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

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Raising the Security Bar with Windows 8.1

SESSION ID: SPO1-W03

Chris Hallum
Senior Product Manager
Windows Commercial - Client and Phone Security
Microsoft Corporation

Session Objectives And Takeaways

Session Objective(s):

Provide insights into:

- the MSFT view of the threat landscape
- what motivated our efforts Windows 8.1

Provide overview of key Windows 8.1 security features

Session Takeaway(s):

Windows has the features needed to address today's threats
Windows 8.1 is a game changer for Windows security
Windows 8.1 security is reason enough to upgrade!

The threat landscape is changing rapidly. But this time it’s not just the attackers driving change, it’s your users.

BYOD represents the end perimeter based security.

Your perimeter fading, maybe it’s already gone.

BYOD is a top pri and one of the biggest challenges

But it’s not the only one when it comes to security.

The improvements that we've made in the Windows platforms have driven our adversaries to new tactics.

Attackers have set their sights on identity theft and they're breaking into systems as you!

Identity theft has been used in some recent and very famous breaches.

A Little Sunshine — 252 comments

05 Target Hackers Broke in Via HVAC Company

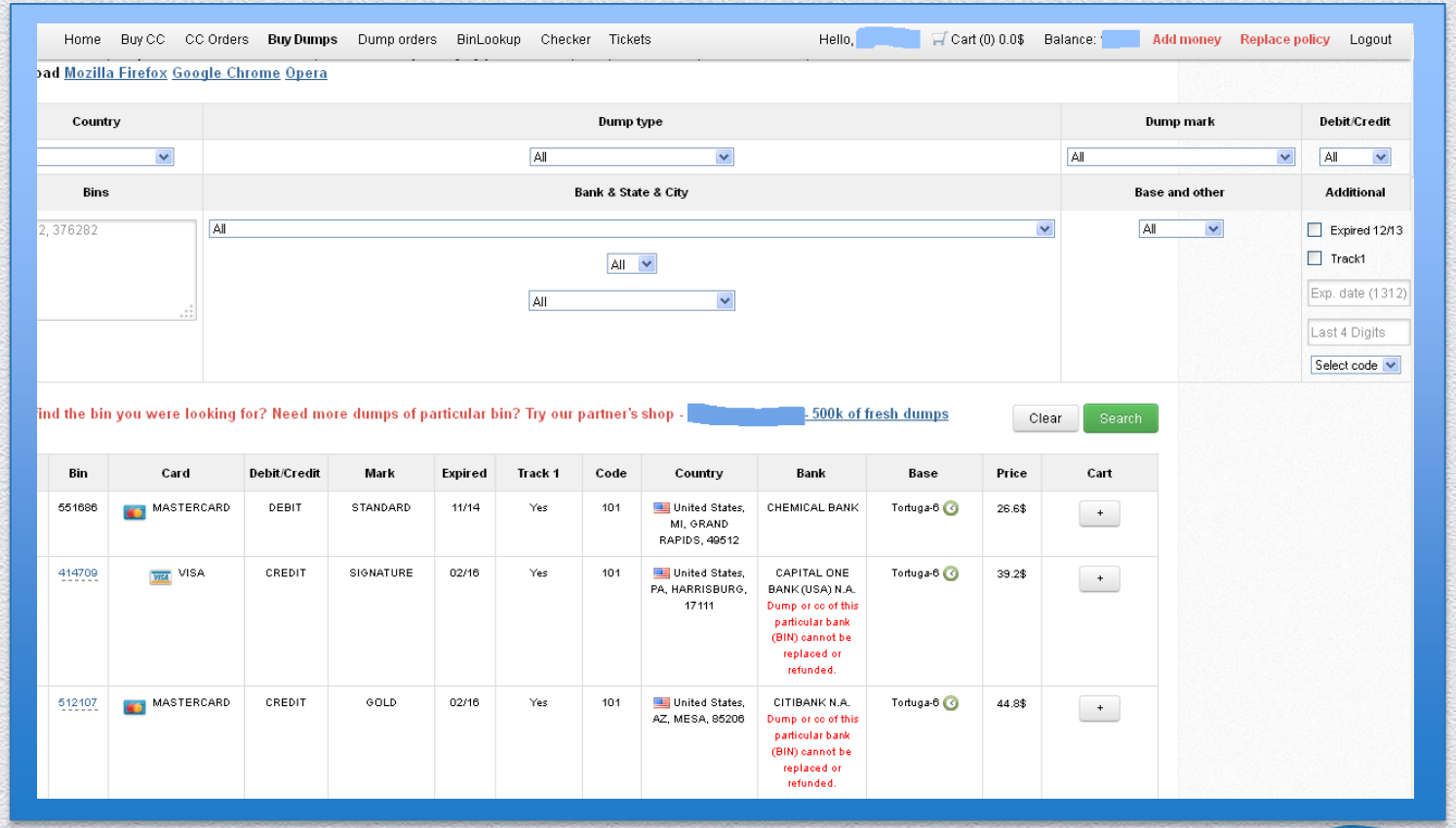
FEB 14

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Recent Posts
Yours Truly Profiled in The New York Times
The New Normal: 200-400 Gbps DDoS Attacks
Email Attack on Vendor Set Up Breach at Target
Security Updates for Shockwave, Windows
Florida Targets High-Dollar Bitcoin Exchangers

There is a prolific and easily accessible black market that facilitates the buying and selling of identities, credit cards, etc.



And so we have a perfect storm.

BYOD is increasing the volume of devices connecting to our networks and they're less managed and often less secure than we're used to.

and the identities used to access corporate resources are under attack like never before.

and so we designed Windows 8.1 specifically to address these big challenges and we're providing you the very best platform to address these modern threats.

Windows Security Investment Areas

Identity and Access Control	Malware Resistance	Information Protection
		

Trustworthy Hardware

Malware Resistance

- Unified Extensible Firmware Interface
  Trusted Boot
  Windows SmartScreen
  Windows Defender
  Provable PC Health

The Threat – Mebromi

Malware

Mebromi, similar to MyBIOS, is a bootkit

Infects Award BIOS and controls the boot up process

Used in combination with one or more additional malware components

Activity

Mebromi is used to enable other malware to persist and tampers with the MBR

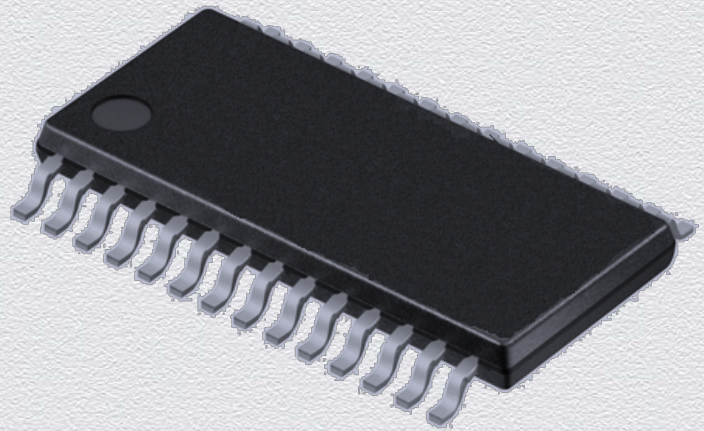
If an antimalware solution is able to clean the MBR Mebromi reinfects

How it stays hidden

By living within the system's firmware Mebromi can remain hidden from most antimalware solutions

Additional malware that Mebromi deploys helps with persistence and tampers with AV

Unified Extensible Firmware Interface



What is UEFI?

A modern replacement for traditional BIOS

A Windows Certification Requirement (UEFI 2.3.1)

Key Benefits

architecture-independent solution

initializes device and enables operation (e.g.; mouse, apps)

Key Security Benefits:

Secure Boot - Supported by Windows 8, Linux, …

Eliminates Bootkit threat by securing the boot process

Encrypted Drive support for Windows

Network unlock support for BitLocker

Malware Resistance

- Unified Extensible Firmware Interface
- ➡ Trusted Boot
- Windows SmartScreen
- Windows Defender
- Provable PC Health

Microsoft

#RSAC

RSACONFERENCE2014

The Threat – Alureon BootKit

Malware

Alureon (also known as TDSS) is a boot and root kit

Second most active botnet in the second quarter of 2010, and infected million's of computers

Became known when update MS10-015 caused Alureon infected systems to crash

Activity

Steals data by intercepting and redirecting system's network traffic

Searches for usernames, passwords, credit card data, click fraud

How it stays hidden

Updates MBR to point boot process to kit, installs rootkit by infecting system driver (atapi.sys)

Disables mandatory kernel-mode driver signing

Trusted and Measured Boot

Trusted Boot

End to end boot process protection (Bootloader to Windows Sign-In)

ELAM complaint antimalware driver is protected, first 3rd party code to start

Automatic remediation/self-healing if compromised

Measured Boot and Remote Attestation

Creates comprehensive set of measurements based on Trusted Boot execution

Can offer measurements to a Remote Attestation Service for analysis

Malware Resistance

- Unified Extensible Firmware Interface
- Trusted Boot
- ➡ Windows SmartScreen
- Windows Defender
- Provable PC Health

The Threat – CryptoLocker

Malware

CryptoLocker (also known as TDSS) is a ransomware virus and bootkit

Often proliferates through email, dupping users into downloading, toolbar vulns

Ransom originally required BitCoins, but now accepting many forms of payment

Activity

CryptoLocker encrypts user data: including pictures, documents, movies, music, etc

How it stays hidden

It doesn't really try and evade detection. Once data is encrypted it's work is done.

Enhancements to Windows Defender and Internet Explorer

Windows SmartScreen (Application Reputation)

Integrated in Internet Explorer download manager and at the OS level (@shellExecute)

Application Reputation checks to cloud on program launch in Windows (all browsers)

Targeted warnings on unknown higher risk applications

Alerts are highly effective (only 5% ignore warning); No warnings for known apps/publishers

Windows Defender

Each edition of Windows include Windows Defender in the box

Includes behavior monitoring and can scan code targeted at binary extension (e.g.: ActiveX)

So how good is Defender and SCEP vs others? AVTest results seem to indicate, not so good!

Nov-Dec 2013 AV Comparatives

Malware Family	Machine Encounters	Missed Machines	Protected	AV test Machine Ecounters	AV test Missed Machines
Top Prevalant Families reported by Microsoft antimalware products					
Sefnit (4)	2,128,853	57,289	97.31%		
Liidu	1,746,224	0	100.00%		
Obfuscator	1,620,970	13,802	99.15%		
Autorun	1,198,344	271	99.98%		
Gamarue	1,155,905	31,036	97.32%		
Sality	571,673	1,188	99.79%		
Dorkbot	551,114	16,960	96.92%		
Conficker	526,758	28	99.99%		
Ramnit	495,375	2,657	99.46%		
Sirefef	495,114	74,944	84.86%		
(1)	10,490,330	198,175	98.11%		
AV Test families not detected by Microsoft at time of testing					
Detplock	283,955	30,361	89.31%	1	1
Dynamer	273,774	8,742	96.81%	157	79
Zbot	229,442	61,335	73.27%	98	61
Sisproc	218,037	1,704	99.22%	121 (3)	21
Injector	166,002	20,321	87.76%	3	0
Rebhip	63,238	3,738	94.09%	4	4
Sisron	54,017	3,156	94.16%	67	1
Cutwail	52,082	5,146	90.12%	678	637
Dimegup	19,788	488	97.53%	11	10
Neeris	6,405	16	99.75%	22	22
Servlice	4,235	30	99.29%	332	282
(1)	1,370,975	135,037	90.15%	1494 (2)	1118

1. Microsoft protects based on prevalence of threats to our customers
2. Microsoft does not focus on comparative tests, as the sample sets conflict with rule 1
3. The test is an instant in time, and we get to them in accordance to rule 1
4. Why was the #1 prevalent family not in the comparative sample set?
5. How do other vendors $core better than Microsoft products on comparative tests?
6. Testing AV in isolation doesn't make sense as other Windows defenses (e.g.: SmartScreen) block infections.

The samples encountered by our customers in this test impacted .004% of our customer base

The Need for Backstop!

The Challenge

UEFI, Trusted Boot, etc are very effective, but no promises

Still a few remote opportunities for defense bypasses

No great way for devices to vet themselves

ISV Opportunities

Remote Health Analysis

Remote Attestation coupled with Access Control

Our Solution for 8.1

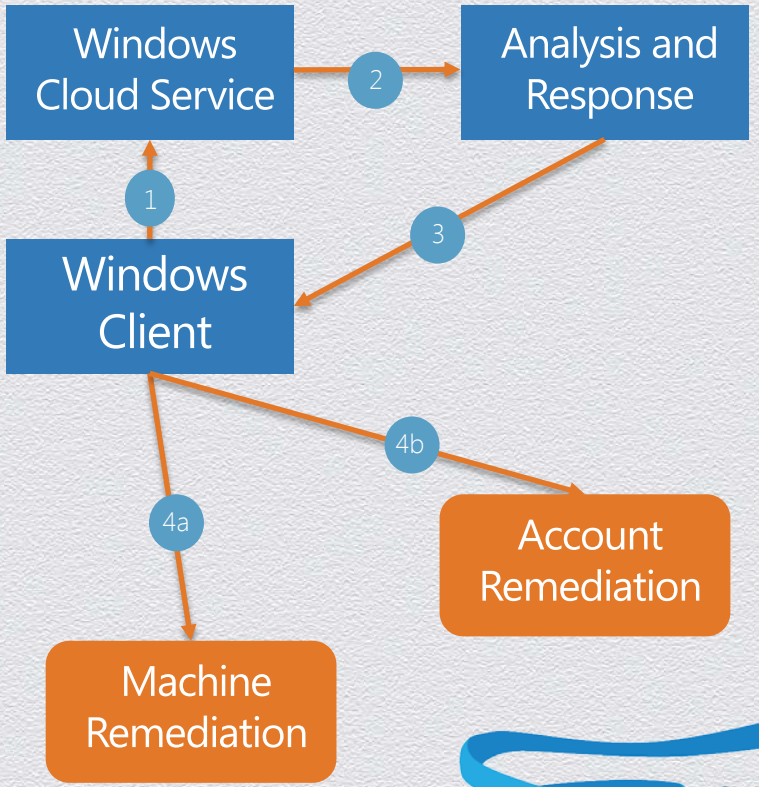
Deliver Remote Health Analysis service for Windows

Provide remediation and notification services

Continue work with ISV to deliver Remote Attestation

Introducing Provable PC Health

1. Client sends heartbeat with state data
   - Measured Boot
   - Action Center Status
2. Cloud service analyzes state data
3. If issue is detected message sent to client
4. Client responds to recommendation
   a) Machine Remediation
   b) Account Remediation



Securing the System Post Boot - AppContainer

Powerful apps that are inherently more secure

Sandboxed apps (AppContainer) run with least priv; Secures system, apps, and data from malicious apps

Access to user data and sensitive Windows capabilities require declaration and user approval

App Capability Declarations

Apps declare which user and system resources they will access (e.g.:Pictures, Webcam)

Access is declared in its package manifest so unlike Desktop apps there is full disclosure

App Contracts

Enable app to app interaction using Source and Target contracts

Source Contract Example - IE has a Source contract to share site info (URL, Image(s), etc).

Target Contract Example - Mail declares ability to receive data and formats it

App Extensions

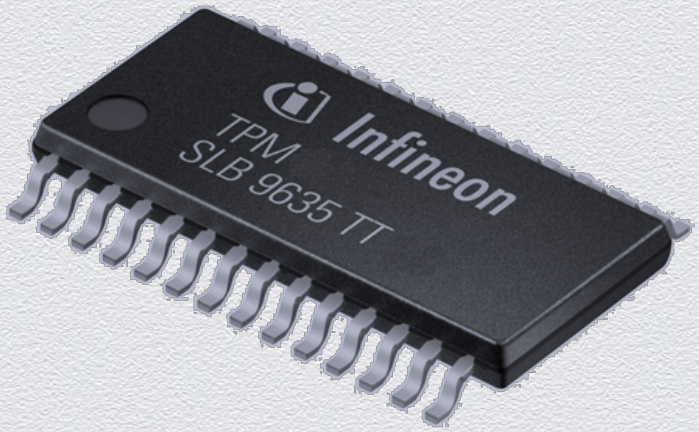
Extensions lets app developers extend or customize standard Windows features

Example - HP could can use a Windows Store device app to customize the Device -> Print flyout.

Modern Access Control

- Trusted Platform Module
- First Class Biometric Experience
- Easy to Deploy Multifactor Authentication
- Trustworthy Identities and Devices

Trusted Platform Module in 8.1



The Opportunity

Dramatically improve security for Consumer and BYOD
Leverage in innovative ways to address modern threats

History in Windows

TPM is currently optional component
Pervasive on Commercial Devices, and most tablets

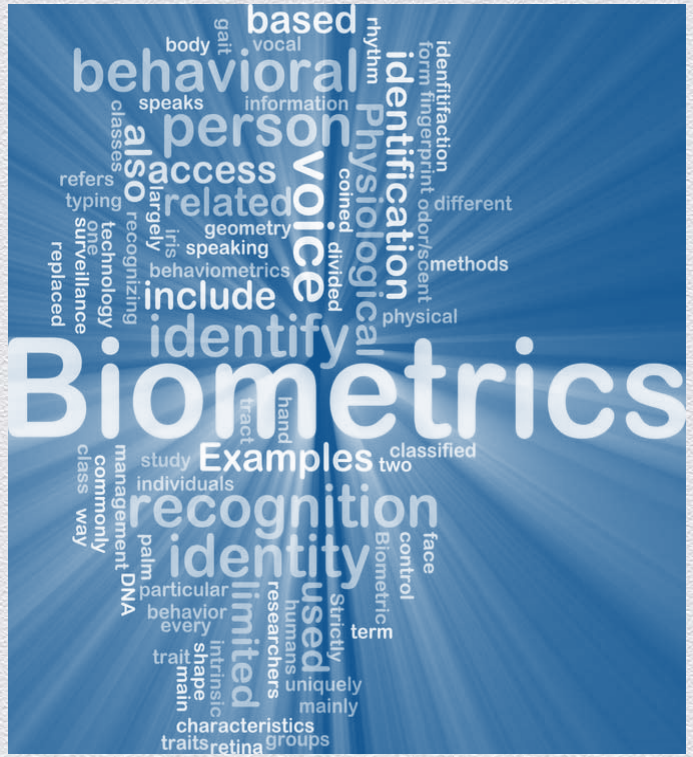
Our Goal in 8.1

Drive adoption of Connected Standby arch with OEM's
Work with Intel to make PTT pervasive on all proc's
Add TPM requirement to 2015 Windows cert reqs

Modern Access Control

- Trusted Platform Module
- ➡ First Class Biometric Experience
- Easy to Deploy Multifactor Authentication
- Trustworthy Identities and Devices

Biometrics In Windows 8.1



The Opportunity

Move forward with strategy to replace for passwords

Reduced friction and improve experience

History in Windows

First added Biometrics capability in Windows XP

Windows Biometric Framework added to Windows 7

3rd parties provide enrollment and drivers

Our Solution 8.1

Make Biometrics the best experience for auth

Create condition where users prefer and use it

Drive adoption in Consumer and Enterprise

Microsoft

#RSAC

RSACONFERENCE2014

Finger Print Device Options for 8.1

Technology Choices

Optical Readers

Thermal Readers

Ultrasound Readers

Capacitive Readers (CMOS)

Characteristics of a Modern Reader

3D Analysis

Liveness Detection

Touch

Microsoft

End to End Support For Fingerprint Biometrics

Three scenarios for Biometrics

Authentication

Providing Consent

User Presence Verification

Windows 8.1 Support

Support for modern Touch based Sensors

Common enrollment experience for all fingerprint sensors

Biometrics sign-in in all Windows experiences (Authentication)

”Touch to Buy” for Windows Store and Xbox Music and Video (Providing Consent)

Apps can enable Biometric (User Presence Verification)

Modern Access Control

- Trusted Platform Module
- First Class Biometric Experience
- ➡ Easy to Deploy Multifactor Authentication
- Trustworthy Identities and Devices

Virtual Smart Cards Ready for BYOD

What are Virtual Smart Cards

TPM virtualized as a Smart Card for auth, encryption, signing, etc.

Address key challenges with existing MFA solutions

Easy to deploy, cost effective, always ready on the device

Top challenges with Virtual Smart Cards

Enrollment process for BYOD (non-domain joined) too complex

Solution for 8.1

API support for provisioning to BYOD (non-domain joined; all arch)

Working with ISV's to incorporate (e.g.: Intercede)

Modern Access Control

- Trusted Platform Module
- First Class Biometric Experience
- Easy to Deploy Multifactor Authentication
- ➡ Trustworthy Identities and Devices

The Need for Trustworthy Certificates

Challenges with certificate trustworthiness

Breaches in security difficult to detect and devastating in impact

Increased dependency on PKI, making it the single point of failure

PKI depends on the assumption that certificates remain secure

DigiNotar Breach
Duped into issuing authentic certs

Stuxnet Malware
Signed malware with stolen certs

Flame Malware
Signed malware with hacked certs

The Opportunity

Increase trust worthiness of PKI system

Help manage and drive crypto-hygiene within ecosystem

Securing Client Side Certificates and Keys

Challenge

If keys not protected by hardware, they may be exportable

If you have access to a private key you own that machine or identity

Compromised private keys can be used from any device (replayable)

Today we assume they have remained secure. Sometimes they're not!

Solution - TPM KSP + Key Attestation

Create a strong binding between private key and hardware (TPM)

Create condition where private keys are inoperable if exported

Provide way to attest if a key was secured with TPM

Certificate Reputation

What did these breaches depend on? Assumptions that:

a certificate that looks un-tampered is authentic

certificate issued from a CA in MSFT Root CA Program are trustworthy

which web servers are issuing authentic certificates is not relevant

What can we do to protect them?

provide a way for anonymous telemetry to collected from clients (SmartScreen)

create analysis services for detecting fraudulent certificates

suggest CA's perform investigation when anomalies are detected

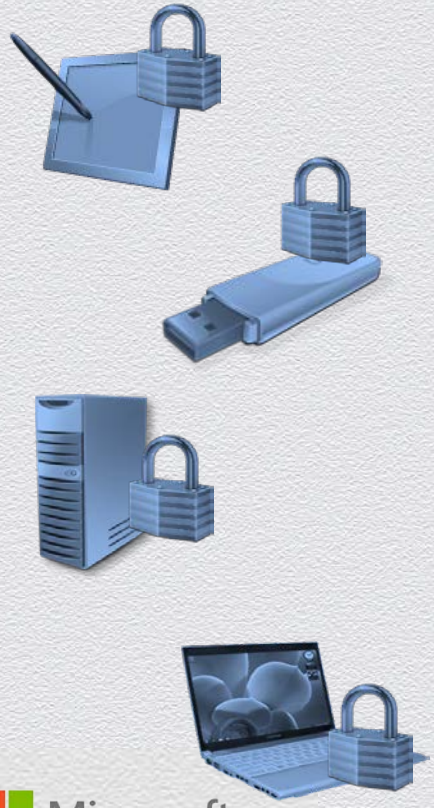
What is the impact on the ecosystem?

Help clean up and better protect public PKI ecosystem

Protecting Sensitive Data

- Pervasive Device Encryption
- Selective Wipe of Corp Data

Full Disk Encryption Going Mainstream



Changing landscape

Traditionally only on business editions of Windows
Critical for business; Increasing demand for consumer
BYOD putting consumer devices in business scenarios
Being used to protect system itself, not just the data

Challenges in making it pervasive

TPM will soon become standard equip, but not there yet
Performance on low end devices not sufficient

Microsoft's direction

Device Encryption available in all editions
Requires Connected Standby certified devices

Device Encryption vs. BitLocker

Device Encryption

Encryption of OS volume is automatic and configured out of the box
Protection is enabled once an administrator uses a Microsoft Account to sign-in
If unmanaged Recovery Key Password is stored in the SkyDrive
Can quickly be configured to use BitLocker features (Pro and Ent only)

BitLocker and BitLocker To Go – Pro and Enterprise

Enables encryption of fixed disk (BitLocker) and removable disks (BitLocker to Go)
Protection is enabled through imaging, mgmt solutions (e.g.: MBAM), or end user
Recovery Keys can be stored in AD or mgmt solutions (e.g.: MBAM)
New and improved FIPS Support

Protecting Devices with Pre-Boot Auth

The conventional wisdom amongst security architects is that the encryption can only be secured by implementing pre-boot authentication

Why have we needed it in the past?

Encryption keys for any encryption solution are loaded into system memory

Cold boot attacks enable attackers with physical access to extract the key from memory

Key Attack Vectors: DMA Port attack; Memory Remanence attack

Downside to pre-boot authentication

Device must be turned off when unattended

Breaks – user experience, management, remote access

Protecting Devices with Pre-Boot Auth, Cont

Modern devices offer immunity to traditional cold boot attacks!!!

Mitigating DMA Port attacks on Windows 8.1 devices

Ports restricted on InstantGo devices

Ports not present on Windows mobile PC's

Windows doesn't load driver for newly attached devices until a user signs in

Ports can be disabled on legacy devices

Mitigating Memory Remanence attack

UEFI prevents published attack (Frozen Memory - Princeton research)

Physical removal of frozen memory trick easier said that done

- not possible on tablets which have fixed memory
- Published research (Canadian DoD) shows attack is highly unreliable

Protecting Sensitive Data

- Pervasive Device Encryption
- ➡ Selective Wipe of Corp Data

Your organization's data is at risk!

Challenges with today's solutions for protecting data

Container model easy to wipe but too restrictive for PC's

"Policy and discovery" model effective but complex

User opt-in model to protect data not always used

Expensive, complex, targeted at sophisticated customers

Windows 8.1 goals

Process of identifying corporate vs. user data

Simplify encryption and access revocation process for corporate data

Better control over corp data when full DLP solution is not an option

Introducing Remote Business Data Removal (RBDR)

RBDR is a platform feature that:

enables services ensure corp data is encrypted as provisioned and can be wiped
offers more control but not a guarantee
uses EFS and Credential Locker protect keys
Used EAS and/or OMA-DM to set policy and issue wipe command

What scenarios does it work for

Shipped the following end to end scenarios:

- Wipe mail, apps, and data via Intune or 3rd party MDM
- Wipes mail from Mail app
- Wipe attachments saved to file system that came from the Mail app
- Wipe WorkFolders data

Driving adoption with 1st and 3rd party apps and DLP products

Windows Phone 8.1 - Ships this Spring

Windows platform alignment

Our goal is to align Windows Client and OS

Some components already aligned, more over time

Shared Hardware

Security Hardware (UEFI, TPM)

Shared Core

Kernel and App Platform

Shared Security Components

ASLR, DEP, Trusted Boot, AppContainers, SmartScreen, Device Encryption…

Enterprise enrollment

Provisions accounts, apps, network profiles, policies and certificates

S/MIME

Signed and encrypted email

VPN

Standards-based IKEv2/IPSec VPN and SSL VPN

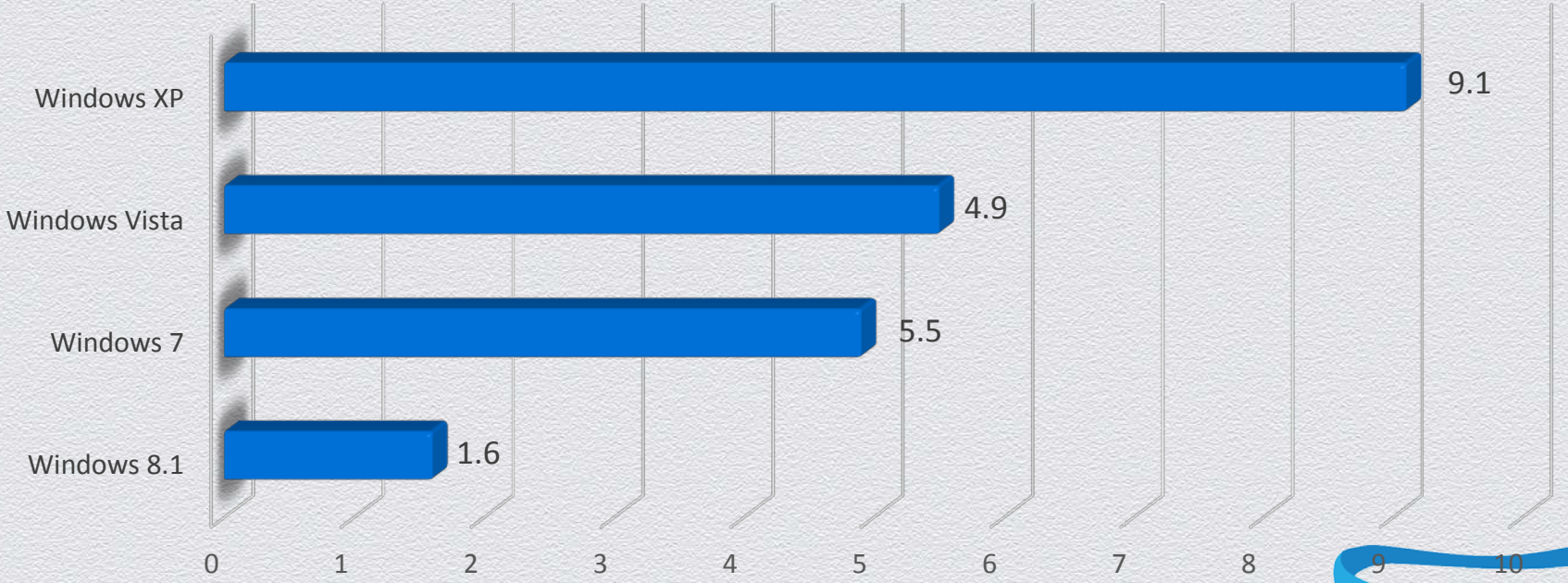
Enterprise Wi-Fi

EAP-TLS and EAP-TTLS

Microsoft

Measuring Windows 8.1 Success: Infection Rates

Windows 8.1 offers the best malware protection of any version of Windows

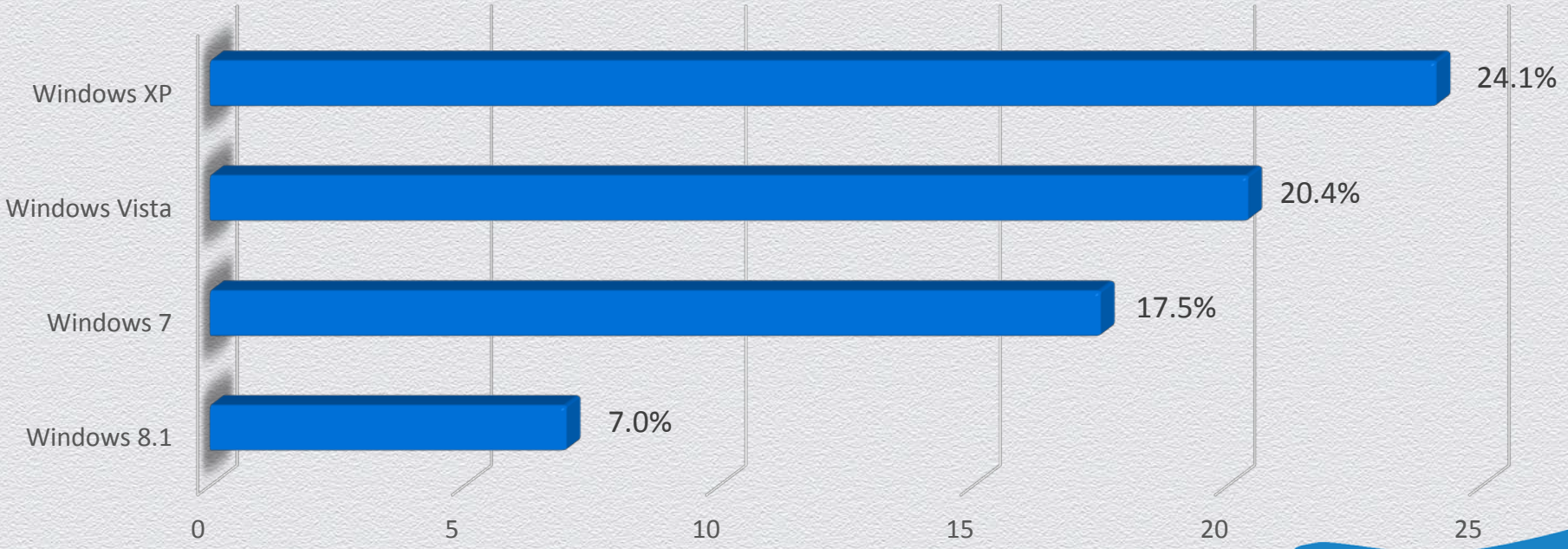


Infection rate per 1000 machines scanned
(SIR Volume 15: January 2013 to June 2013)

Microsoft

Measuring Windows 8.1 Success: AV Running Rate

Windows 8.1 offers the best malware protection of any version of Windows



% of machines scanned not running an up-to-date anti-malware solution
(SIR Volume 15: January 2013 to June 2013)

In Review Session –Takeaways

Session Takeaway(s):

Windows has the features needed to address today's threats

Windows 8.1 is a game changer for Windows security

Windows 8.1 security is reason enough to upgrade!

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO