



Cyber Threat Intelligence – messages from the frontlines of Cyber Defense

Robert Kosla, Lt. Col. (Ret.)

Regional Director – Public Safety / National Security / Defense
Microsoft Central and Eastern European Headquarters (CEE HQ)

ISACA Conference

– 23rd of October 2013 – Riga - Latvia

Cyber Defense – Microsoft's Commitment

- Trustworthy Computing @ 10 Years
- Security Development Lifecycle
- Digital Crimes Unit
- Government Security Program
- Security Cooperation Program
- Cyber Defense – Technology View

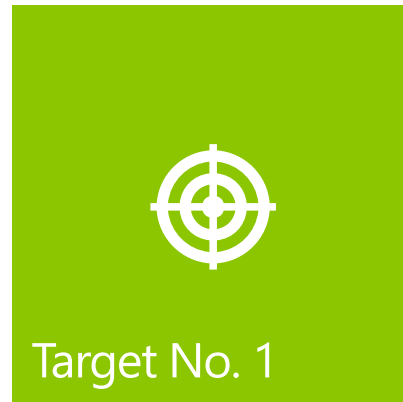
Cybercrimes Front Line – Early Warning Needs

Infrastructure Impact

80% of world's critical infrastructures
Determined, resourceful, global adversaries

Targeted Resources

Attacked > 40,000 times a day
At least one DDoS a day
Logged attacks from every country



Industry Value to Cyber Defense

Detecting Threats

Advanced tools to find new attacks
Deep expertise hunting for the Determined Human Adversary

Innovative Mitigations

Hardening existing assets
New approaches to counter threats

Custom Approach

Specialized software development guidance
Integrate the Security Development Lifecycle into Cybercrime Center environment development



Cybersecurity Practice



Global Reach and Delivery with World Class Architects, Consultants, and Engineers



Sensors & Intelligence



Response & Investigation



Recovery & Mitigations



Architecture & Advisory



Expert SDL Developer Services



Advanced Programs

Enabling End to End Trust – Microsoft View



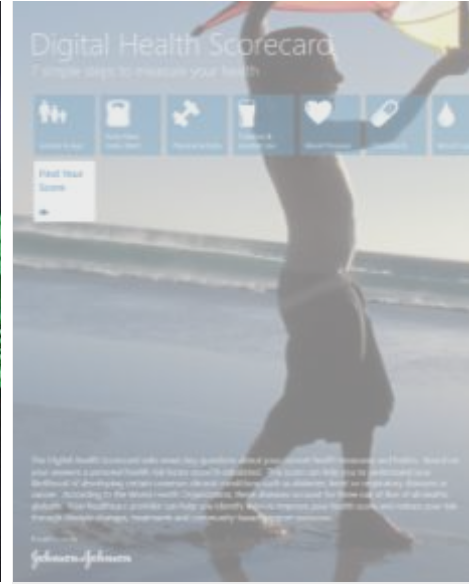
Trusted People



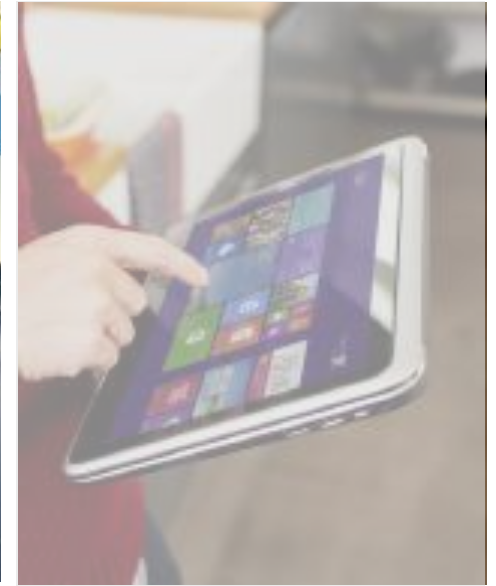
Trusted Devices



Trusted OS



Trusted Software



Trusted Data

Trusted Platform

Microsoft Cyber Defense Resources

Trustworthy Computing Security



- Security Science
- Microsoft Security Response Center

Microsoft Malware Prevention Center



- Malware analysis
- Anti-malware capabilities

Microsoft Product Development



- Product architecture & engineering insight

Customer Service & Support - Cybersecurity



- Diagnosis and technical investigation
- IT ecosystem viewpoint

- PRODUCT EXPERTISE
- THREAT INTELLIGENCE
- PROVEN PRACTICES





Global view to Global
Cyber Threats –
Microsoft
Intelligence – SIR
Report vol. 14

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

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.

About SIRv14

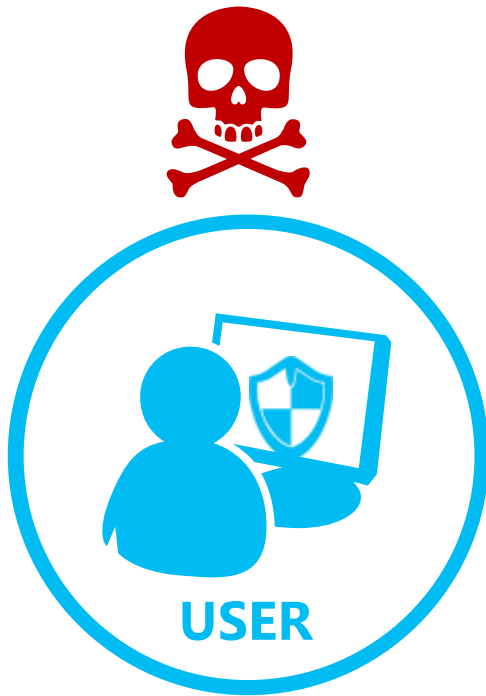


Product name	Main customer segment		Malicious software		Spyware and potentially unwanted software		Available at no additional charge	Main distribution methods
	Consumers	Business	Scan and remove	Real-time protection	Scan and remove	Real-time protection		
Windows Malicious Software Removal Tool	•		Prevalent 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

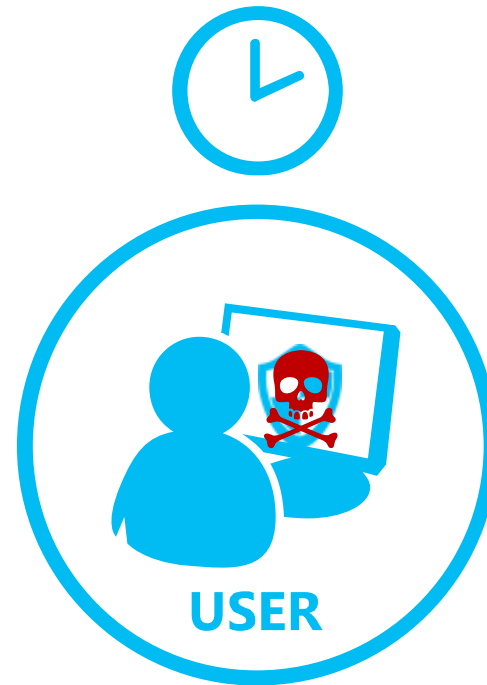
Introduction

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

Why some users are not running an up-to-date real-time antimalware solution



Scenario 1: malware disables real-time antimalware to 'stay quiet'

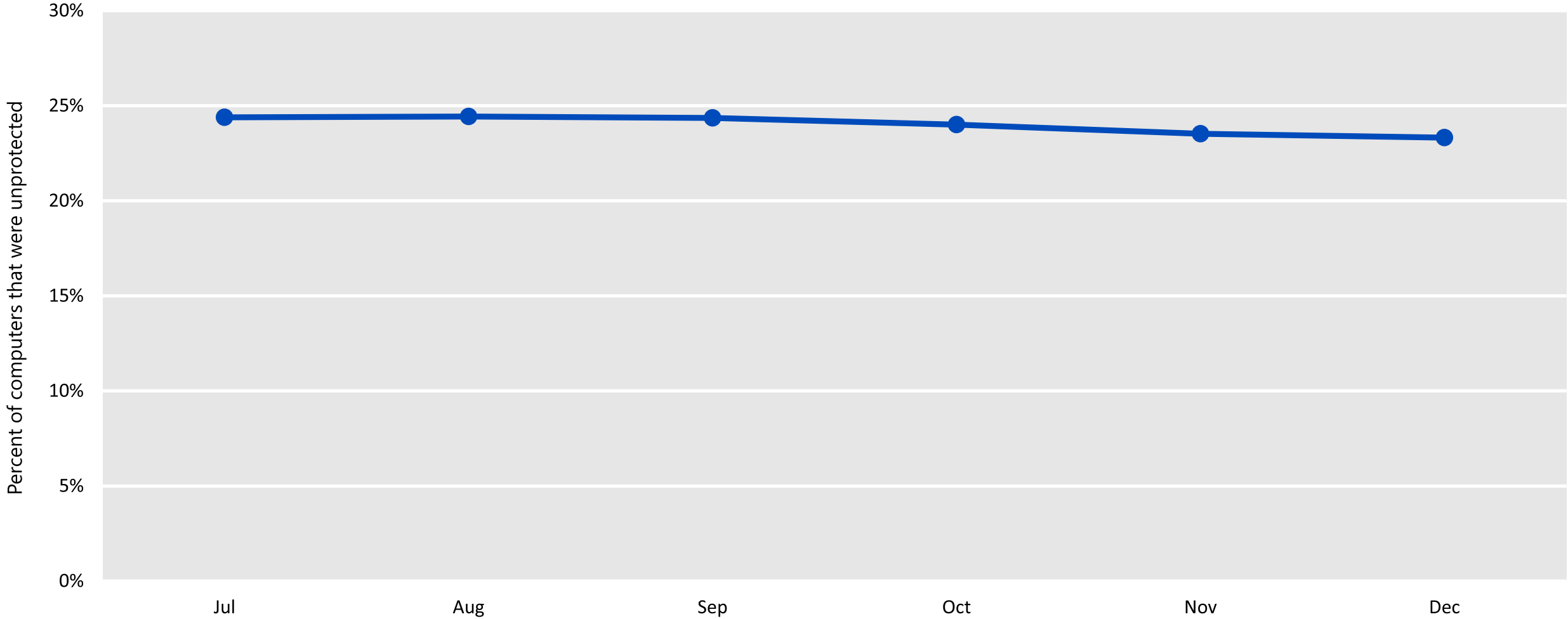


Scenario 2: user disables real-time antimalware because of perceived performance improvements



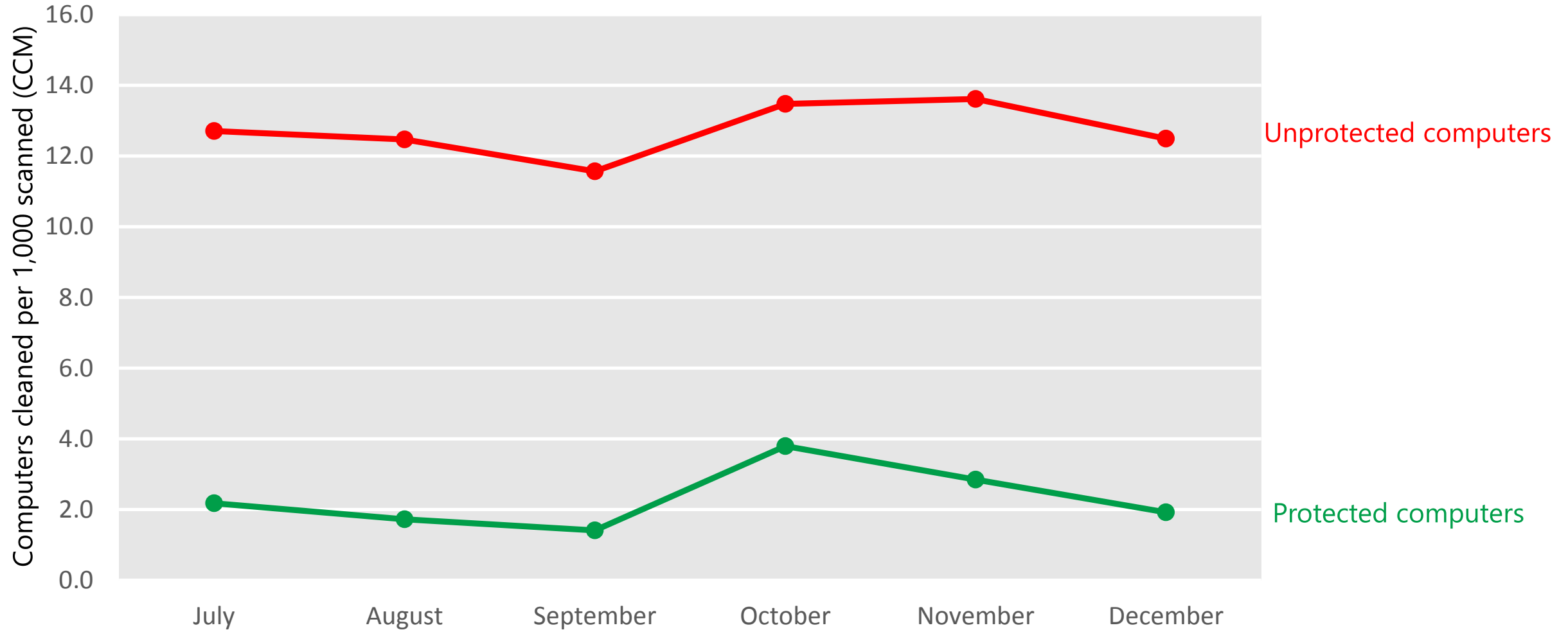
Scenario 3: subscription lapses

Computers lacking up-to-date real-time antimalware protection



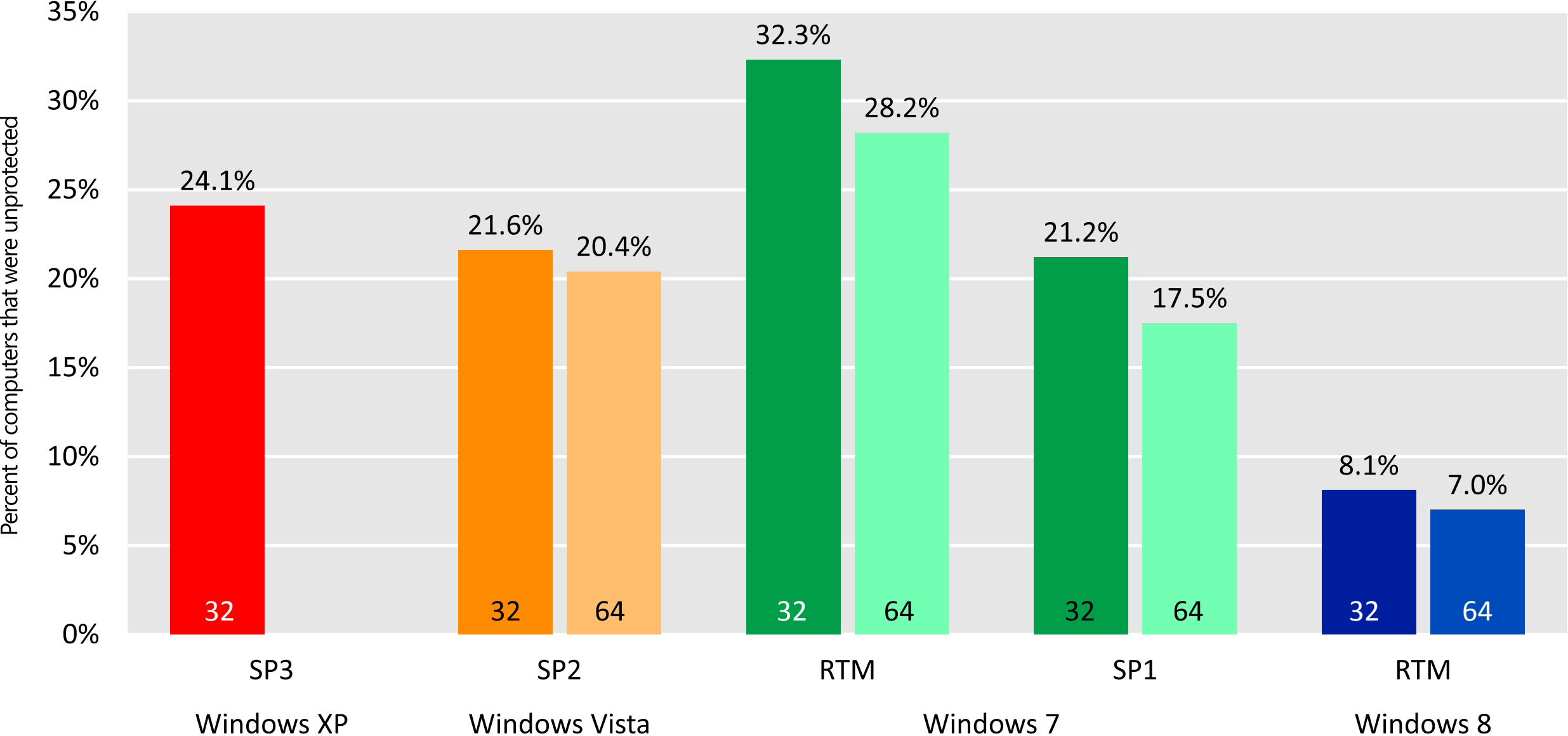
On average, about 24 percent of computers scanned by the MSRT each month in 2H12 were not running real-time antimalware software at the time they were scanned

Infection rates for protected and unprotected computers

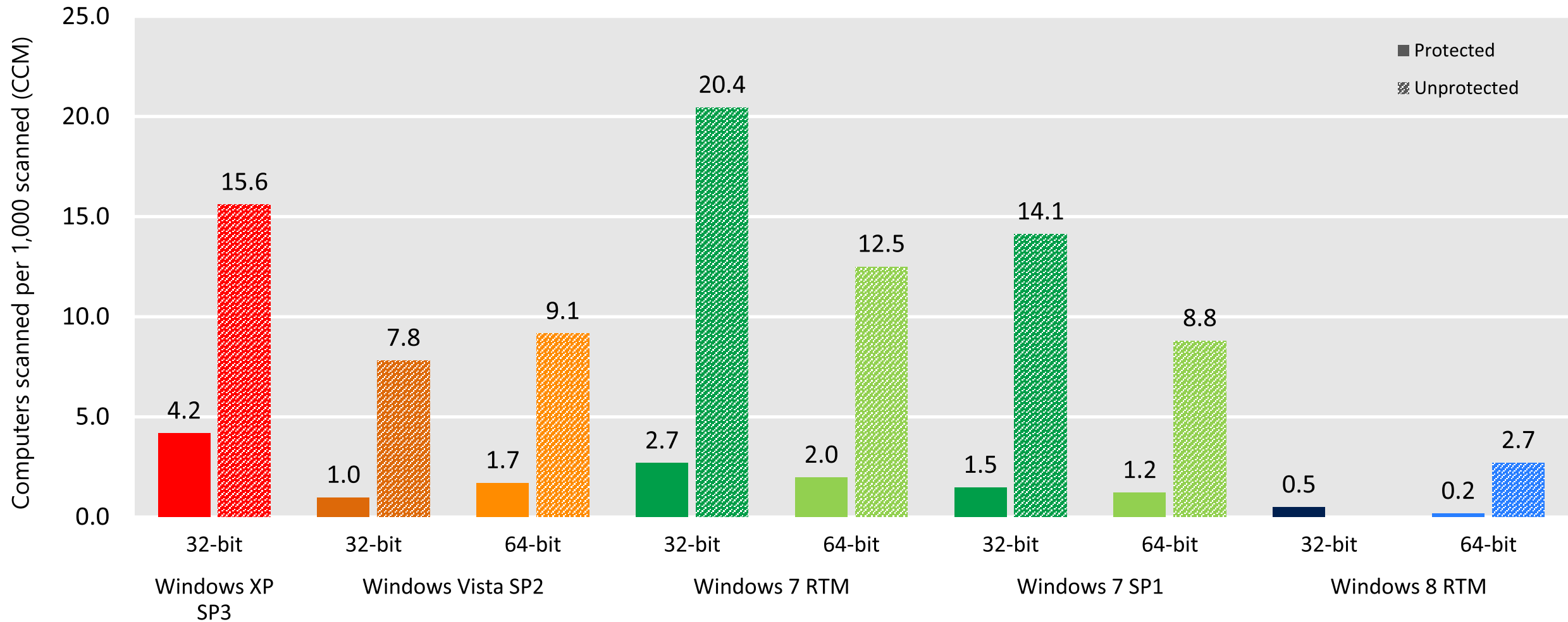


Computers without up-to-date real-time antimalware protection were 5.5 times more likely on average to report malware infections each month than computers with protection

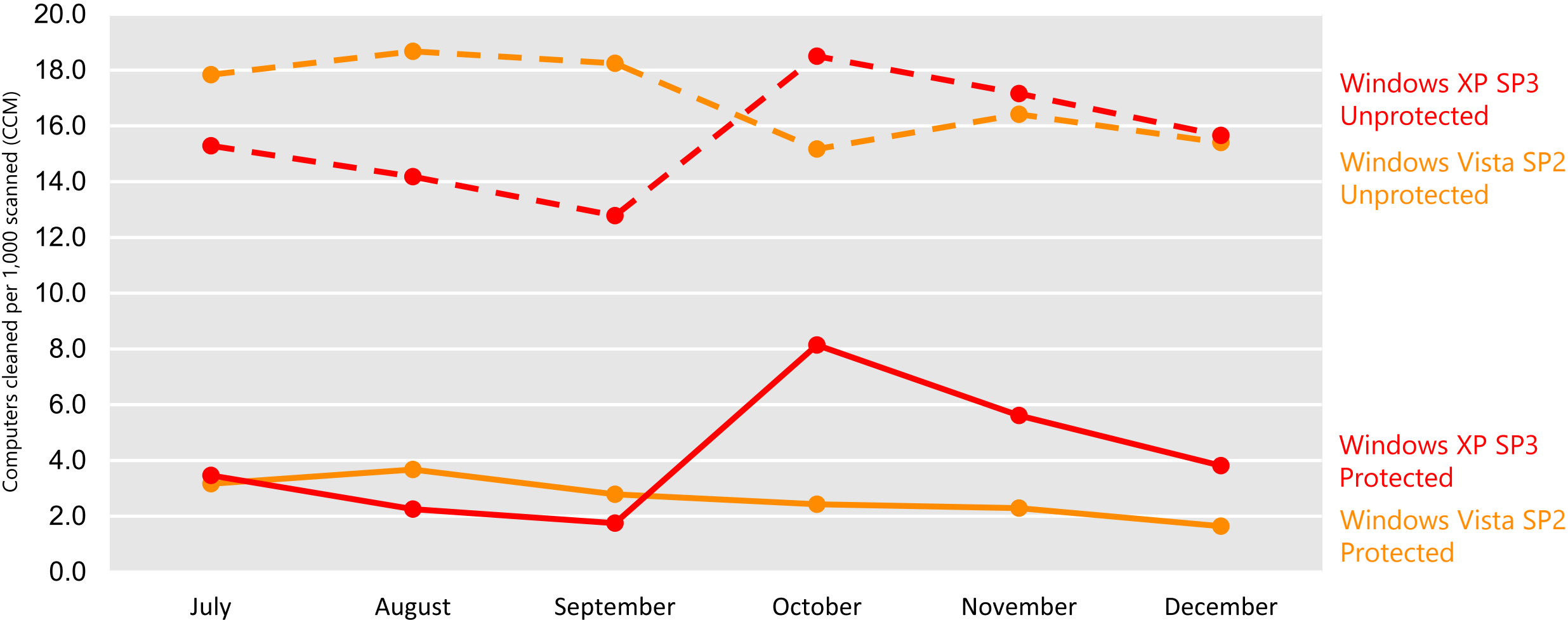
Computers lacking up-to-date real-time antimalware protection by OS



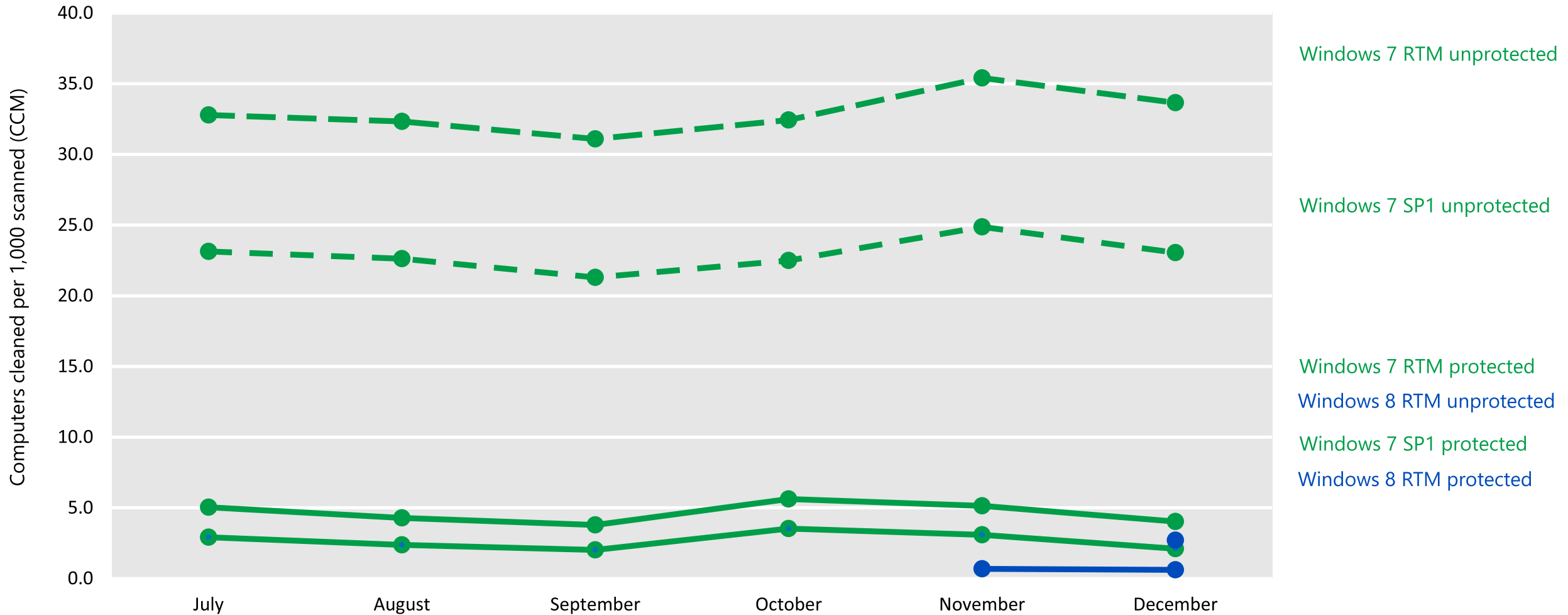
Infection rates for computers with and without up-to-date real-time antimalware protection



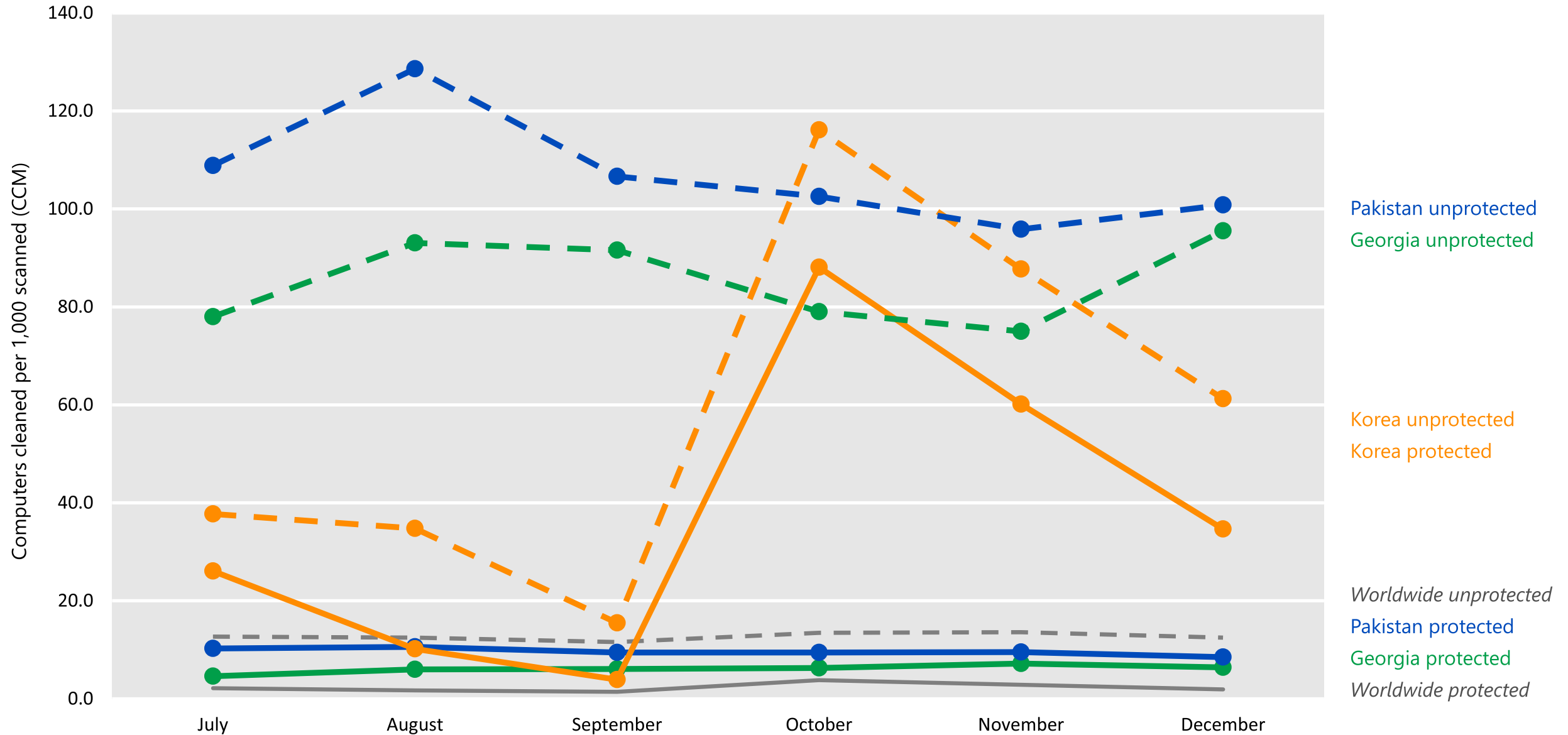
Infection rates for computers running Windows XP and Windows Vista



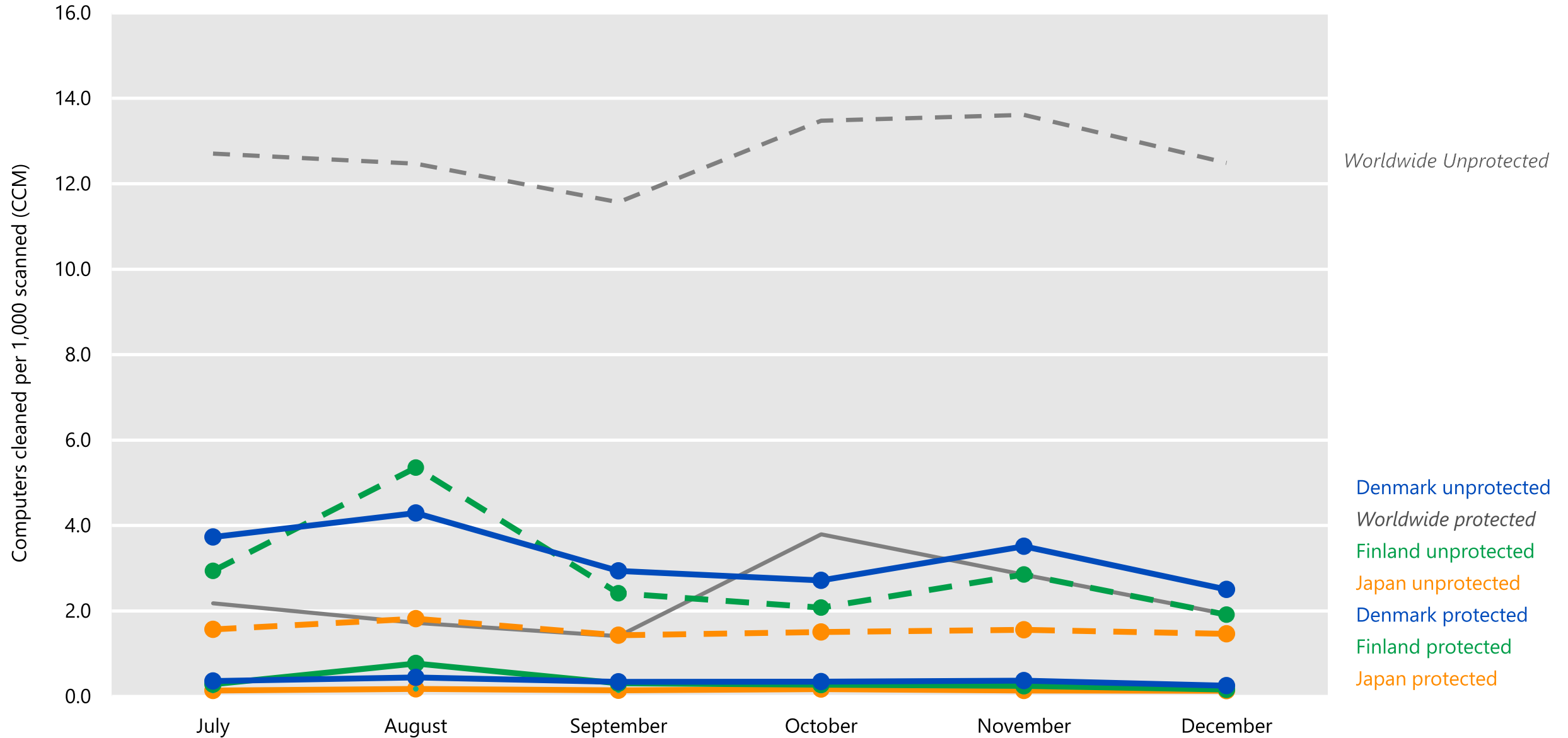
Infection rates for computers running Windows 7 and Windows 8



Infection rates in three locations with high CCM



Infection rates in three locations with low CCM



Guidance

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

Latvia in SIRv14 – Infection Rate

- The statistics presented here are generated by Microsoft security programs and services running on computers in Slovakia in 4Q12 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region

Infection rate statistics for Latvia

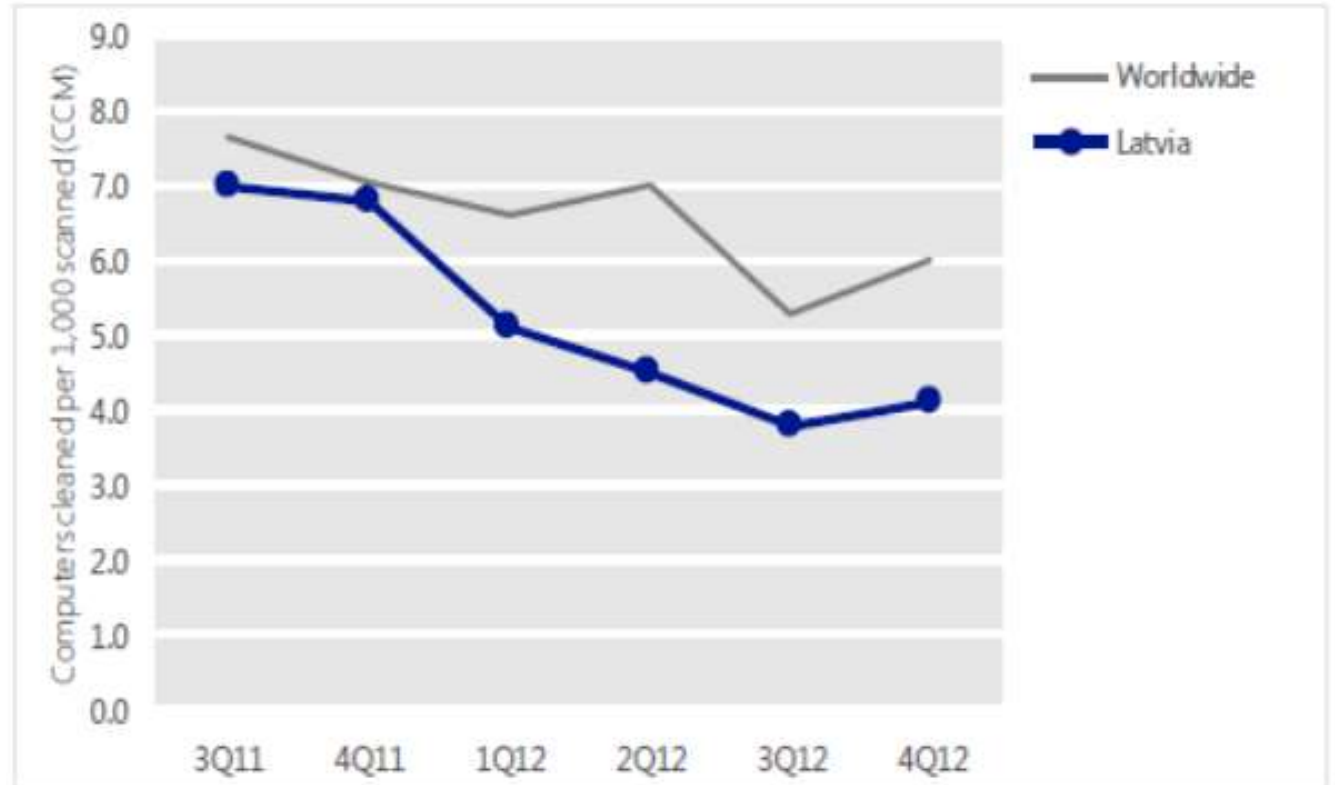
Metric	1Q12	2Q12	3Q12	4Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.1	4.5	3.8	4.1
Worldwide average CCM	6.6	7.0	5.3	6.0

- See the Security Intelligence Report website at www.microsoft.com/sir for more information about threats in Latvia and around the world, and for explanations of the methods and terms used here

Latvia in SIRv14 – Infection Trends

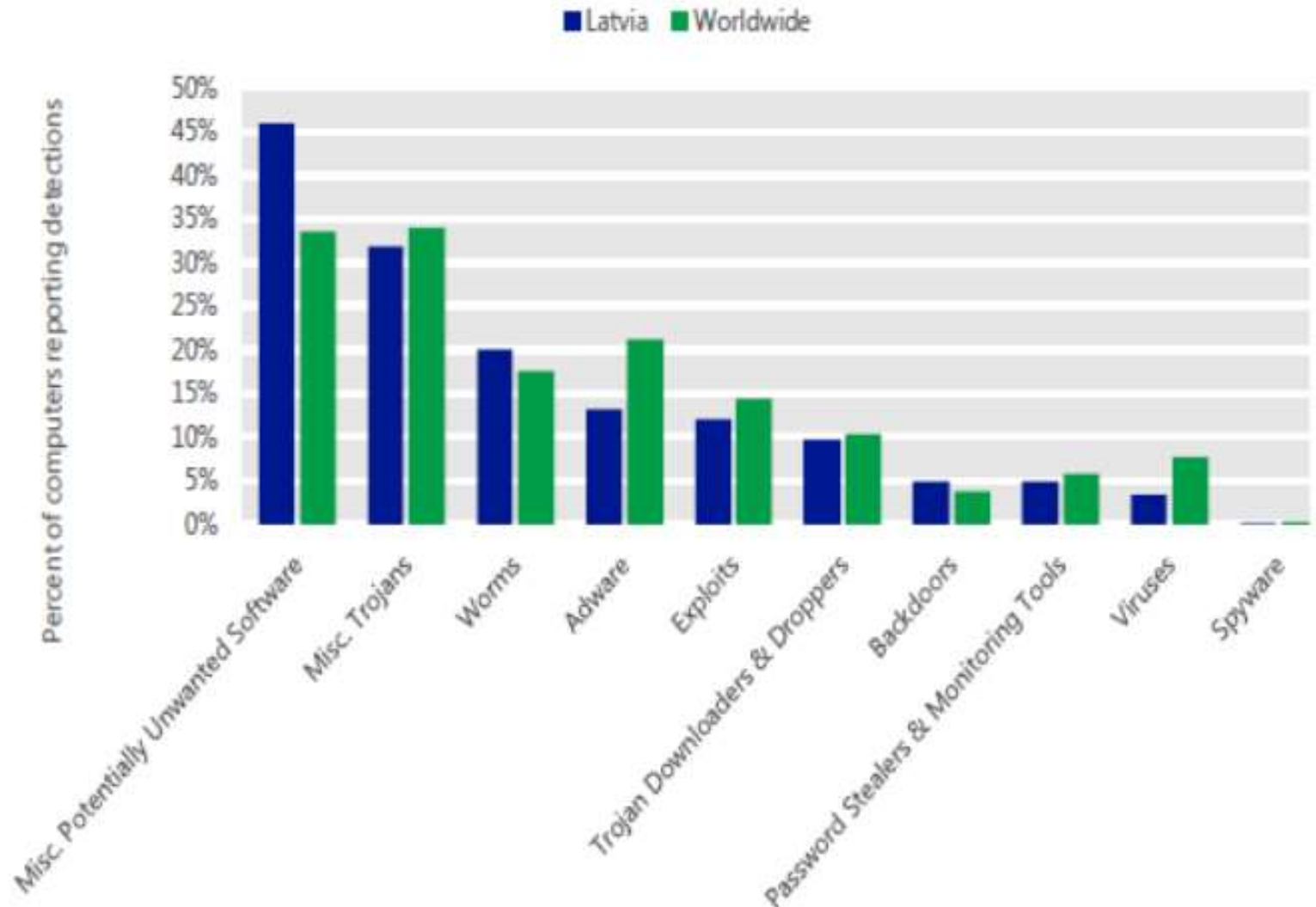
- The MSRT detected malware on 4.1 of every 1,000 computers scanned in Latvia in 4Q12 (a CCM score of 4.1, compared to the 4Q12 worldwide average CCM of 6.0)
- The figure shows the CCM trend for Latvia over the last six quarters, compared to the world as a whole

CCM infection trends in Latvia and worldwide



Latvia in SIRv14 – Threat Categories

- The most common category in Latvia in 4Q12 was **Miscellaneous Potentially Unwanted Software**. It affected 45.9 percent of all computers with detections there, up from 45.6 percent in 3Q12
- The second most common category in Latvia in 4Q12 was **Miscellaneous Trojans**. It affected 31.9 percent of all computers with detections there, down from 28.7 percent in 3Q12.
- The third most common category in Latvia in 4Q12 was **Adware**, which affected 20.1 percent of all computers with detections there, down from 14.1 percent in 3Q12.



Latvia in SIRv14 – Threat Families

- The most common threat family in Latvia in 4Q12 was [Win32/Keygen](#), which affected 21.2 percent of computers with detections in Latvia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products
- The second most common threat family in Latvia in 4Q12 was [Win32/Dorkbot](#), which affected 7.7 percent of computers with detections in Latvia. [Win32/Dorkbot](#) is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits
- The third most common threat family in Latvia in 4Q12 was [Win32/Obfuscator](#), which affected 7.3 percent of computers with detections in Latvia. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques

The top 10 malware and potentially unwanted software families in Latvia in 4Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	21.2%
2	Win32/Dorkbot	Worms	7.7%
3	Win32/Obfuscator	Misc. Potentially Unwanted Software	7.3%
4	JS/IframeRef	Misc. Trojans	7.2%
5	INF/Autorun	Misc. Potentially Unwanted Software	5.1%
6	Java/Blacole	Exploits	4.9%
7	Win32/Pdfjsc	Exploits	4.7%
8	Win32/Hotbar	Adware	4.0%
9	Win32/Pameseg	Misc. Potentially Unwanted Software	3.7%
10	Win32/Wpakill	Misc. Potentially Unwanted Software	3.6%

Latvia in SIRv14 – Malicious Websites

- Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm
- The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected

Malicious website statistics for Latvia

Metric	3Q12	4Q12
Phishing sites per 1,000 hosts (Worldwide)	3.85 (5.41)	5.43 (5.10)
Malware hosting sites per 1,000 hosts (Worldwide)	8.06 (9.46)	13.66 (10.85)
Drive-by download per 1,000 URLs (Worldwide)	0.51 (0.56)	1.52 (0.33)



Cyber Threats vs. Updated Software

- Retire
Windows XP

Get value today. Get modern.

Eliminate risks of Windows XP
End of Support

Deployment tools and services
available to assist in migration

APRIL 8, 2014

On **April 8, 2014** Windows XP will reach the end of support lifecycle and will no longer be supported.

**Windows XP
Launch**

October
2001

**Windows XP SP3
Launch**

April
2008

**Windows XP SP3
End of Support**

**April 8
2014**

Thank you for being a Windows XP User!

How security & threats evolved since 1995...

Key Threats

- Internet was just growing
- Mail was on the verge

1995

Windows 95

- -

Key Threats

- Melissa (1999), Love Letter (2000)
- Mainly leveraging social engineering

2001

Windows XP

- Logon (Ctrl+Alt+Del)
- Access Control
- User Profiles
- Security Policy
- Encrypting File System (File Based)
- Smartcard and PKI Support
- Windows Update

Key Threats

- Code Red and Nimda (2001), Blaster (2003), Slammer (2003)
- 9/11
- Mainly exploiting buffer overflows
- Script kiddies
- Time from patch to exploit: Several days to weeks

2004

Windows XP SP2

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Security Development Lifecycle (SDL)
- Auto Update on by Default
- Firewall on by Default
- Windows Security Center
- WPA Support

Key Threats

- Zotob (2005)
- Attacks «moving up the stack» (Summer of Office 0-day)
- Rootkits
- Exploitation of Buffer Overflows
- Script Kiddies
- Raise of Phishing
- User running as Admin

2007

Windows Vista

- Bitlocker
- Patchguard
- Improved ASLR and DEP
- Full SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Firewall improvements
- Signed Device Driver Requirements
- TPM Support
- Windows Integrity Levels
- Secure "by default" configuration (Windows features and IE)

Key Threats

- Organized Crime
- Botnets
- Identity Theft
- Conficker (2008)
- Time from patch to exploit: days

2009

Windows 7

- Improved ASLR and DEP
- Full SDL
- Improved IPSec stack
- Managed Service Accounts
- Improved User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

Key Threats

- Organized Crime, potential state actors
- Sophisticated Targeted Attacks
- Operation Aurora (2009)
- Stuxnet (2010)

2012

Windows 8

- UEFI (Secure Boot)
- Firmware Based TPM
- Trusted Boot (w/ELAM)
- Measured Boot and Remote Attestation Support
- Significant Improvements to ASLR and DEP
- AppContainer
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- Application Reputation moved into Core OS
- BitLocker: Encrypted Hard Drive and Used Disk Space Only Encryption Support
- Virtual Smartcard
- Picture Password, PIN
- Dynamic Access Control
- Built-in Anti-Virus

How security & threats evolved... until 2013

Key Threats

- Melissa (1999), Love Letter (2000)
- Mainly leveraging social engineering

2001

Windows XP

- Logon (Ctrl+Alt+Del)
- Access Control
- User Profiles
- Security Policy
- Encrypting File System (File Based)
- Smartcard and PKI Support
- Windows Update

Key Threats

- Code Red and Nimda (2001), Blaster (2003), Slammer (2003)
- 9/11
- Mainly exploiting buffer overflows
- Script kiddies
- Time from patch to exploit: Several days to weeks

2004

Windows XP SP2

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Security Development Lifecycle (SDL)
- Auto Update on by Default
- Firewall on by Default
- Windows Security Center
- WPA Support

Key Threats

- Zotob (2005)
- Attacks «moving up the stack» (Summer of Office 0-day)
- Rootkits
- Exploitation of Buffer Overflows
- Script Kiddies
- Raise of Phishing
- User running as Admin

2007

Windows Vista

- BitLocker
- Patchguard
- Improved ASLR and DEP
- Full SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Firewall improvements
- Signed Device Driver Requirements
- TPM Support
- Windows Integrity Levels
- Secure "by default" configuration (Windows features and IE)

Key Threats

- Organized Crime
- Botnets
- Identity Theft
- Conficker (2008)
- Time from patch to exploit: days

2009

Windows 7

- Improved ASLR and DEP
- Full SDL
- Improved IPSec stack
- Managed Service Accounts
- Improved User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

Key Threats

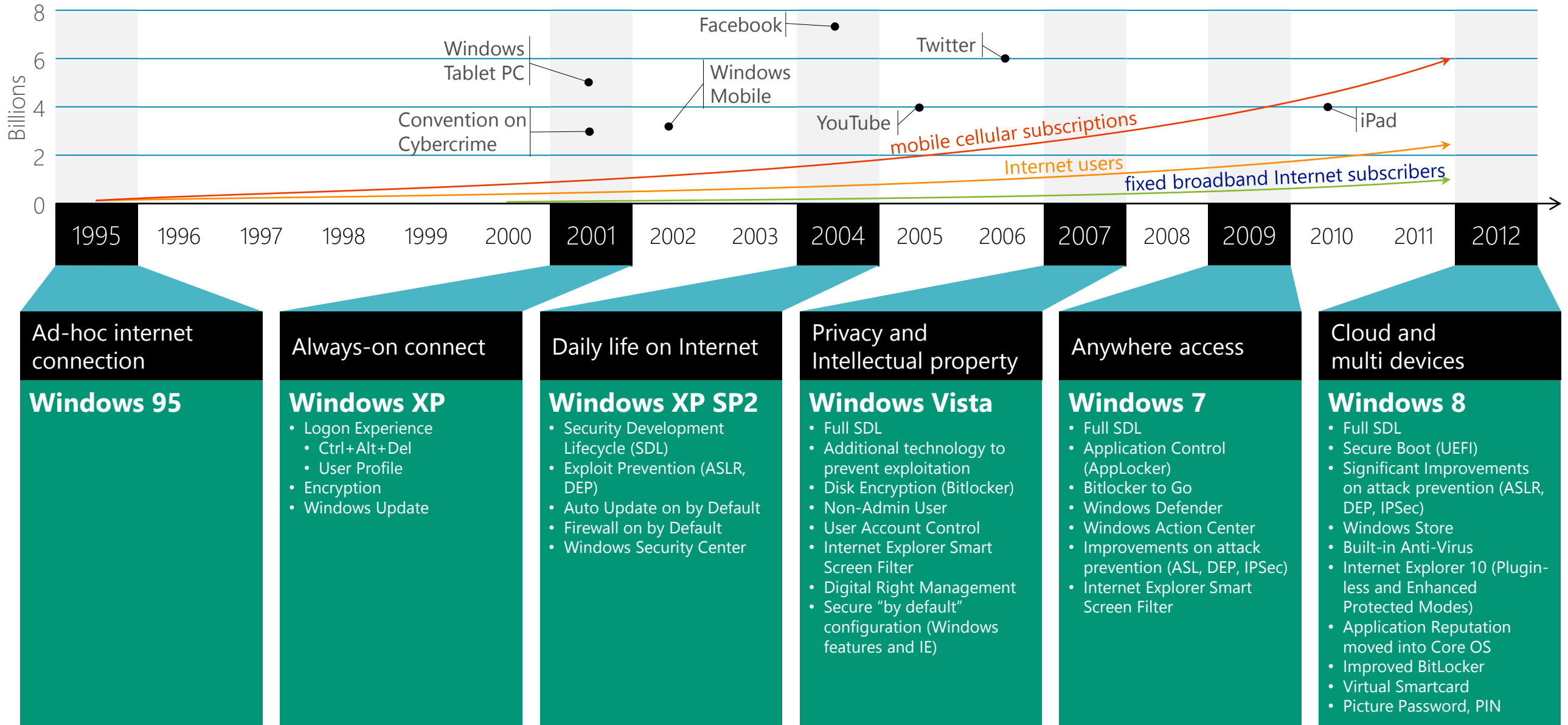
- Organized Crime, potential state actors
- Sophisticated Targeted Attacks
- Operation Aurora (2009)
- Stuxnet (2010)
- Passwords under attack
- Digital identity theft and misuse
- Signatures based AV unable to keep up
- Digital signature tampering
- Browser plug-in exploits
- Data loss on BYOD devices

2013

Windows 8.1

- UEFI (Secure Boot)
- Firmware Based TPM
- Trusted Boot (w/ELAM)
- Measured Boot and Remote Attestation Support
- Significant Improvements to ASLR and DEP
- AppContainer
- TPM Key Protection
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- Application Reputation moved into Core OS
- BitLocker: Encrypted Hard Drive and Used Disk Space Only Encryption Support
- Virtual Smartcard
- Picture Password, PIN
- Dynamic Access Control
- Built-in Anti-Virus
- Touch Fingerprint Sensors
- Improved Biometrics
- TPM Key Attestation
- Certificate Reputation
- Improved Virtual Smartcards
- Provable PC Health
- Improved Windows Defender
- Improved Internet Explorer
- Device Encryption (All Editions)
- Remote Business Data Removable

How 'anywhere connectivity' evolved



Windows 8 Security Capabilities

Malware Resistance



Securing the Boot
Securing the Code and Core
Securing the Desktop

Protect Sensitive Data



Securing Data With Encryption

Modern Access Control



Securing the Sign-In
Secure Access to Resources

Trustworthy Hardware

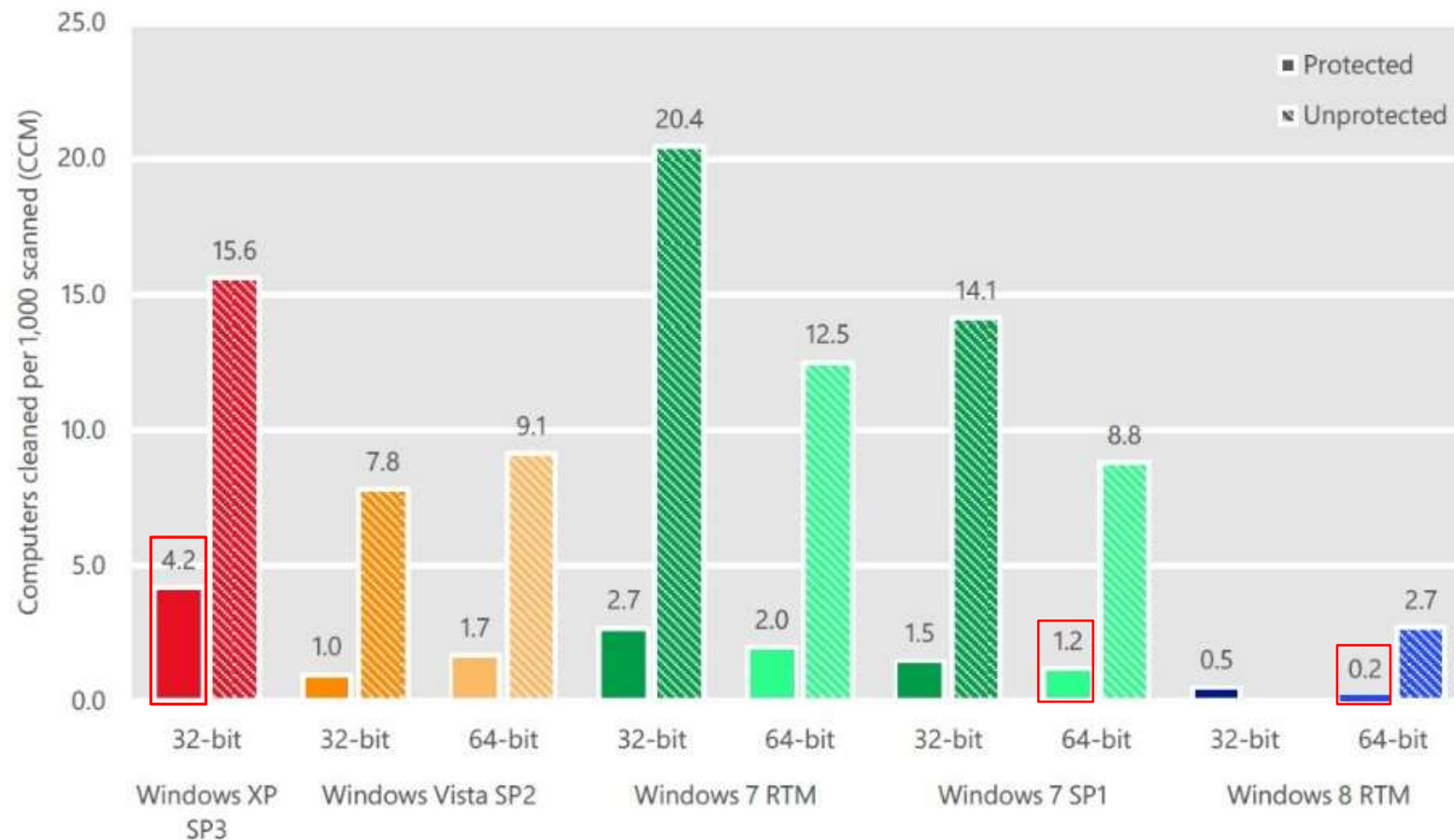
Universal Extensible Firmware Interface (UEFI)

Trusted Platform Module (TPM)

Measuring Windows 8 Security Success

The largest volume of security investments ever made in a single release of Windows have yielded great results.

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



Windows 8 and 8.1 Security Capabilities

Modern Access Control



Securing the Sign-In
Secure Access to Resources

First Class Biometric Experience
Multifactor Authentication for BYOD
Trustworthy Identities and Devices

Malware Resistance



Securing the Boot
Securing the Code and Core
Securing the Desktop

Provable PC Health
Improved Windows Defender
Improved Internet Explorer

Protect Sensitive Data



Securing Device with Encryption

Pervasive Device Encryption
Selective Wipe of Corp Data

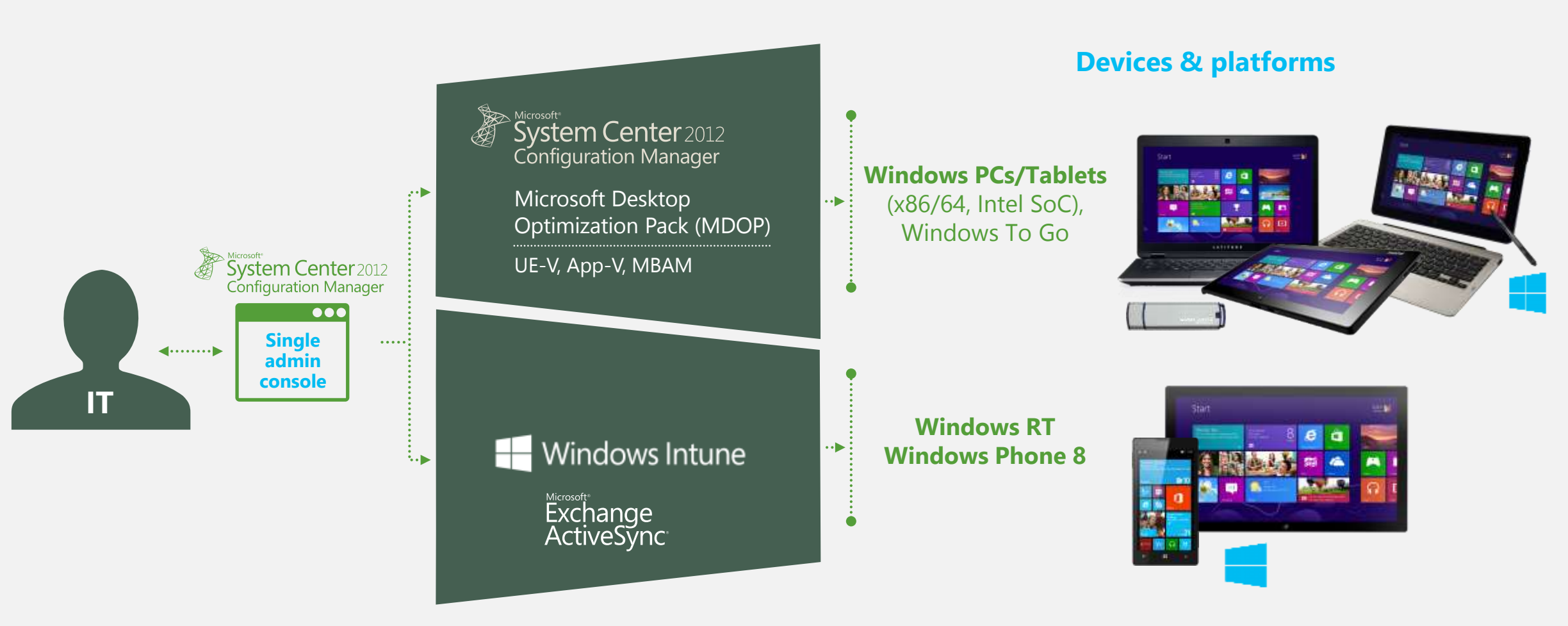
Trustworthy Hardware

UEFI

Modern Biometric Readers

TPM

Cyber Threat Mitigation - Enterprise management



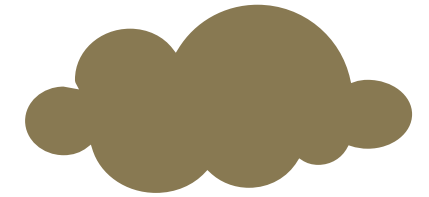


From Unsecure
Desktop to
Securely Managed
Environment

Comprehensive Protection Stack

Cyber Defense building on Windows Platform security

MANAGEMENT	System Center Configuration Manager and Endpoint Protection						
	Endpoint Protection Management	Software Updates + SCUP	Settings Management	Operating System Deployment	Software Distribution	Exchange Connector	
ANTIMALWARE	System Center 2012 Endpoint Protection						
	Antimalware	Behavior Monitoring	Dynamic Translation	Vulnerability Shielding	Windows Defender Offline	Cloud clean restore	ELAM & Measured Boot
PLATFORM	Windows						
	Internet Explorer	AppLocker	BitLocker	Data Execution Prevention	Address Space Layout Randomization	User Access Control	
		Windows Resource Protection	Secure Boot through UEFI	Early Launch Antimalware (ELAM)	Measured Boot		



DYNAMIC CLOUD UPDATES

Dynamic Signature Service

Microsoft Malware Protection Center

 Available *only* in Windows 8

 Enhanced in Windows 8 (or Internet Explorer 10)

Introducing Microsoft BitLocker Administration and Monitoring MBAM 2.0

 New Version



Maintain and enforce compliance

- Simplifies the BitLocker provisioning process at scale
- Deploy BitLocker to new devices or to those already provisioned to users
- Report on device encryption compliance and audit access to keys




Integration and Scalable

- Centralized reporting and hardware management with System Center Configuration Manager 2007 and 2012
- Manages 100's or even 100's of thousands of devices



Reducing Costs

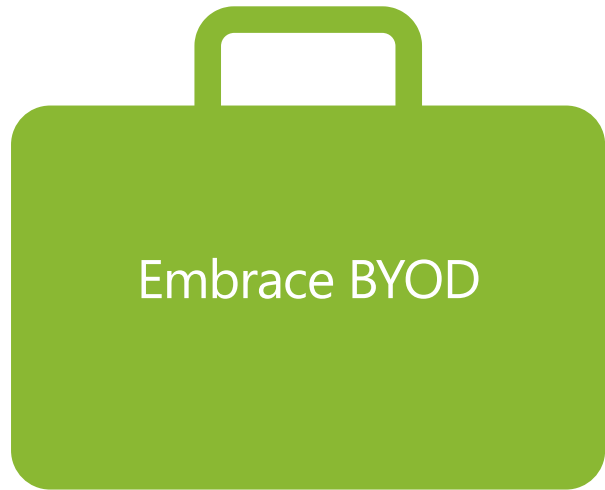
- Users are able to recover devices using a Self Service Recovery console
- IT Recovery console enables IT to access recovery data on behalf of users
- Users can initiate PIN resets and volume encryption tasks



BYOD = Bring Your
Own Pain?

Embrace Bring Your Own Device to Military Environment

A Variety of Solutions that Fits Your Organization



VDI: Access to corporate image



Windows To Go: Consistent Windows 8 experience on any PC* from USB



ConfigMgr: User/device-specific management



Windows Intune: Cloud management for Windows-based PCs & tablets

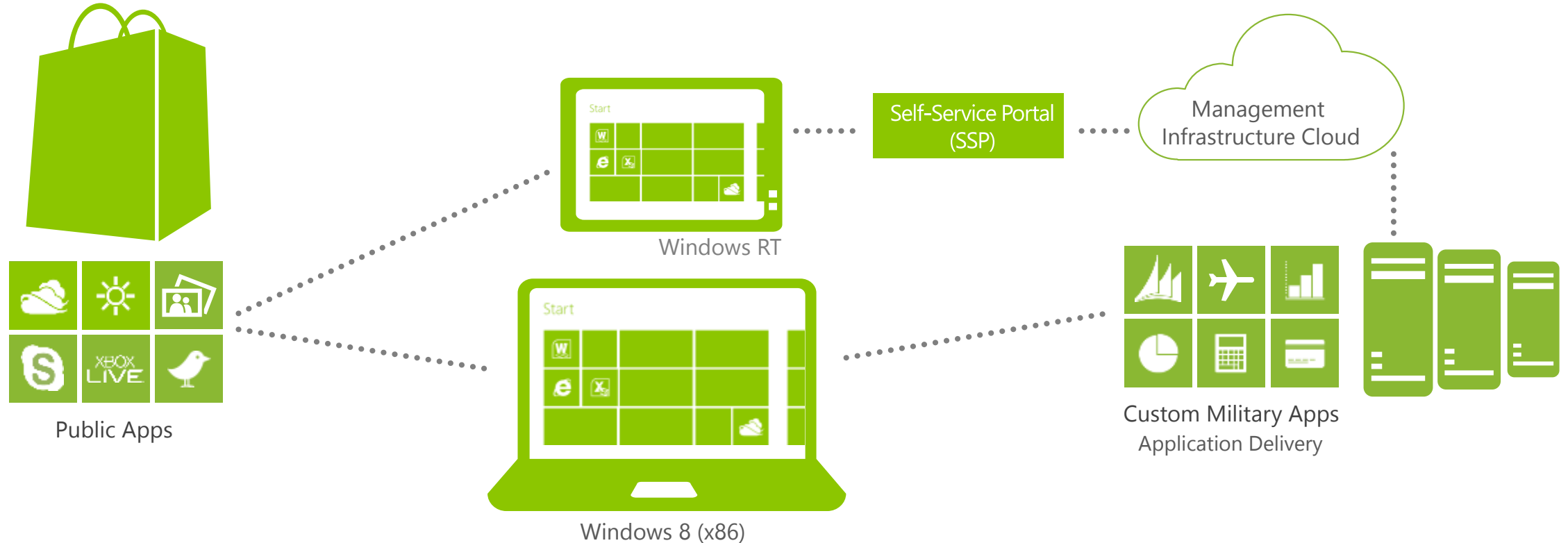
*any device certified for use with Windows 7 or Windows 8

Windows 8 App Delivery



Download from Windows Store

Side Load from Your Infrastructure





From observation
to Cybercrime fight

Microsoft Cybercrime Center

- DCU has designed a collaborative and secure space where experts from across Microsoft's product groups can work side by side with each other, DCU, and industry partners to **develop and execute cybercrime disruption strategies**
- The Microsoft Cybercrime Center **provides hi-tech investigative resources and access to intelligence on infected PCs and associated malware** that product and service teams can use to combat account and platform compromise and service abuses, including denial of service attacks, ad fraud, and botnet creation



Microsoft Cybercrime Center

Redmond

Windows Server
Running Hadoop

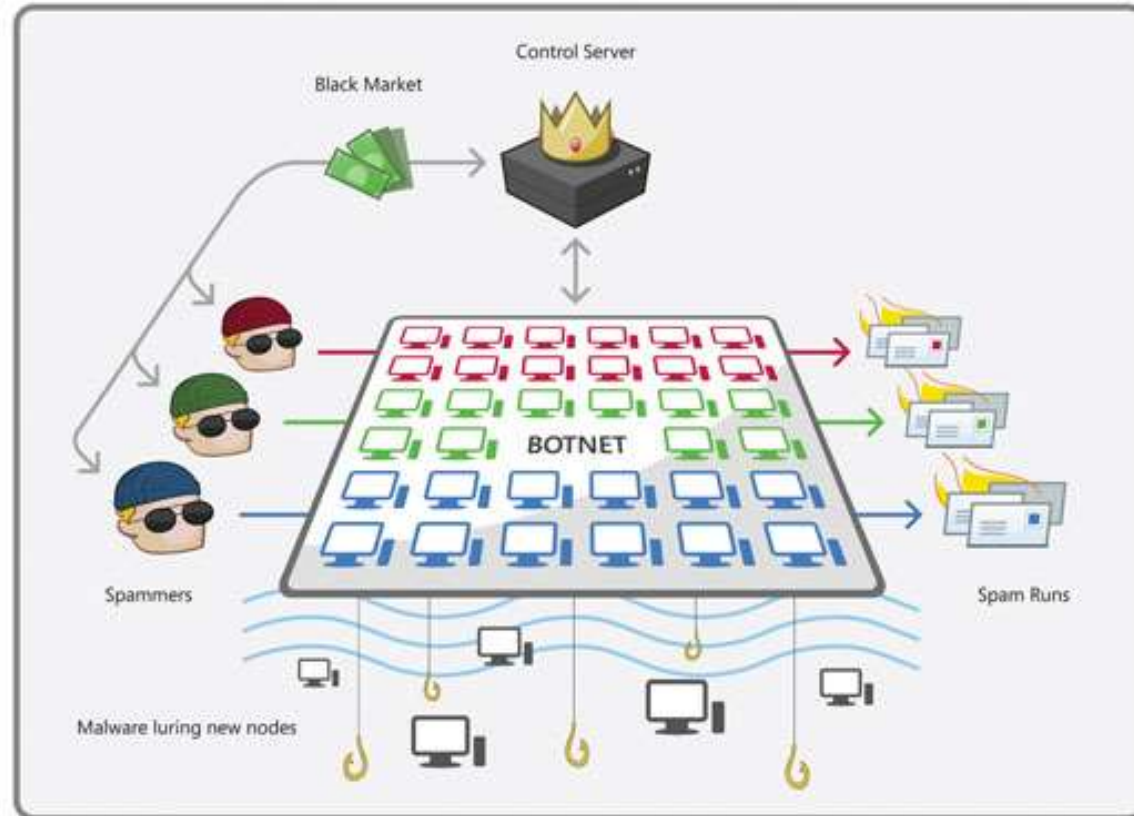
Windows Azure
for SinkHole
distribution

Microsoft SQL
Server

Interested?
Contact local
Microsoft Team

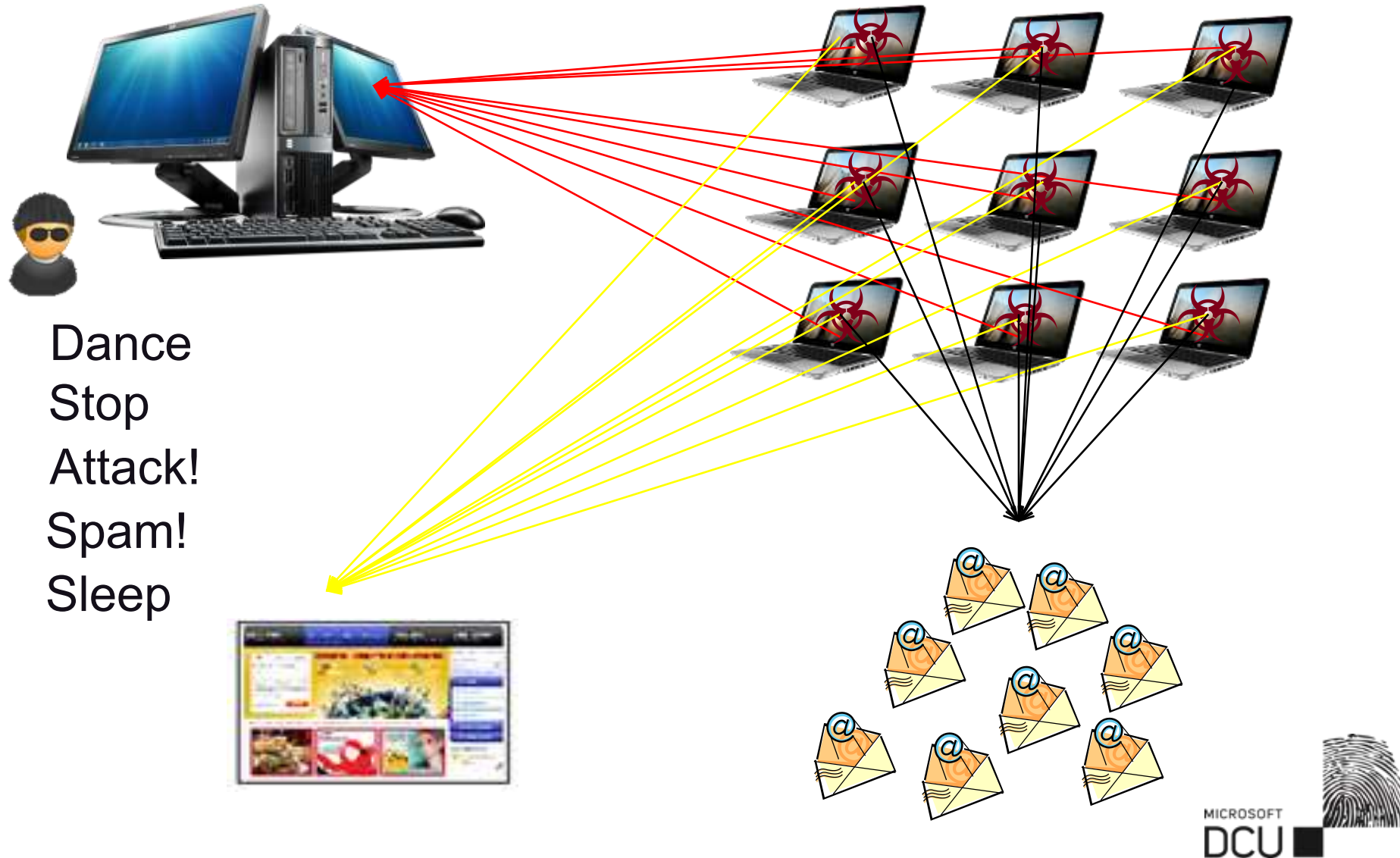
Disrupting the Criminal Infrastructure: "Botnets"

- Botnets are networks of infected computers that can be remotely controlled by an individual or organization
- Used to conduct a variety of attacks
 - Spam
 - Denial of service
 - Click fraud
 - More malware distribution

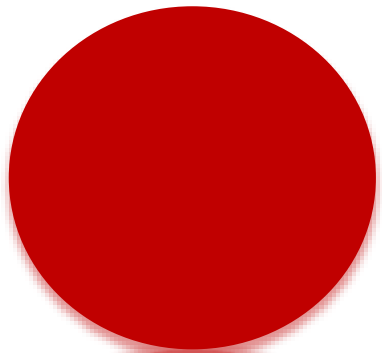


www.microsoft.com/mccorp/twc/operationb19

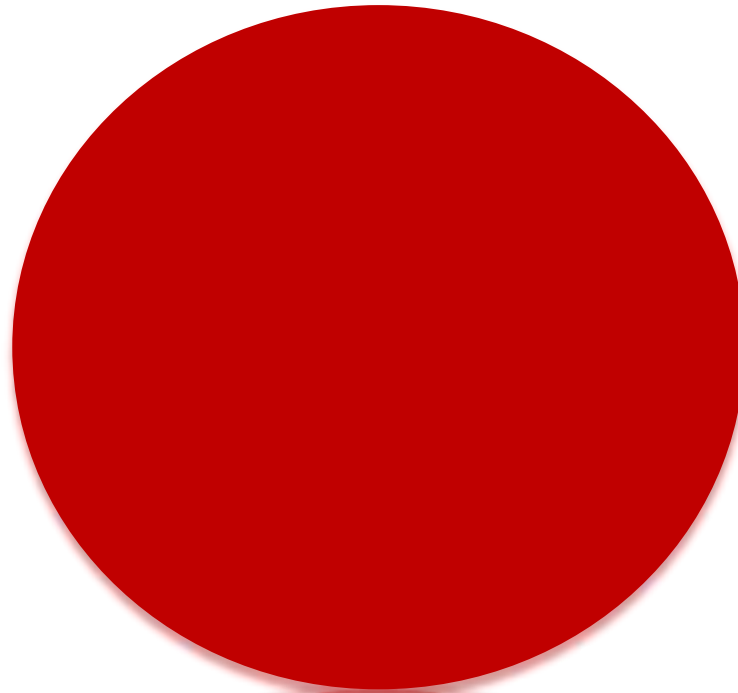
Robot networks – Botnets 101



Disrupting Criminal Business

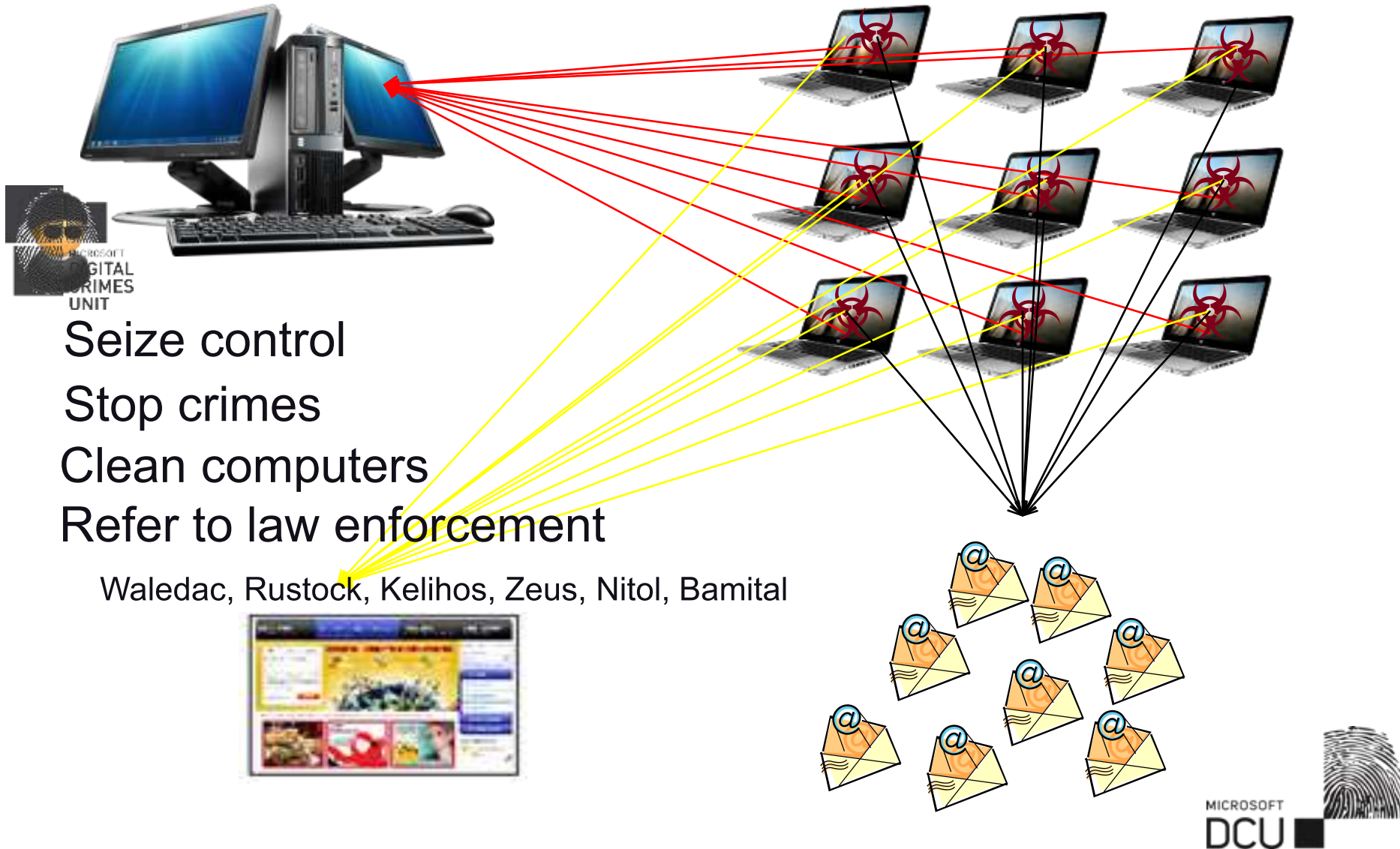


Cost of Criminal
Business



Value of Infection

Botnet Takedowns by Microsoft DCU



Building Threat Intelligence



Disrupting Cybercrime - Project MARS

Project MARS (Microsoft Active Response for Security) is a joint effort between Microsoft Teams: Digital Crimes Unit, Malware Protection Center and the Trustworthy Computing team to proactively combat botnets and help undo the damage they cause



- Operation b49: The Waledac botnet takedown - *February 2010*
- Operation b107: The Rustock botnet takedown - *March 2011*
- Operation b79: The Kelihos botnet takedown - *Sept 2011*
- Operation b71: The Zeus botnet disruption - *March 2012*
- Operation b70: The Nitol botnet disruption - *September 2012*
- Operation b58: The Bamital botnet disruption - *February 2013*
- Operation b54: The Citadel botnet disruption - *July 2013*

Trustworthy
Computing



Malware Protection Center
Threat Research and Response



Disrupting Cybercrime - Project MARS

OPERATION
b49
Waledac

February 2010

Proving the model
of industry-led
efforts

Severed 70,000-
90,000 infected
devices from the
botnet

OPERATION
b107
Rustock

February 2011

Supported by
stakeholders
across industry
sectors

Involved US and
Dutch law
enforcement, and
CN-CERT

OPERATION
b79
Kelihos

September 2011

Partnership
between Microsoft
and security
software vendors

First operation with
named defendant

Disrupting Cybercrime - Project MARS

OPERATION
b71
Zeus

March 2012

Cross-sector partnership with financial services

Focused on disruption because of technical complexity

OPERATION
b70
Nitol

September 2012

Nitol was introduced in the supply chain

Recently settled with operator of malicious domain

OPERATION
b58
Bamital

February 2013

Bamital hijacked people's search results, took victims to dangerous sites

Takedown in collaboration with Symantec, proactive notification and clean-up process

OPERATION
b54
Citadel

June 2013

Citadel commits online financial fraud, responsible for more than \$500,000 in losses

Coordinated disruption showcases impact of public-private sector partnerships to combat cybercrime

Notable Coverage and Quotes on Botnets

THE WALL STREET JOURNAL.

Spam Network Shut Down



Microsoft gets legal might to target spamming botnets

The New York Times

Microsoft Raids Tackle Internet Crime



Exclusive: Microsoft and Symantec disrupt cyber crime ring

AP **MICROSOFT FINDS MALWARE ON NEW COMPUTERS IN CHINA**

"Taking the disruption into the courthouse was a brilliant idea and is helping the rest of the industry to reconsider what actions are possible, and that action is needed and can succeed."

- Richard Perlotto, Shadowserver Foundation, about Microsoft and FS-ISAC's disruption of the Zeus botnets

"Anything which makes life more difficult for the cybercriminals, and disrupts their activities, has to be applauded."

- Graham Cluley, Sophos, about Microsoft's action against the Nitel botnet

"It may be odd seeing a private company take the lead in a law enforcement action, but overall I'm glad it's happening. Shutting down these criminal operations, freeing up the infected computers and prosecuting the cyberscum involved can't happen quickly enough."

- Dwight Silverman, San Francisco Chronicle, about Microsoft and FS-ISAC's disruption of the Zeus botnets

"Microsoft has done the online world a great service by establishing a repeatable process and a legal framework for taking down botnets and bringing malware distributors to justice."

- Stephen Cobb, ESET Security Evangelist, about Microsoft and FS-ISAC's disruption of the Zeus botnets



Operation b70: Nitol Disruption

AP



Who do you know in Seattle that's been arrested? You? You...
[Learn more...](#)



Add to your fragrance: Biogest Winsred Cutler's unrecited...
[More info...](#)



Mom Publishes Free Teeth Whitening Secret that has Angered Dentists!
[Read more...](#)

Advertisement

THE BIG STORY

[Latest News](#) [10 Things to Know](#) [Why it Matters](#) [Class of 2012](#)

FROM BRAND NEW LAPTOP TO INFECTED BY PRESSING 'ON'

by RICHARD LARDNER — Sep. 13 4:35 AM EDT

[Home](#) » [Business](#) » From brand new laptop to infected by pressing 'on'

WASHINGTON (AP) — A customer in Shenzhen, China, took a brand new laptop out of its box and booted it up for the first time. But as the screen lit up, the computer began taking on a life of its own. The machine, triggered by a virus hidden in its hard drive, began searching across the Internet for another computer.

The laptop, supposedly in pristine, super-fast, direct-from-the-factory condition, had instantly become part of an illegal, global network capable of attacking websites, looting bank accounts and stealing personal data.

THURSDAY SEPT. 13

RAOY PAS 19-2402 \$0

SEE MORE DEALS

LATEST NEWS

Date of First Publication: September 13, 2012

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION,
a Washington corporation

Plaintiff,

vs.

Peng Yong, an individual;
Changzhou Bei Te Kang Mu Software Technology
Co., LTD., d/b/a Bitcomm, Ltd; John Does 1-3

Defendants.

Case No. 1:12cv1004 GBL/IDD

Plaintiff Microsoft has sued defendants Peng Yong; Bei Te Kang Mu Software Technology, d/b/a Bitcomm Ltd.; and John Does 1-3, associated with 3322.org and sub-domains of 3322.org, and the Nitol botnet. Microsoft alleges that Defendants have violated Federal and state law by operating a computer botnet and other malicious software through more than 70,000 sub-domains of 3322.org, causing the unlawful intrusion into, infection of, and further illegal conduct involving, the personal computers of innocent persons, thereby causing harm to those persons, Microsoft, and the public at large. Microsoft seeks a preliminary injunction directing that it be made the authoritative name server for 3322.org in order to block traffic to the sub-domains of 3322.org being used to support Nitol and other malware operations. Microsoft seeks a permanent injunction and damages. Full copies of the pleading documents are available at <http://www.noticeofpleadings.com>.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the plaintiff's attorney, Gabriel Ramsey, Orrick, Herrington & Sutcliffe LLP, 1000 Marsh Road, Menlo Park, California, 94025. If you have questions, you should see an attorney immediately. If you need help in finding an attorney, you may call the Virginia State Bar at (804) 775-0808 (in Richmond) or (800) 552-7977 (Statewide or Nationwide).

*原告微软公司 (Microsoft) 对被告 Peng Yong; 贝特康姆软件技术 (d/b/a Bitcomm Ltd) 有限公司, 以及 与'3322.org'、'3322.org'子域和'Nitol'僵尸网络相关的不知名当事人 1、2、3 提出控告。微软公司宣称被告人违反了联邦和州级法律, 被告通过 70,000 多个'3322.org'子域操作计算机僵尸网络和其他恶意软件, 进行非法侵入、感染以及其他更多涉及无辜者个人电脑的违法行为, 并因此对相关人士、微软公司和一般公众造成危害。微软公司特此申请针对'3322.org'授权域名

MICROSOFT
DCU



Security Cooperation Program

- Overview

- A worldwide program providing a structured way for governments and governmental organizations responsible for computer incident response, protection of critical infrastructure, and computing safety to collaborate with Microsoft in the area of IT security
- Includes incident response, information exchange, and public outreach components

- Benefits

- Public/private partnership in incident response and information exchange can help decrease risk to national security, economic strength, and social welfare from attacks on the country's IT infrastructure.
- Microsoft provides a 24/7 hotline for SCP participants, and works with participants to define a process for disseminating information in the event of a critical incident or emergency

SCP Around the World

105 SCP Participants

93 disclosed

12 undisclosed

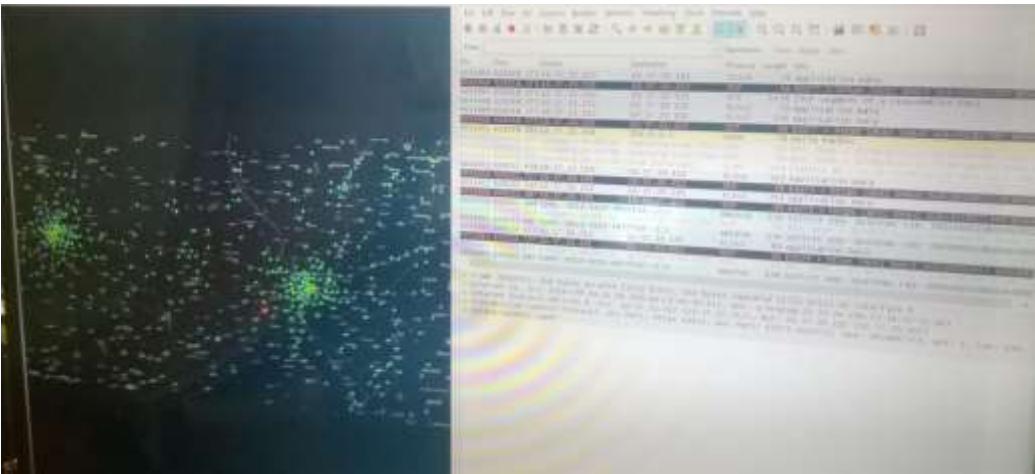


Cyber Threat Intelligence Program

- Project MARS created a botnet detection and cleanup effort supported by Microsoft Trustworthy Computing and the Microsoft Malware Protection Center
- Cyber Threat Intelligence Program delivers **actionable, real-time intelligence on currently tracked threats** to customers and partners

Year	Month	Day	SourceIP	SRCIP_OCT1	SRCIP_OCT2	SRCIP_OCT3	SRCIP_OCT4	ASN	CountryCode	ThreatName	Latitude	Longitude	Hits
2013	Feb	23	39008591	2	83	57	79AS3243	PT	b70-Generic	39.7477	-8.805	2	
2013	Feb	23	1.05E+09	62	169	122	64AS24698	PT	Rustock	38.7597	-9.2397	8	
2013	Feb	23	1.37E+09	81	193	128	224AS3243	PT	Conficker	38.7167	-9.1333	18	
2013	Feb	23	1.39E+09	82	154	189	52AS3243	PT	Conficker	37.1366	-8.5398	4	
2013	Feb	23	1.44E+09	85	138	33	195AS12542	PT	Conficker	38.7167	-9.1333	6	
2013	Feb	23	1.44E+09	85	243	18	200AS3243	PT	Conficker	37.7333	-25.6667	5	
2013	Feb	23	1.44E+09	85	247	188	118AS3243	PT	Conficker	38.5333	-8.9	32	
2013	Feb	23	1.44E+09	85	247	251	91AS3243	PT	Conficker	38.645	-9.1484	25	
2013	Feb	23	1.5E+09	89	155	17	154AS12542	PT	Conficker	41.4444	-8.2962	53	
2013	Feb	23	1.57E+09	93	102	35	83AS24698	PT	b70-Generic	41.1445	-8.5322	4	
2013	Feb	23	1.57E+09	93	102	35	83AS24698	PT	Conficker	41.1445	-8.5322	4	
2013	Feb	23	1.57E+09	93	108	50	30AS12353	PT	Conficker	41.1336	-8.6174	4	
2013	Feb	23	1.57E+09	93	108	226	251AS12353	PT	Conficker	38.7167	-9.1333	6	
2013	Feb	23	1.59E+09	94	132	230	175AS12542	PT	Conficker	41.195	-8.5103	1	
2013	Feb	23	3.16E+09	188	80	185	231AS3243	PT	Conficker	41.4542	-8.168	25	
2013	Feb	23	3.17E+09	188	250	70	43AS3243	PT	Conficker	39.7477	-8.805	10	

Cyber Threat Intelligence Program – what do we see?





Operational Support

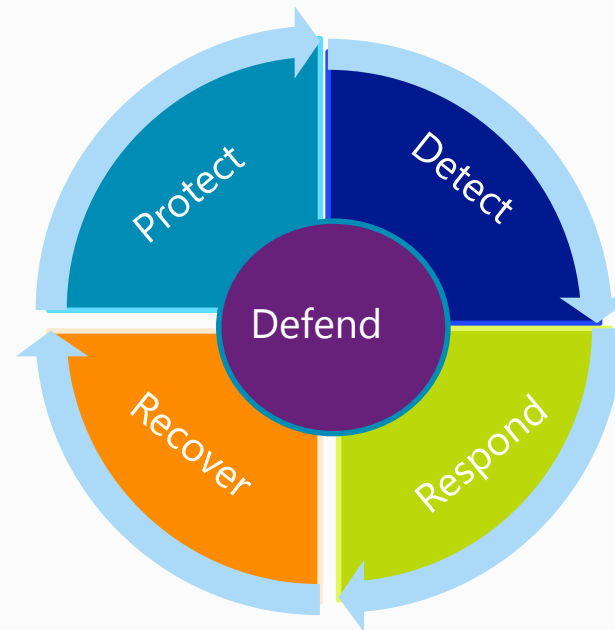
Microsoft Cyber Defense Services

Protect

- System Configuration and Optimization
- Security and Availability Virtualization Solutions
- Network Access Protection and Health Solutions
- Network Isolation Solutions
- Secure and Seamless Remote Access Solutions
- Active Directory Design and Hardening
- Identity Lifecycle Management Solutions
- Secure Public Key Infrastructure Solutions
- Application Server Protection Solutions
- Data Protection and Access Solutions
- Secure Development Lifecycle Solutions

Recover

- Enterprise Recovery Services
- Offline System Recovery
- Enterprise Security Education Services
- Forensics Investigations Education Services



Detect

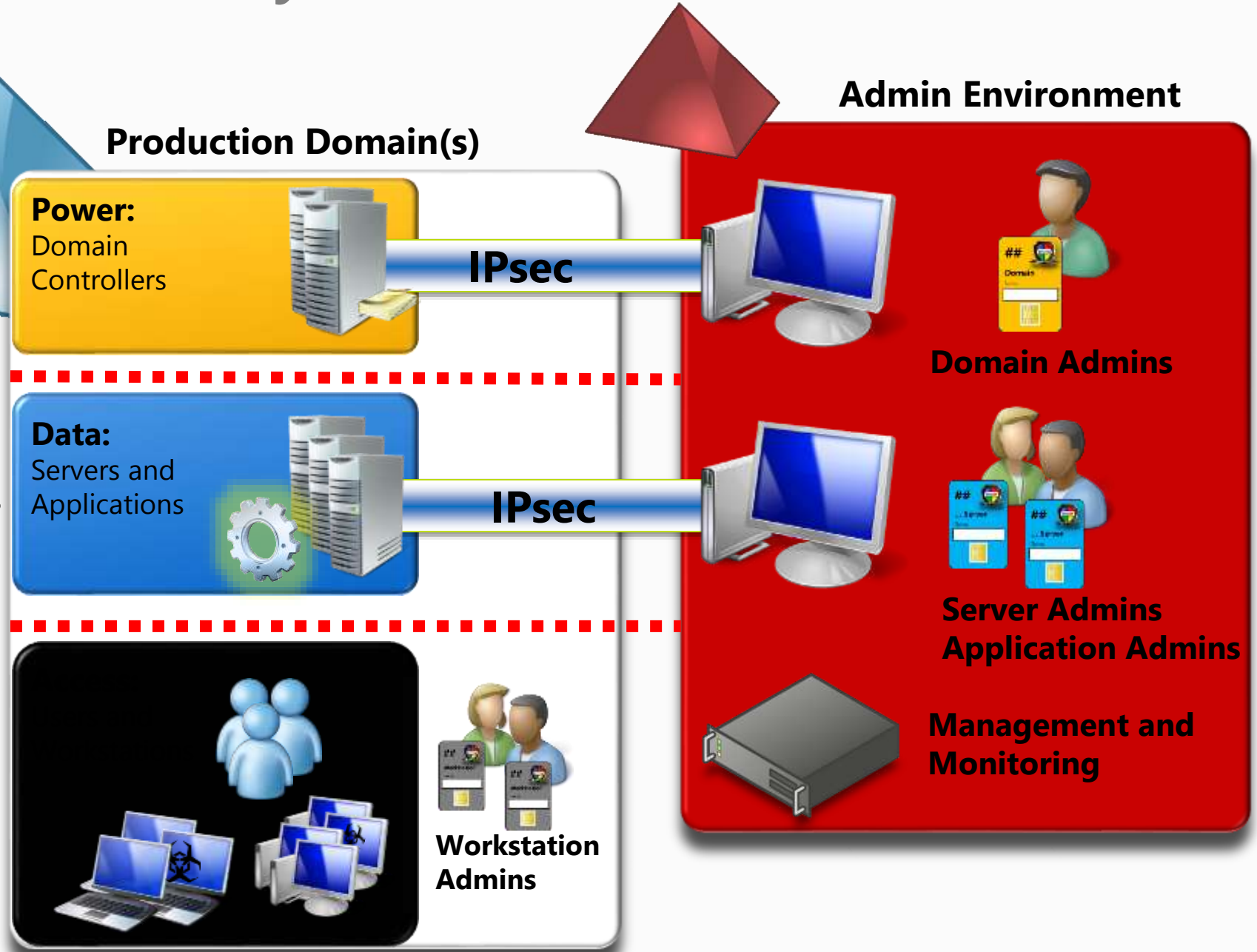
- Enterprise Configuration Management Solutions
- Enterprise End-to-End Monitoring Solutions
- Mobile Device Management Solutions
- Advanced Server Virtualization Solutions
- Client and Server Anti-Malware Solutions
- Audit Collection Services
- Advanced Intrusion Detection Services
- Automated Vulnerability Assessment Services
- Systems Error Reporting and Analysis Services

Respond

- **Windows Online Forensic Services**
- **Enterprise Incident Response Services**
- **Critical Asset Analysis and Investigations Services**
- **Security Response Training Services**

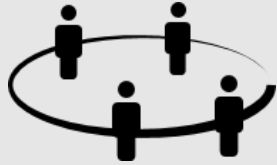
Enhanced Security Admin Environment

- ✓ **Credential Partitioning**
- ✓ **Hardened Admin Environment**
 - ✓ **Hardened Workstations**
 - ✓ **Network security**
 - ✓ **Accounts and smartcards**
 - ✓ **Auto-Patching**
 - ✓ **Security Alerting**
 - ✓ **Tamper-resistant audit**
- ✓ **Service Account Hardening**



Summary -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

Windows 8 vs 7 and XP malware resistance:

- Windows XP is 21 times more likely to be infected by malware than Windows 8
- Windows 7 is 6 times more likely to be infected by malware than Windows 8

These great numbers were direct result of a few technologies like UEFI, Trusted Boot, ASLR, DEP, SmartScreen

Useful Resources

Security Response
Center

[www.microsoft.com
/security/msrc](http://www.microsoft.com/security/msrc)

Security
Intelligence
Report

[www.microsoft.com
/security/sir](http://www.microsoft.com/security/sir)

Security
Development
Lifecycle

[www.microsoft.com
/sdl](http://www.microsoft.com/sdl)

Security
TechCenter

[technet.microsoft.com
/security](http://technet.microsoft.com/security)

Microsoft Security
Update Guide

[www.microsoft.com
/securityupdateguide](http://www.microsoft.com/securityupdateguide)

Identity and
Access

www.microsoft.com/ida

Trustworthy
Computing

[www.microsoft.com
/twc](http://www.microsoft.com/twc)

End to End Trust

[www.microsoft.com
/endoendtrust](http://www.microsoft.com/endoendtrust)

Malware
Protection Center

[www.microsoft.com
/security/portal](http://www.microsoft.com/security/portal)

Security Blog

[www.microsoft.com
/about/twc/en/us/blogs.aspx](http://www.microsoft.com/about/twc/en/us/blogs.aspx)



Cyber Threat Intelligence – messages from the frontlines of Cyber Defense

Thank you for your attention

Robert.Kosla@microsoft.com

Real Impact for Better Defense

www.microsoft.com/safetyanddefense