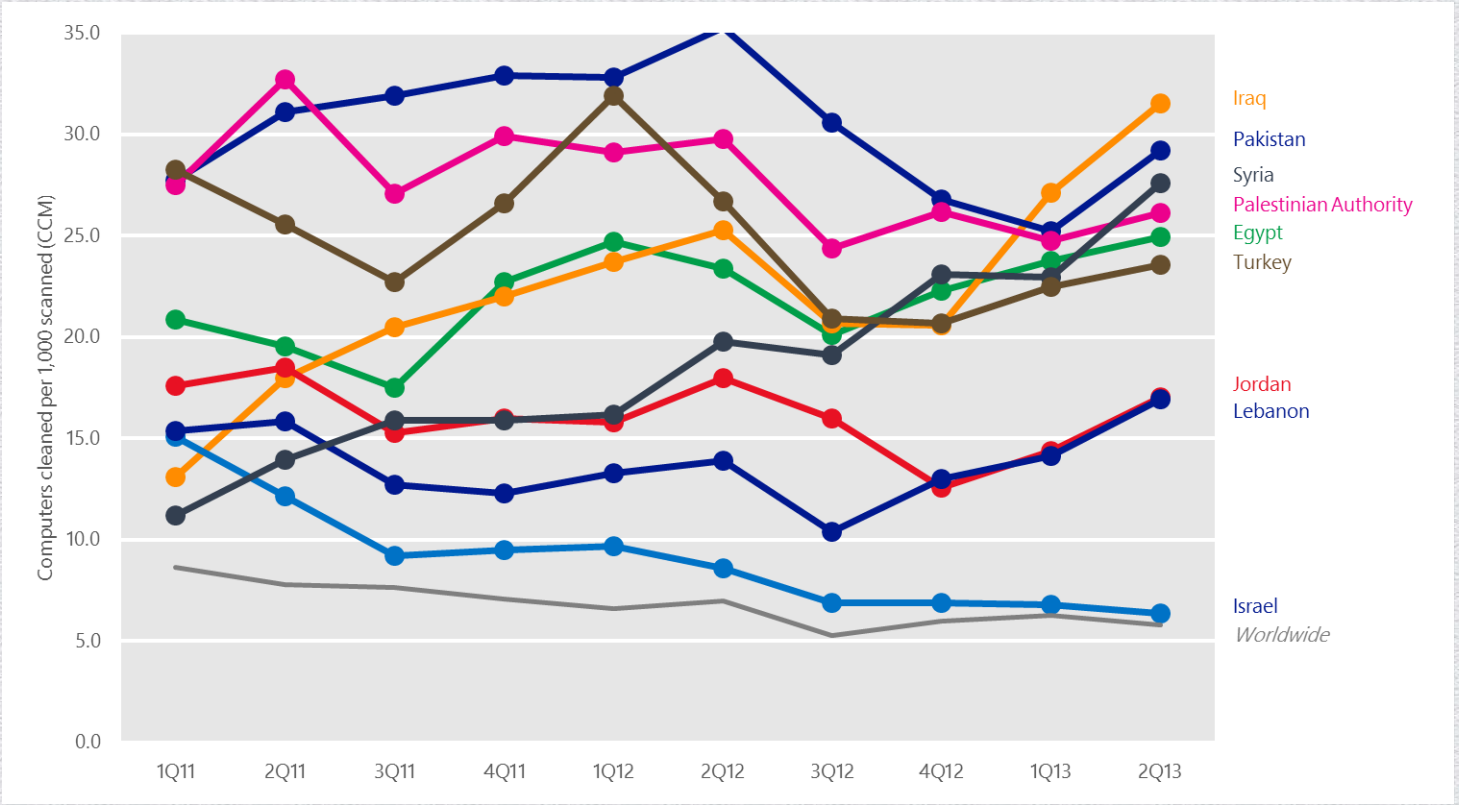
- Geopolitical
  - Above-average level of strife and turmoil
  - Many political transitions
- High-profile malware attacks
  - Stuxnet
  - Saudi Aramco

Malware encounter and infection Rates

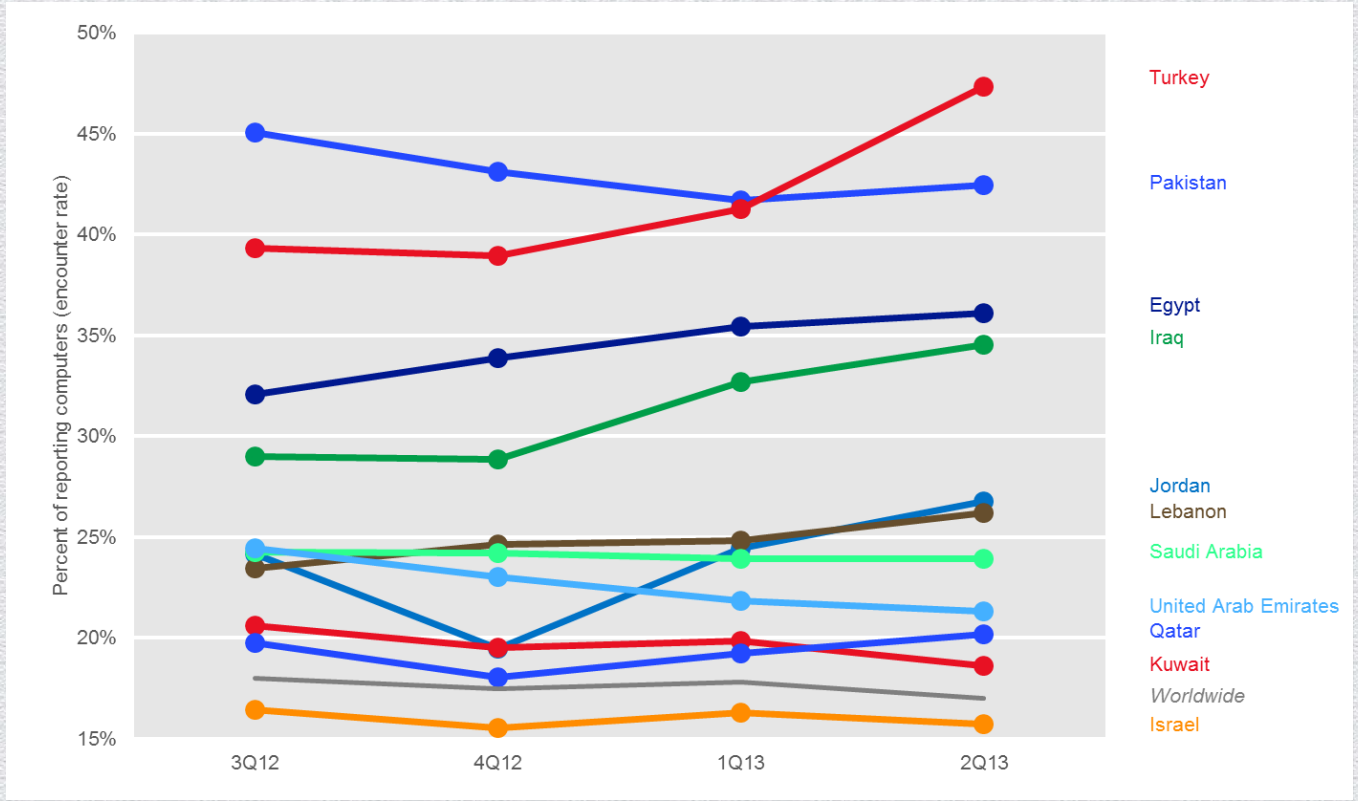
Malware infection rates 1Q11-2Q13 - Gulf



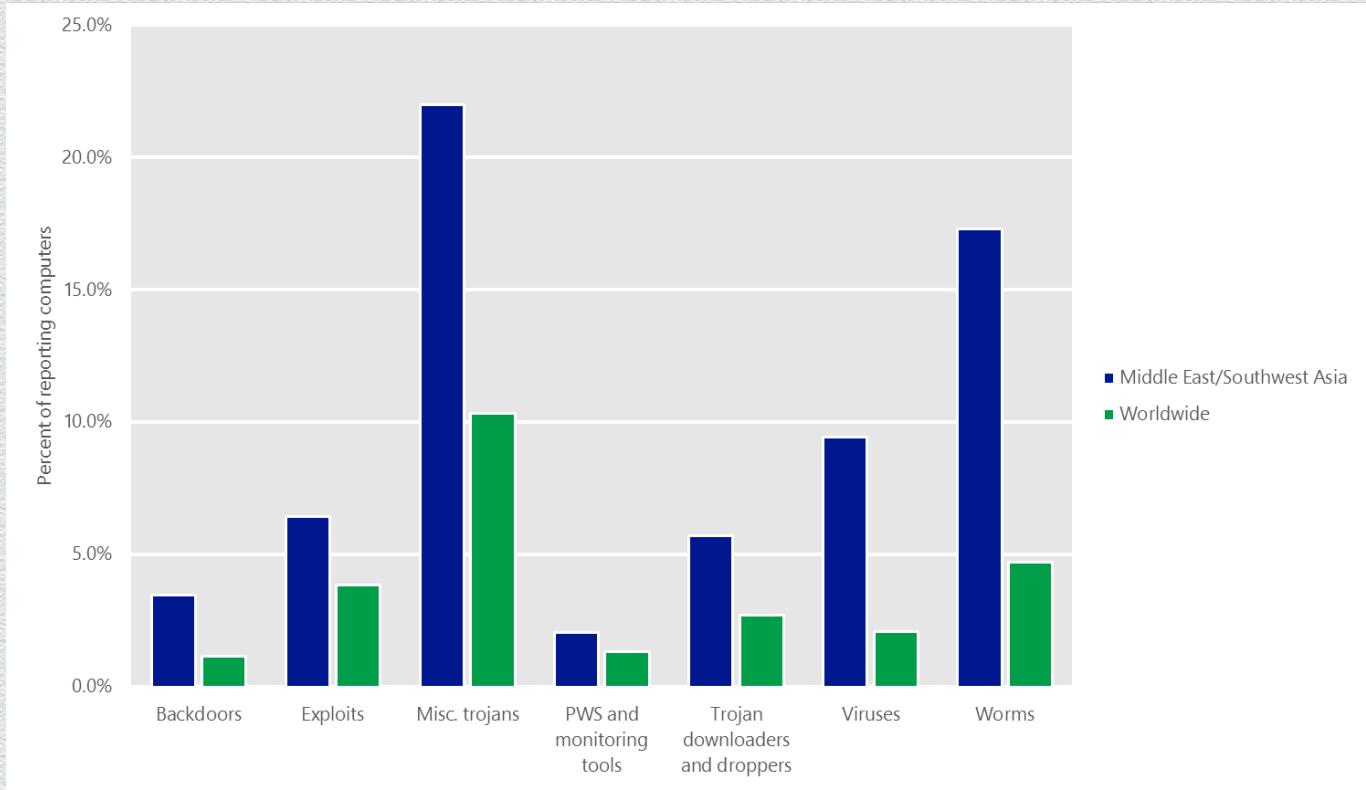
Malware infection rates 1Q11-2Q13



Malware encounter rate 3Q12-2Q13



Threat categories encountered

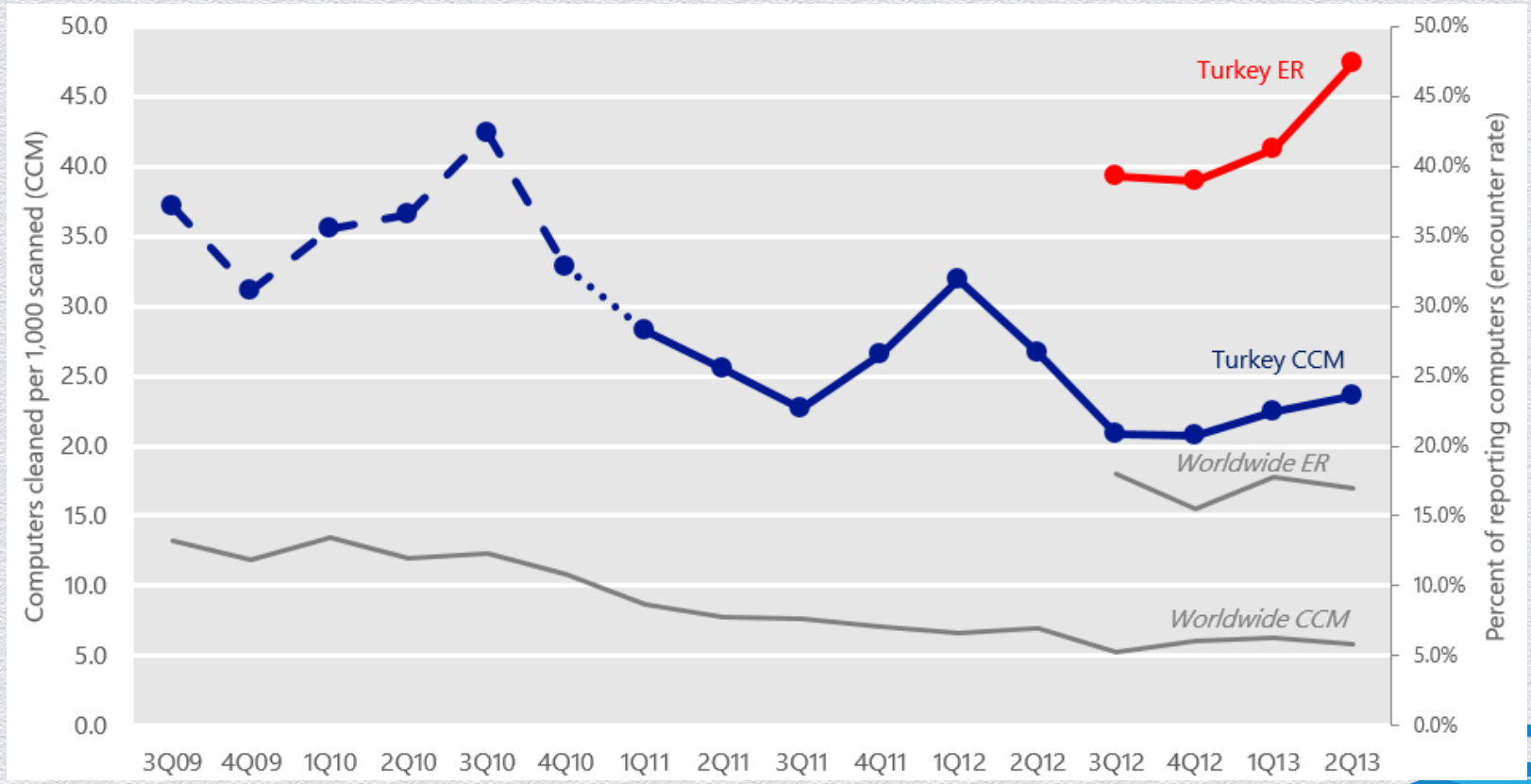


Top 10 families by encounter rate

Family	Most significant category	3Q12	4Q12	1Q13	2Q13
Autorun	Misc. trojans	7.72%	8.11%	7.60%	6.94%
Gamarue	Worms	0.24%	0.19%	0.97%	4.45%
Obfuscator	Misc. trojans	1.55%	2.14%	3.00%	4.43%
Sality	Viruses	4.25%	4.66%	4.55%	4.27%
IframeRef	Misc. trojans	0.88%	2.42%	3.48%	3.53%
Ramnit	Misc. trojans	2.07%	2.64%	2.70%	2.73%
Kilim	Misc. trojans	-	-	-	2.40%
Dorkbot	Worms	1.55%	2.02%	1.94%	2.32%
Nuqel	Worms	2.07%	2.46%	2.40%	2.27%
CplLnk	Exploits	1.74%	2.23%	2.22%	2.17%
Murkados	Worms	-	-	-	1.89%

Case study: Turkey

Malware infection and encounters: Turkey



Comparing Turkey's 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 percent because some computers reported threats from more than one category.

Targeted families - Turkey

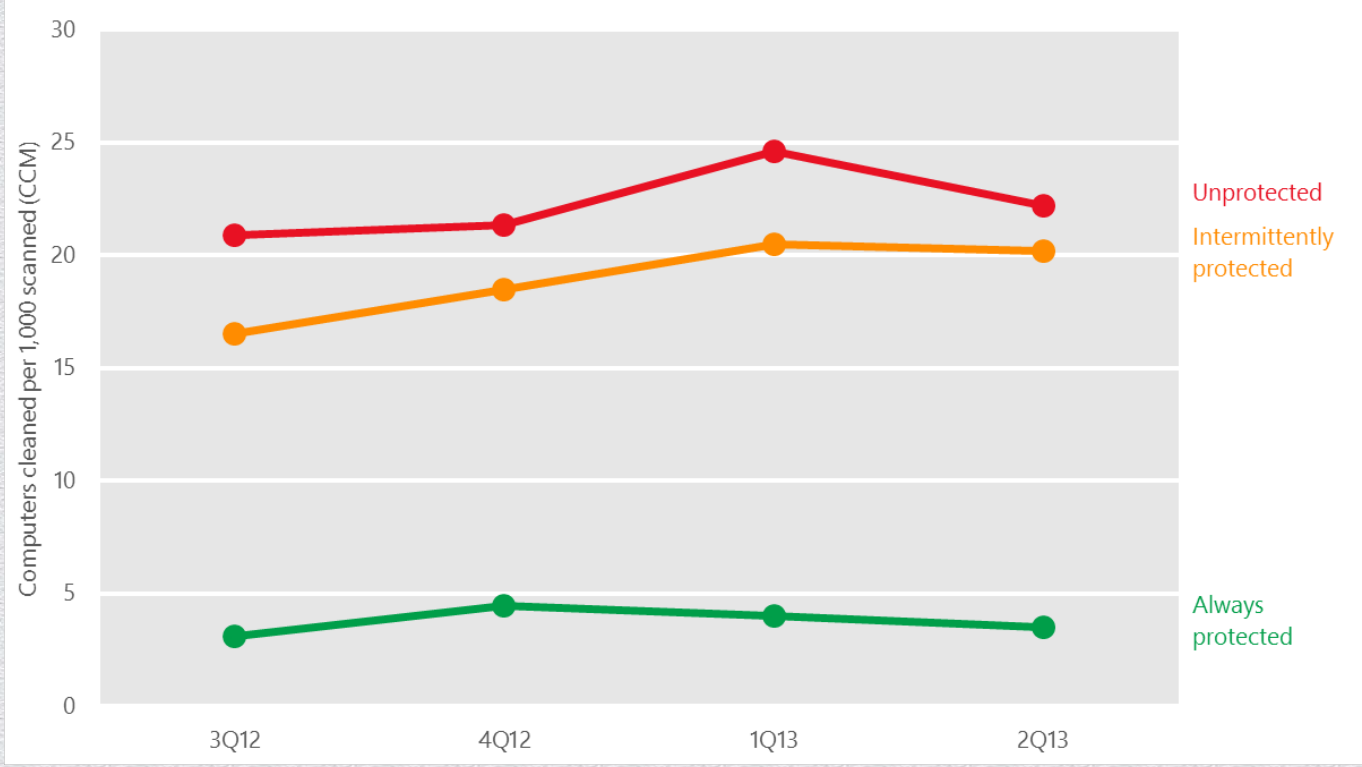
Category	Brazil	China	France	Germany	India	Mexico	Russia	Turkey	United Kingdom	United States
Backdoors	0.02%	0.08%	0.04%	0.00%	0.02%	0.00%	0.00%	0.00%	0.00%	0.10%
Exploits	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.01%
Misc. Trojans	1.86%	0.18%	0.00%	0.64%	0.72%	1.57%	1.50%	11.31%	0.00%	1.58%
PWS and Monitoring Tools	1.76%	0.09%	0.00%	0.32%	0.01%	0.01%	0.10%	0.08%	0.00%	0.01%
Trojan Downloaders and Droppers	3.65%	0.10%	0.00%	0.00%	0.00%	0.04%	1.97%	4.44%	0.00%	0.13%
Viruses	0.04%	0.57%	0.00%	0.00%	0.04%	0.00%	0.02%	0.00%	0.00%	0.00%
Worms	0.28%	0.09%	0.00%	0.00%	2.58%	1.23%	0.03%	4.74%	0.00%	0.00%

Targeted if at least 80 percent of the infected computers are located in a single country

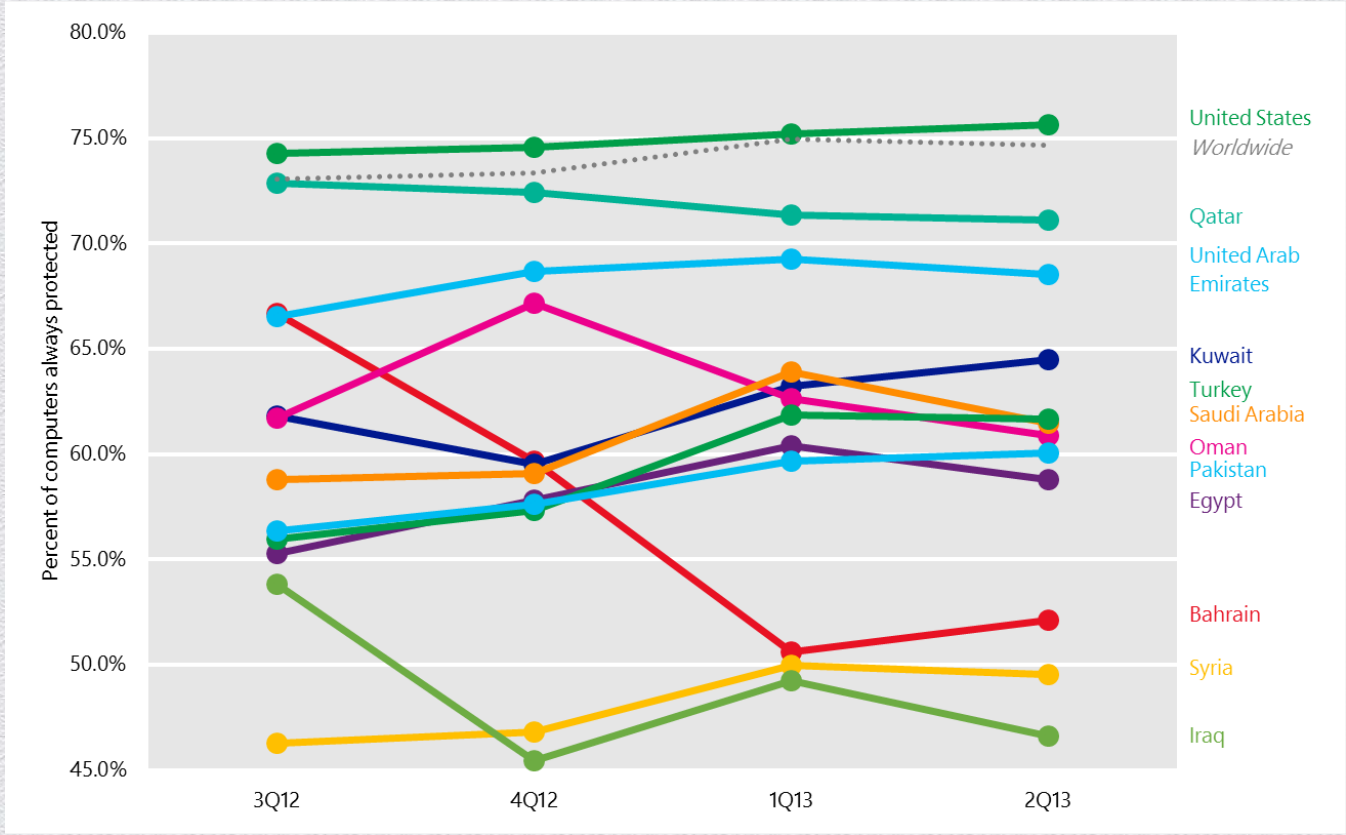
Category	Family	Turkey Machines	Non-Turkey Machines	Percentage in Turkey
Misc. Trojans	Kilim	217,260	17,360	92.60%
Worms	Murkados	164,132	5,051	97.01%
Trojan Downloaders and Droppe	Truado	120,623	17,188	87.53%
Misc. Trojans	Preflayer	89,625	7,430	92.34%
Misc. Trojans	Reksner	45,388	1,200	97.42%

Regional antivirus usage

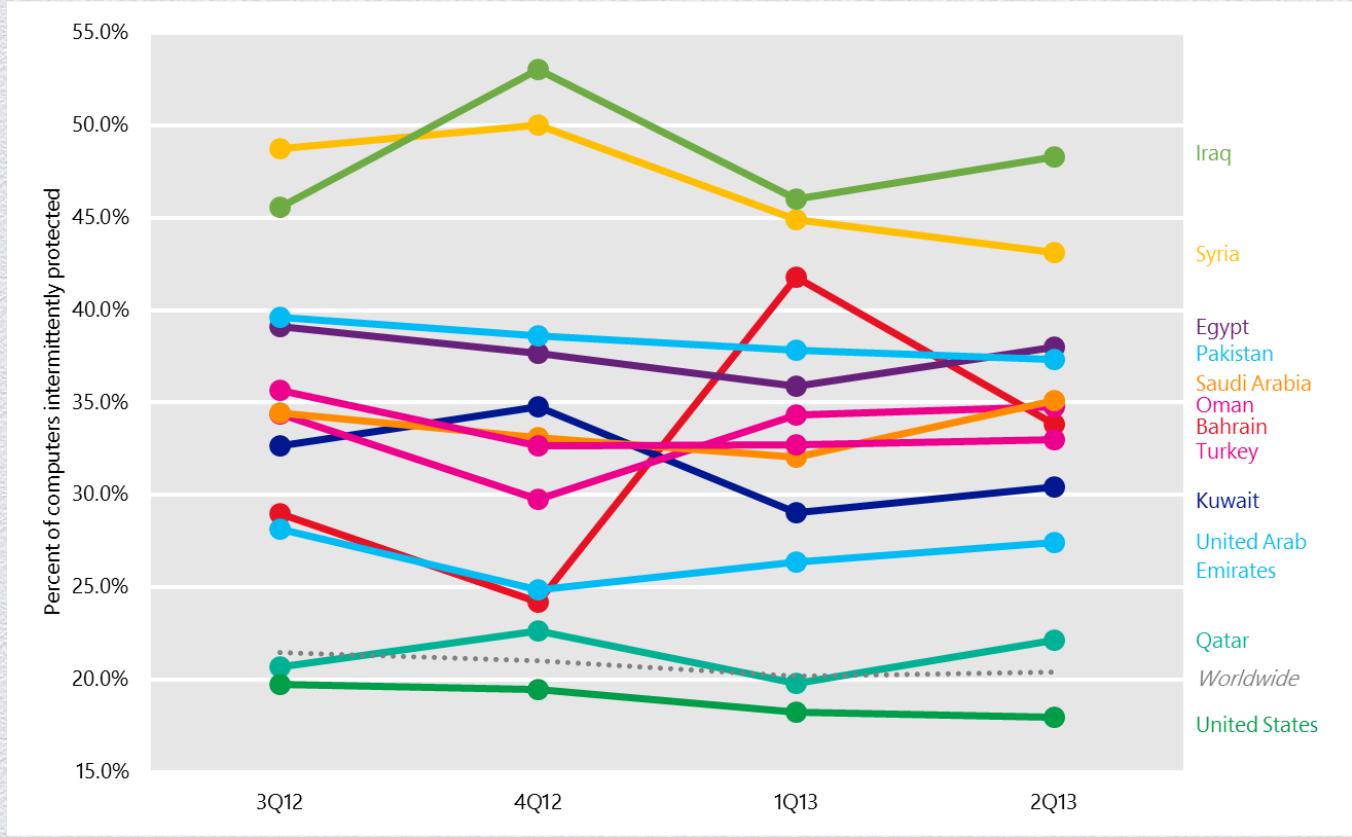
CCM by antivirus state



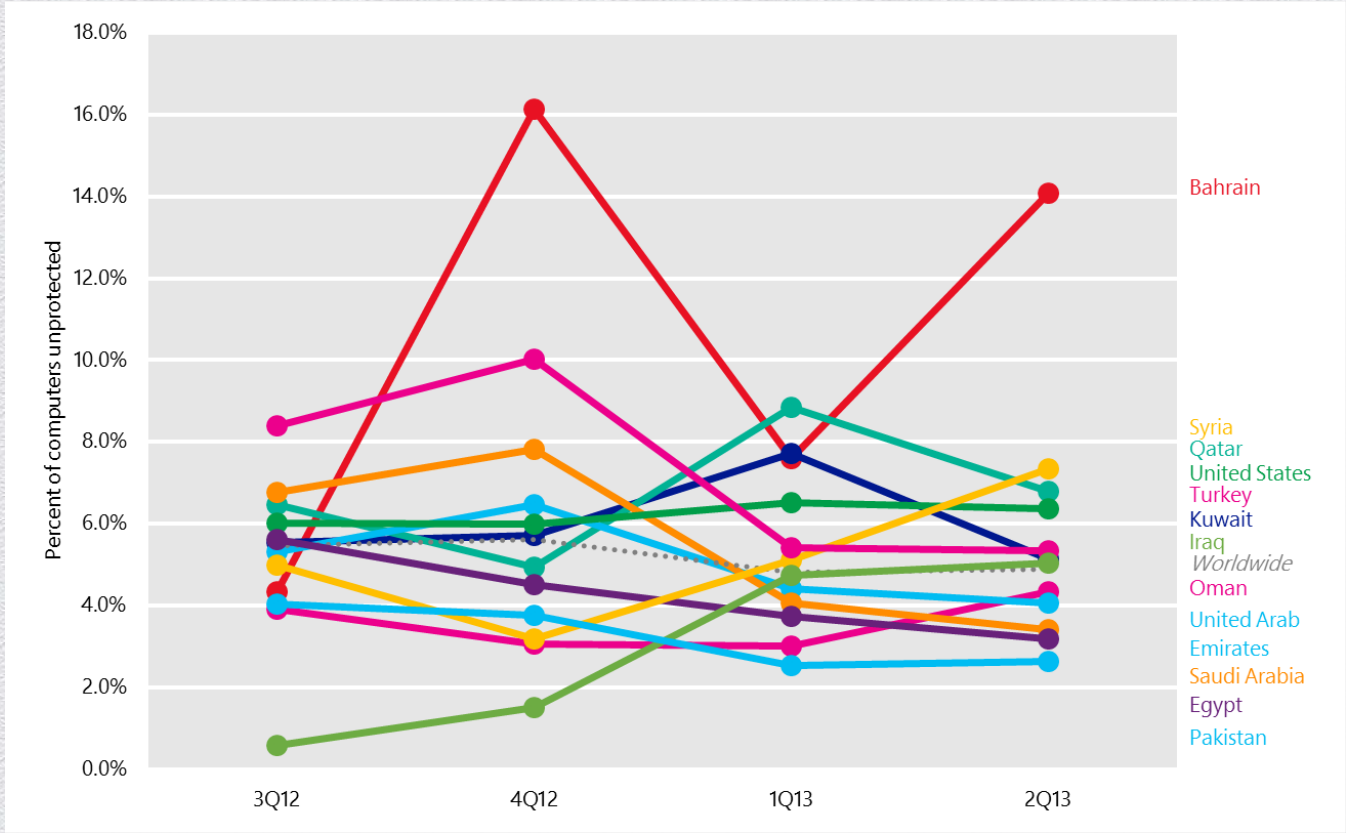
Realtime antivirus: always protected



Realtime antivirus: intermittently protected

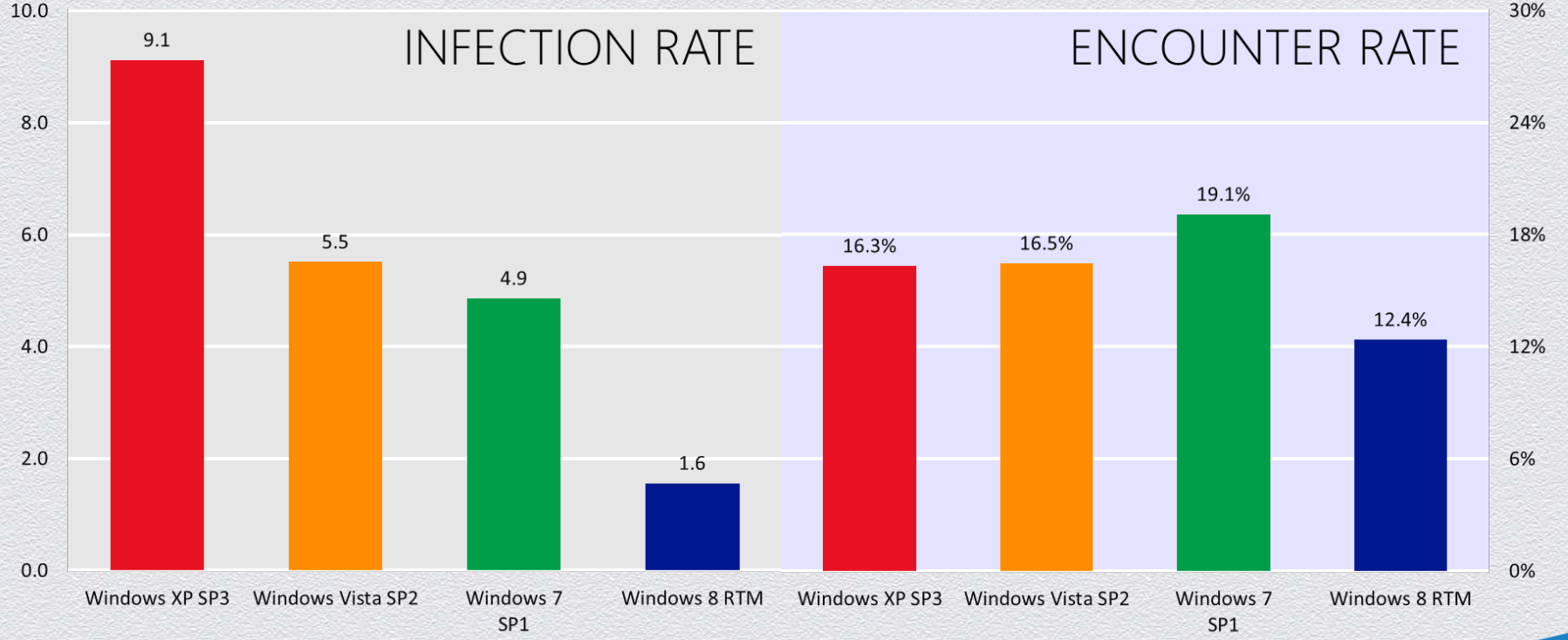


Realtime antivirus: unprotected



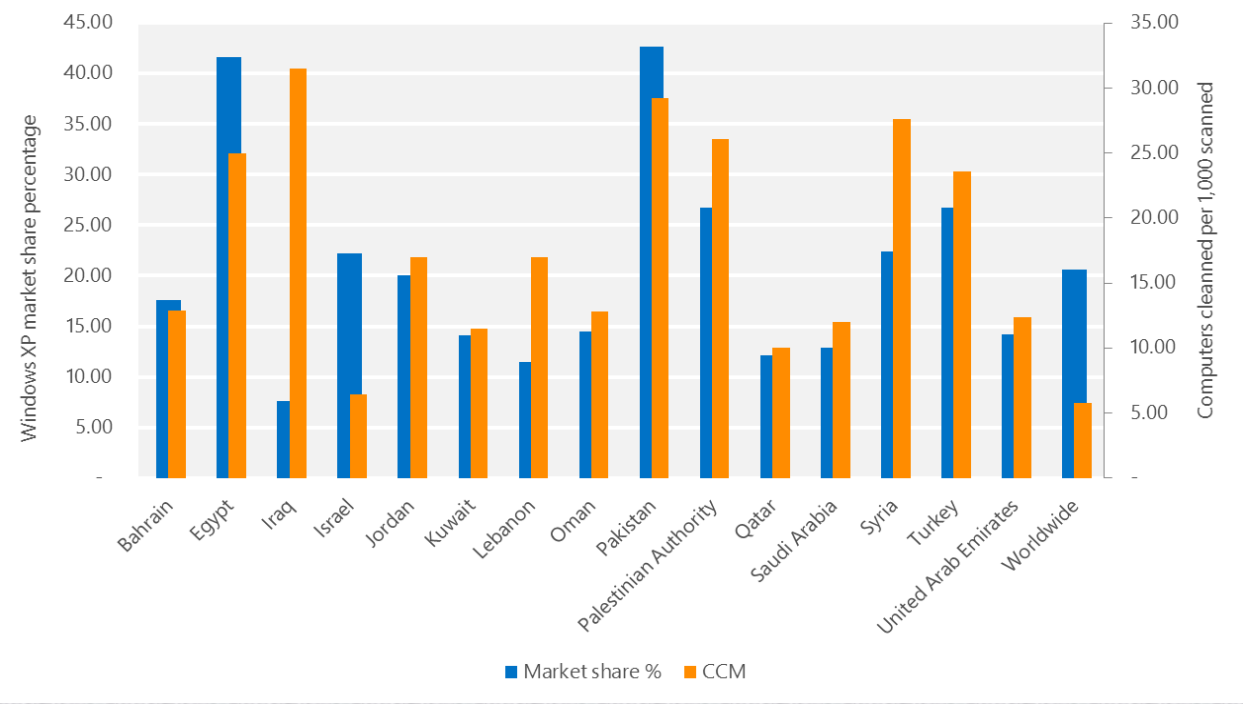
Windows XP usage

Infection and encounter rates: OS, 2Q13



This data is normalized. 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.

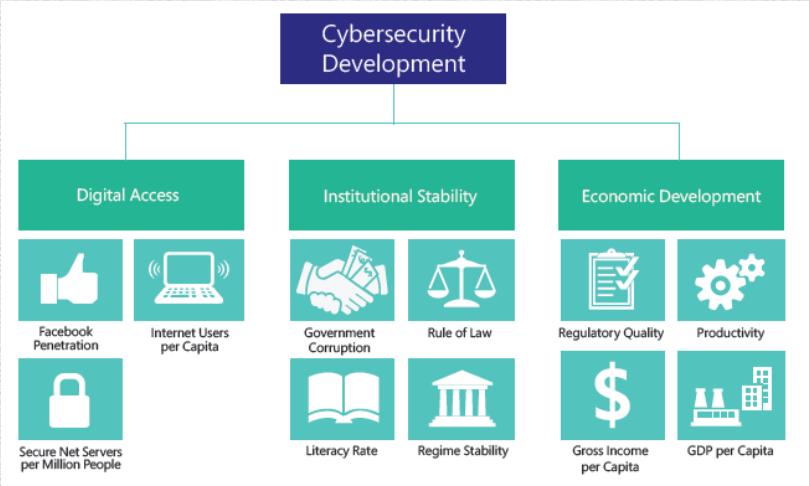
Windows XP market share percentage

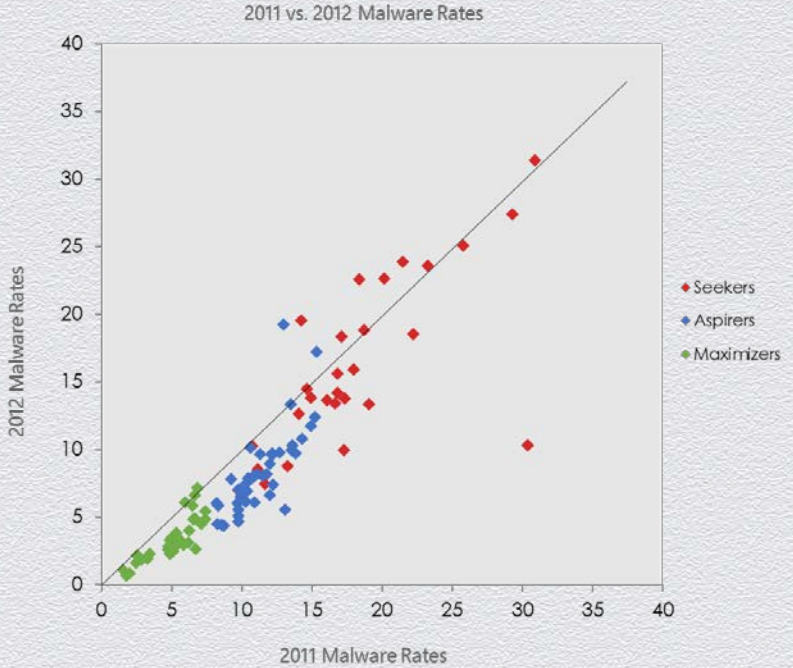


Windows XP Market share %, *source: statcounter.com.* This work by StatCounter is licensed under a Creative Commons Attribution-Share Alike 3.0 Unported License. No changes were made to the content.
CCM, *source: Microsoft Security Intelligence Report, Volume 15*

Socio-economic factors & regional malware infection rates

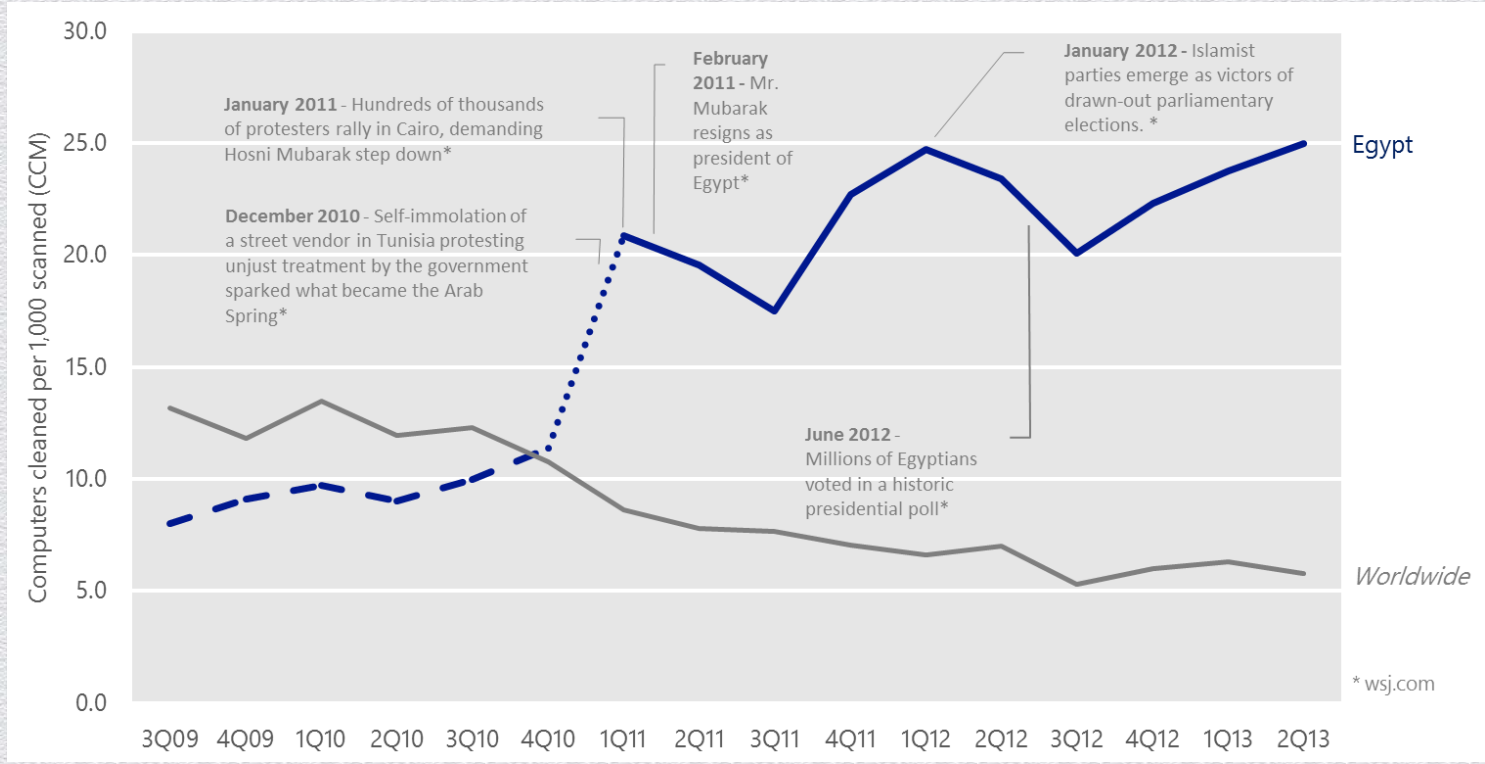
Relationships with cybersecurity





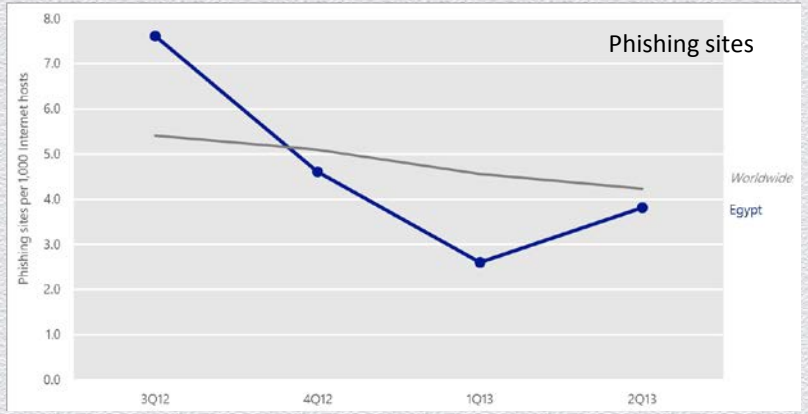
http://bit.ly/1dallZd

Recent events & CCM: Egypt

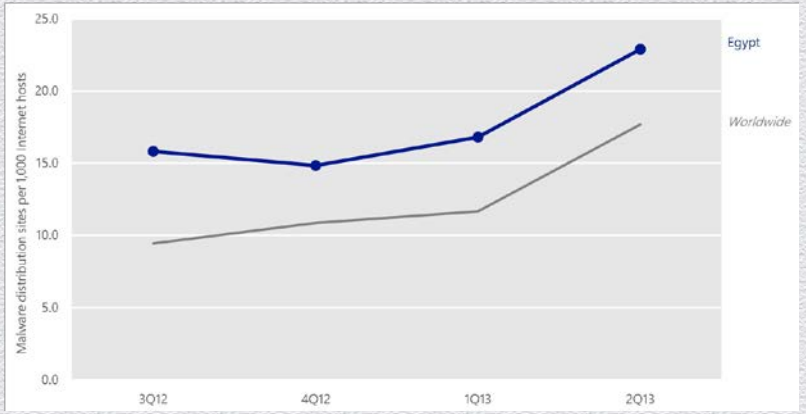


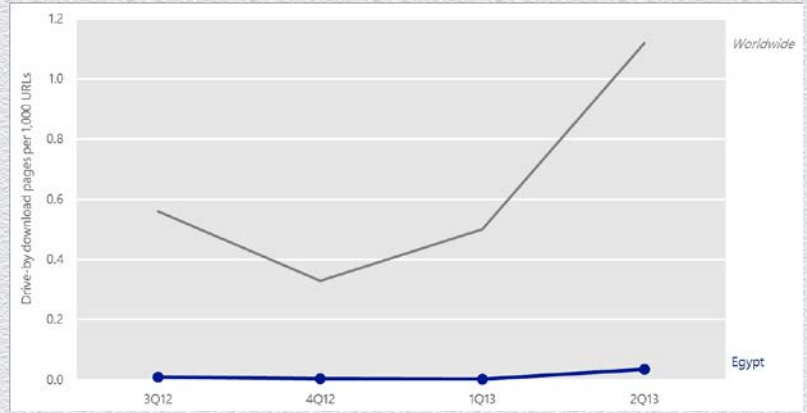
Malicious websites in Egypt

Phishing sites



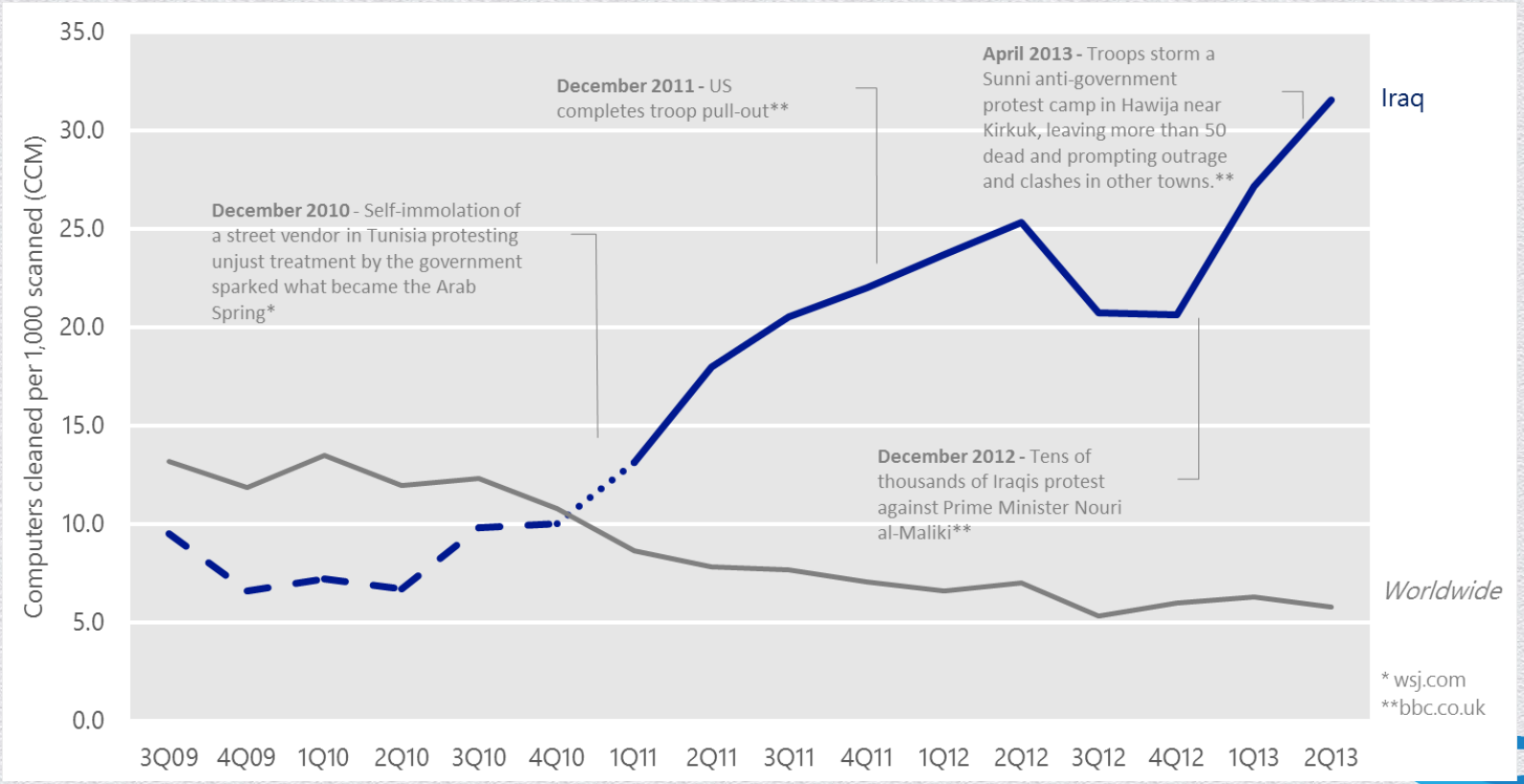
Malware hosting sites





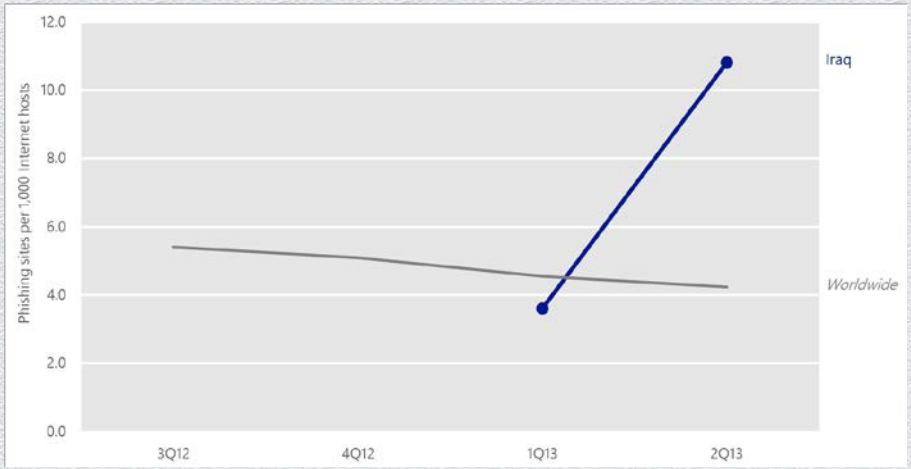
Drive-by download sites

Recent events & CCM: Iraq

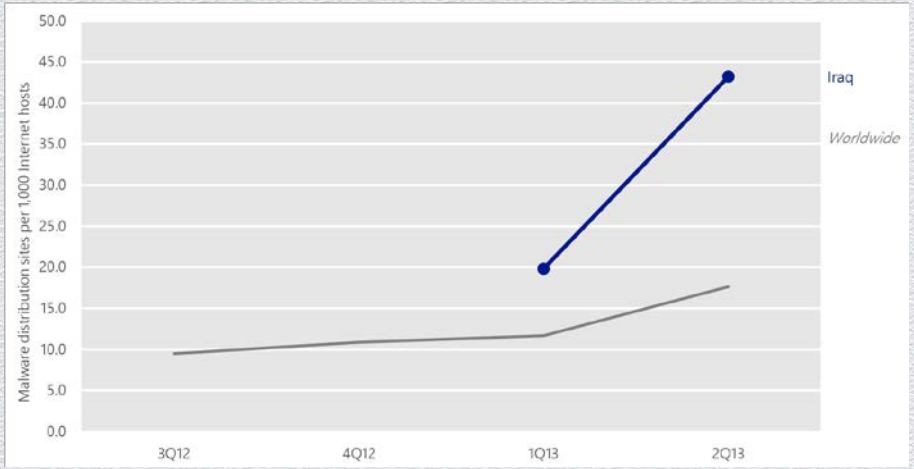


Malicious websites in Iraq

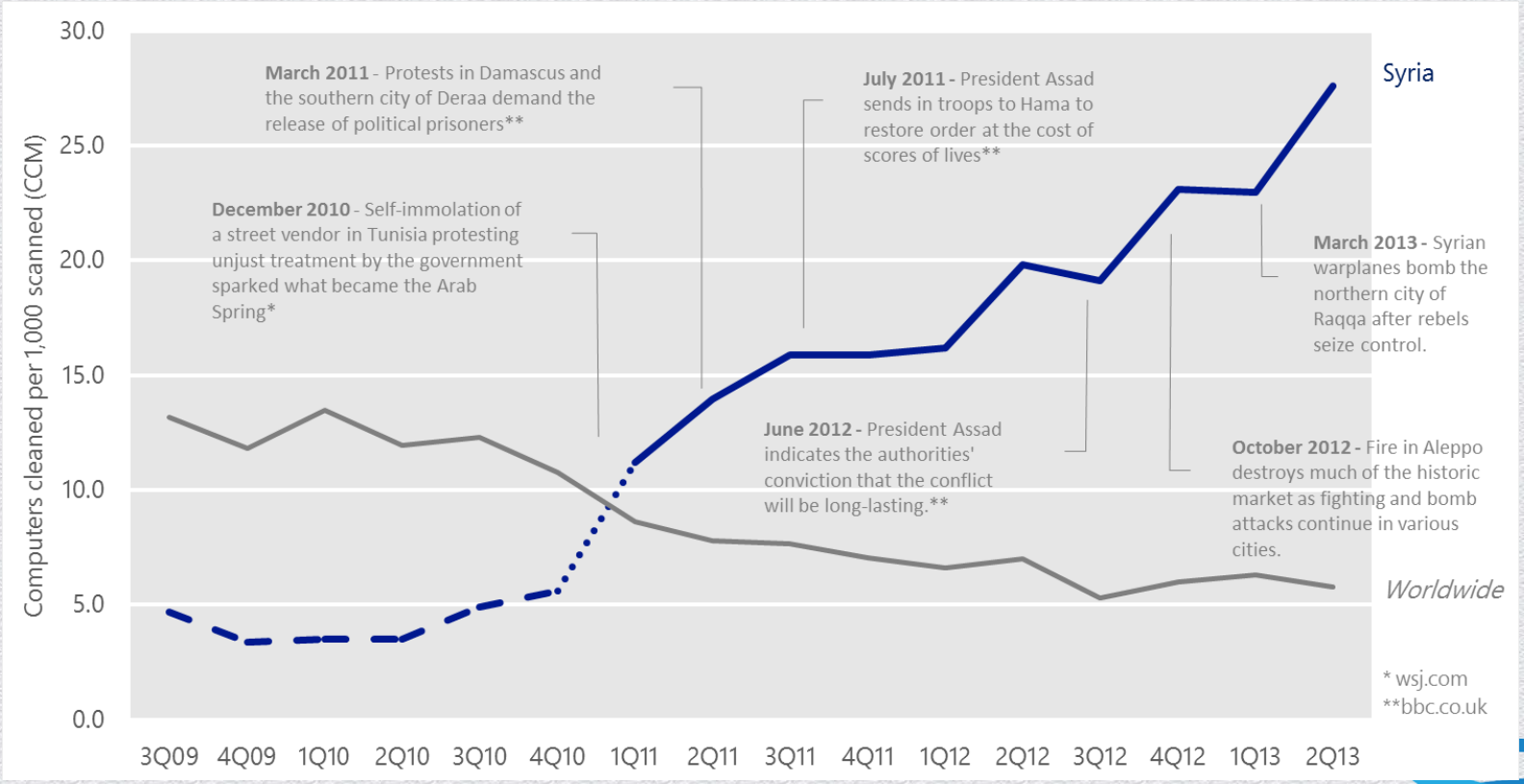
Phishing sites



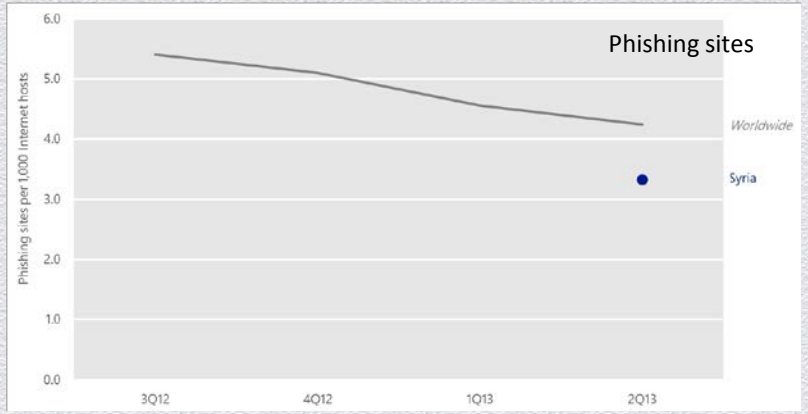
Malware hosting sites

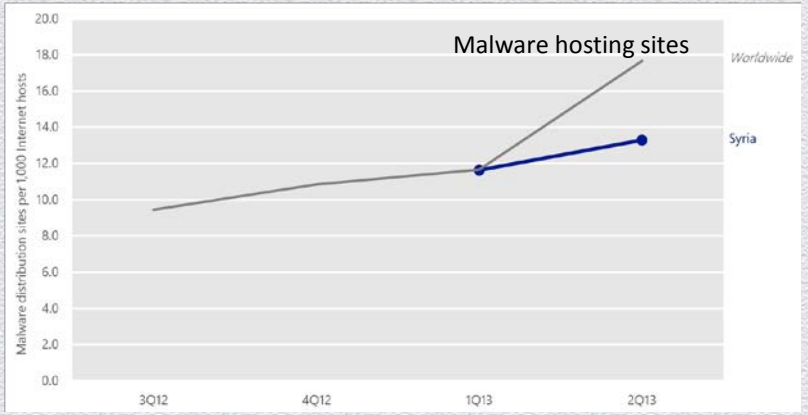


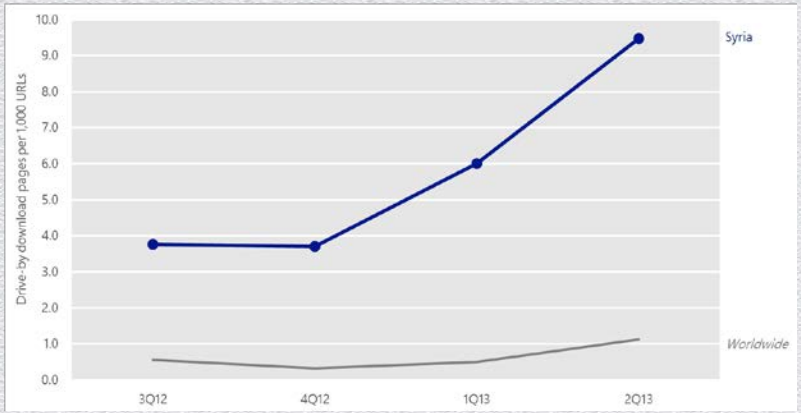
Recent events & CCM: Syria



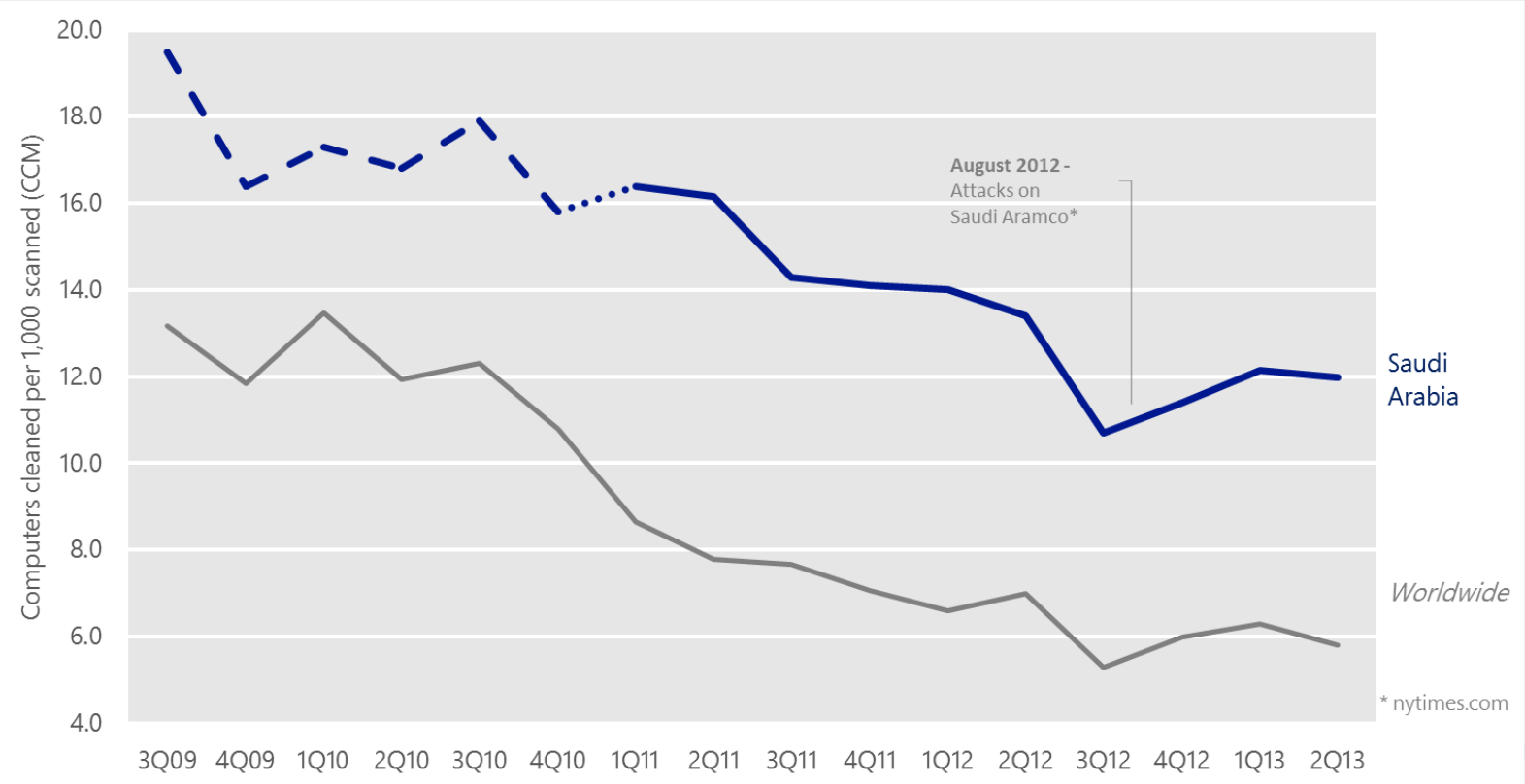
Malicious websites in Syria



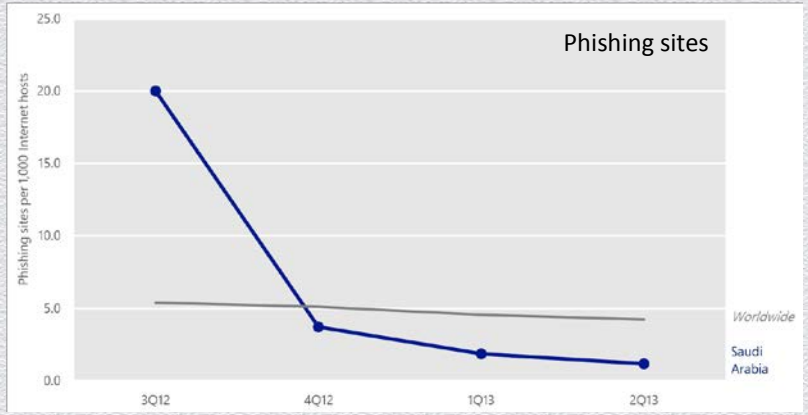


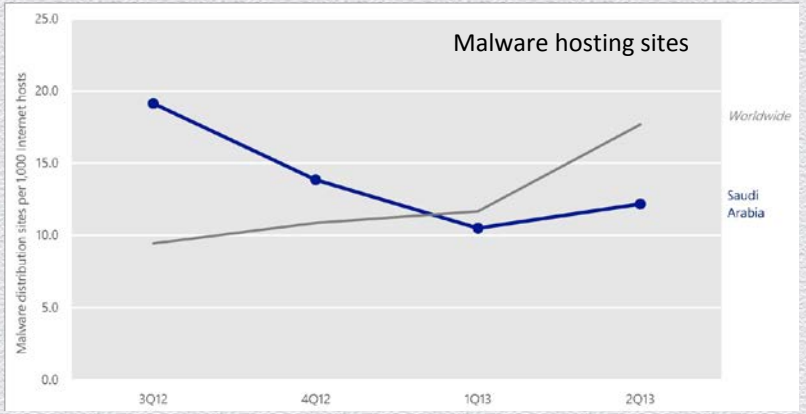


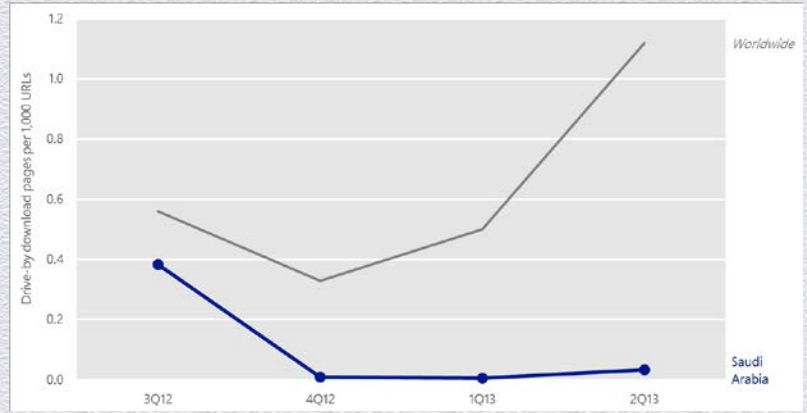
High profile attack & CCM: Saudi Arabia



Malicious websites in Saudi Arabia

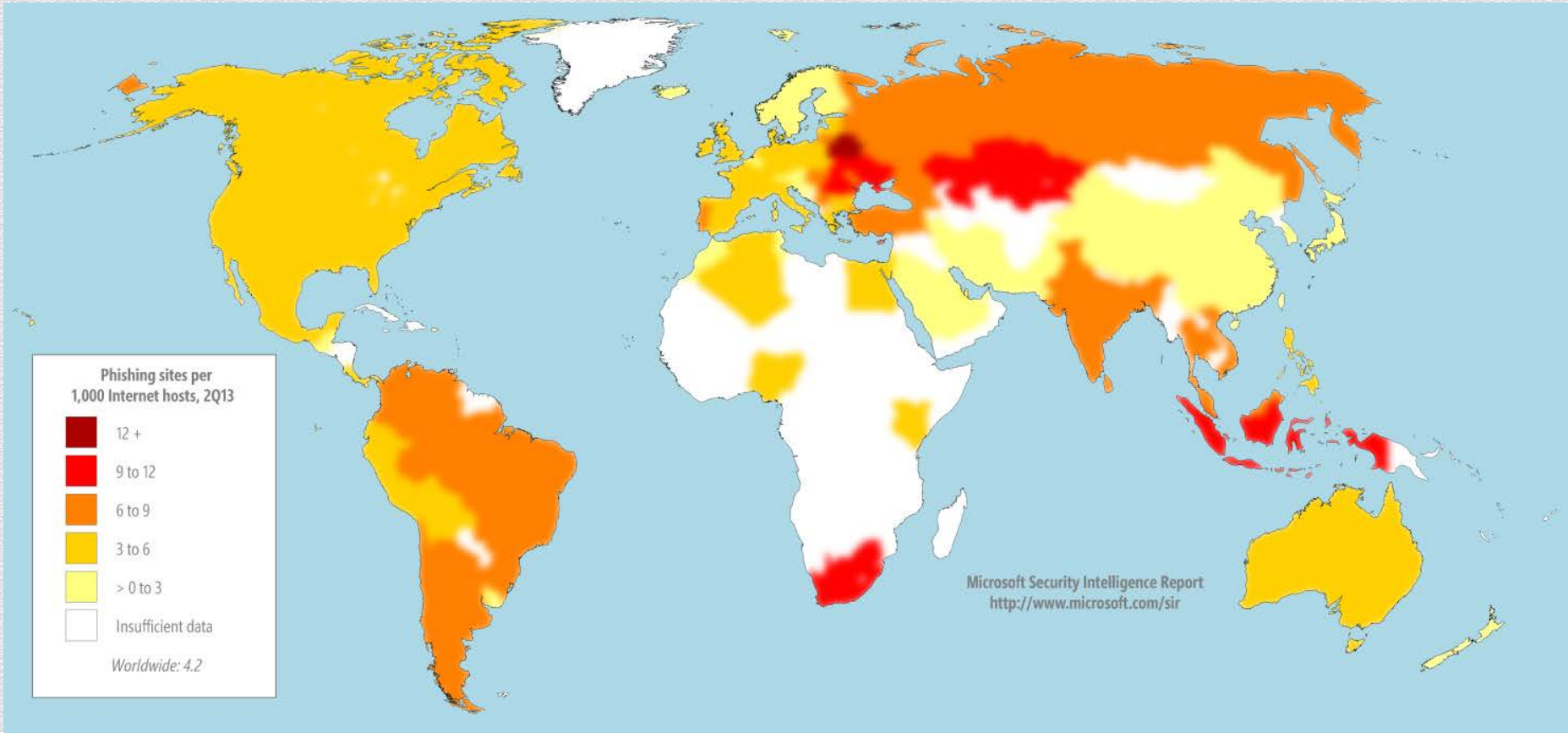




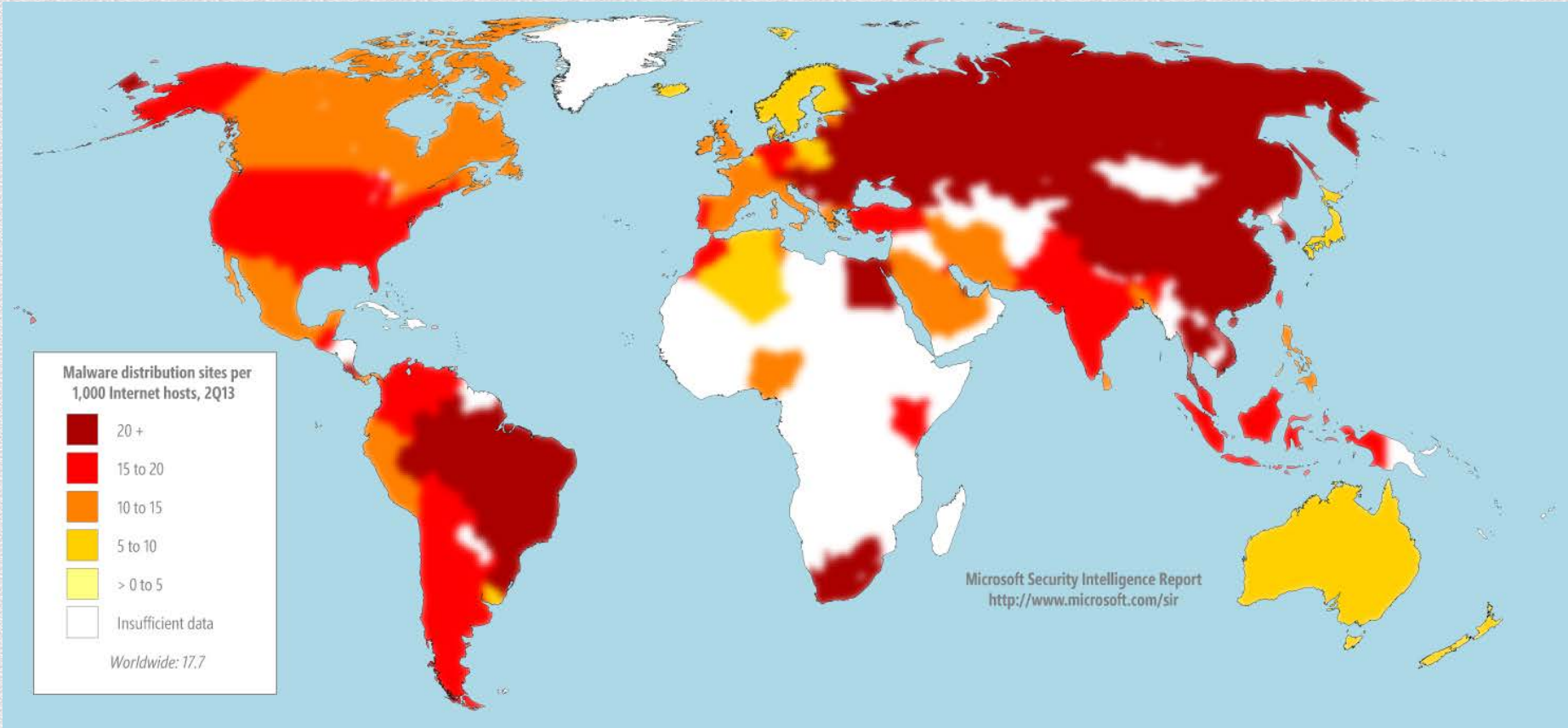


Drive-by download sites

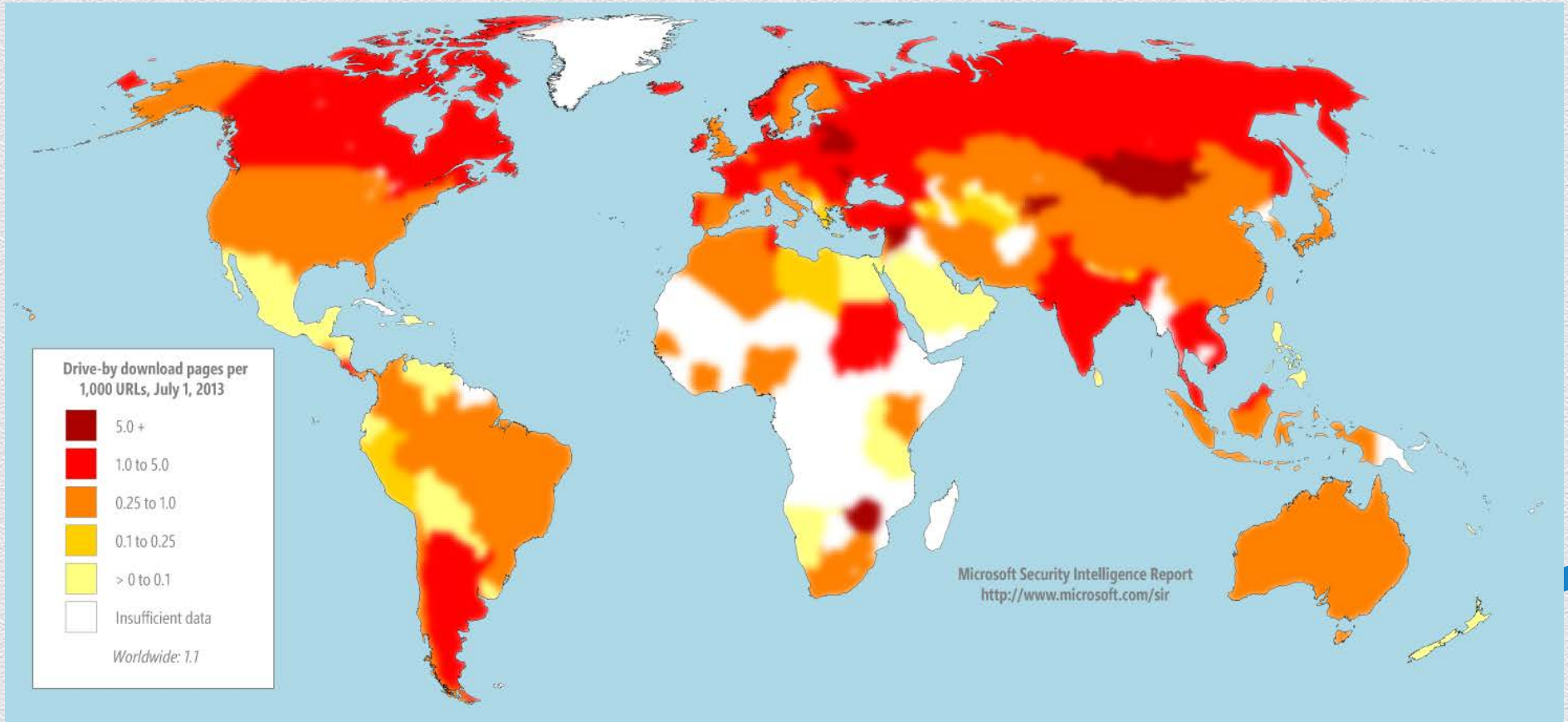
Phishing sites by country or region



Malware distribution sites by country or region

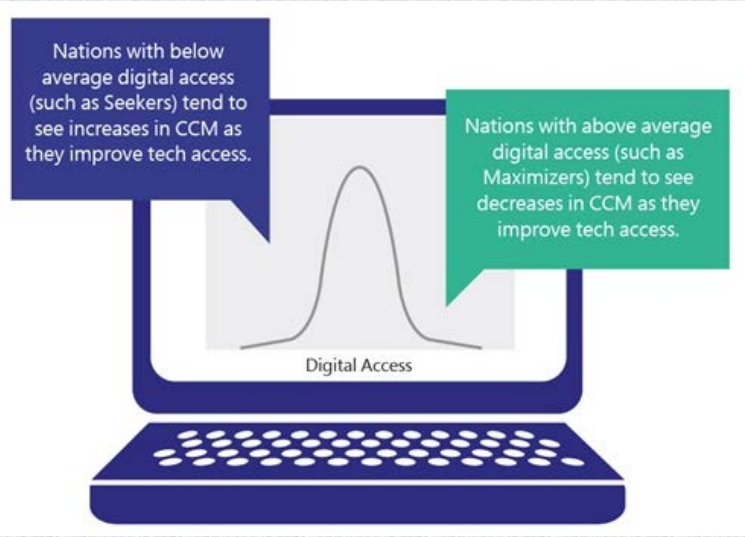


Drive-by downloads by country or region



The Cybersecurity Risk Paradox

2011 Predictors of Digital Access	Technologically Mature Countries (Maximizers)	Seeker Countries
Secure Net Servers/Million People	.19	.86
Broadband Penetration	-.33	.68
Mobile Internet Penetration	-.19	.58
Internet-Enabled PC Ownership	-.34	.20



http://bit.ly/1daIlZd

Best Practices

Best practices of locations with low CCM

- Strong public – private partnerships
- CERTs, ISPs and others actively monitoring for threats in the region
- An IT culture where system administrators respond rapidly to reports of system infections or abuse
- Enforcement policies and active remediation of threats via quarantining infected systems on networks
- Regional education campaigns and media attention
- Low software piracy rates and widespread usage of Windows Update/Microsoft Update
- Consider the Council of Europe Cybercrime treaty and/or the London Action Plan

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