One Ring to Rule them All
A primer on virtualization enhanced security

@SimonCrosby
Co-founder & CTO
We use micro-virtualization to secure endpoints

We serve enterprises and government agencies

We are experts in virtualization and security

Team of ~180 in Cupertino, CA and Cambridge, UK

A Microsoft Security Partner
The Threat Landscape

- In 2014, 5 unique attacks per second caused 79,790 incidents and 2,122 confirmed data breaches in 61 countries.
- Sadly, 71% of vulnerabilities had a patch available for over a year before.
- Over 90% of all incidents were caused by a user.
- And over 70% of malware was unique to the target organization.

Source: Verizon DBIR’15
“The rise of the targeted attack is shredding what is left of the anti-malware market’s stubborn commitment to reactive protection techniques. It is clear that the industry is failing in its primary goal of keeping malicious code off PCs.”

GARTNER MQ FOR ENDPOINT PROTECTION
Q1, 2015, DOCUMENT G00262733
Virtualization has long been used to wring efficiency out of over-sized infrastructure, solving security problems by creating virtual environments that isolates applications from everything else on a system.

"The essence of virtualization-enhanced security is the ability to arbitrarily shrink the OS and network attack surface of an application to the point that it is completely isolated from everything else on a system."
Why Endpoints Remain Vulnerable

➢ Today’s arsenal
  ▪ Anti-Virus
  ▪ HIPS
  ▪ EMET (ROP Mitigation)
  ▪ Rootkit Detection
  ▪ EDR

➢ Depend on the integrity of the Windows kernel

➢ Easily disabled by malware that exploits a kernel 0day

© Bromium - 2015
Goal: Protect the OS kernel by isolating any malicious user task (application)
Goal: Protect the OS kernel by isolating any malicious user task (application)

CVE-2015-5119 (Hacking Team)
Goal: Protect the OS kernel by isolating any malicious user task (application)

The attacker directly compromises the kernel, bypassing the sandbox

CVE-2015-2426
Application.exe
Application DLLs

Application Sandbox

JavaScript
Chakra
Browser

C# VB
Silverlight 4/5
.OOB

C# VB

C++ MFC ATL

Win32 API

COM
DCOM

GDI+
DirectX

Devices / Printing
File system

NTDLL.DLL

Hypervisor

35 Hyper calls
Desktop Virtualization

- Centralization
- Manageability
- Compliance
Next-gen IDS
Virtualization uses an additional ring of hardware protection and a small TCB
New Micro-VM per ‘user task’
Protected

- OS
- Network
- Intranet
- SaaS Sites
- Applications
- Files
- Credentials

Isolated

- Websites
- Attachments
- USB / shares
- Untrusted networks
- Vulnerable Applications
1. Micro-VM introspection
2. One task per micro-VM
3. Complete record of execution state (diffs, pcaps, files)
4. Real-time analytics & reporting
5. Self-remediation
Low FP forensic detail for each attack
Enhancing the Security of Windows 10
Windows 10 Device Guard

Device integrity
- UEFI Secure Boot prevents device tampering and ensures OS starts with integrity

Cryptographic processor
- TPM processor provides tamper proof integrity validation and prevents unauthorized access to sensitive information

Virtualization
- Processor based virtualization isolates critical system components and data and protects even in the event full system compromise

Biometric sensors
- Using a biometric for authentication increases the level of difficulty for an attacker to the highest level

© Bromium - 2015
Result

- A compromised PC is less valuable
- Device still has network access
  - AD, Exchange, Intranet, shares
- Files/data can be stolen
- A keylogger / screen scraper can steal data & credentials
- Cryptolocker etc…

Windows 10 Device Guard

- Adopts Virtualization Based Security (VBS) to protect credentials and key OS services
- Even if the OS is compromised, key data can’t be stolen
- Reduces credential theft and pass-the-hash attacks
Micro-virtualization and Windows 10

The microvisor isolates each task and self-remediates untrusted networks, files.
Micro-virtualization will transform cloud security
An engine that enables any payload to be encapsulated as a lightweight, portable, self-sufficient container...

...that can be manipulated using standard operations and run consistently on virtually any hardware platform.
What's the threat model?
Isolation = Protection
Micro-virtualization for Docker Containers

Intel Clear Containers

- Security and isolation advantages of virtualization to isolate containerized applications on Linux
- Fast booting small Linux VM per container
- Containers can reside in multi-tenant environments
vSphere Integrated Containers

Team A

REST/HTTP

Team B

Deploy via vCenter
Specify coarse configuration:
Datastore
Cluster
Network
Limits

Shared Storage (vSAN or other)

vCenter & current management tools
SGX Programming Environment

Protected execution environment embedded in a process

- With its own code and data
- Provide Confidentiality
- Provide integrity
- With controlled entry points
- Supporting multiple threads
- With full access to app memory