Bromium: Virtualization-Based Security

TAG-Cyber Briefing

Presented by Simon Crosby
CTO, Co-Founder of Bromium
Hardware-isolate individual user tasks and OS services using endpoint CPU virtualization
- Search for attacks in real-time
- Isolate & remediate infected devices
- Learn, Adapt & Distribute new attack vectors & IoCs
- Send to SIEM and share with peer orgs
Bromium eliminates malware completely, reducing the need for reimaging and patching.

- Security Director, Valspar
Microsoft Edge browser isolation announcement

- Windows Defender Application Guard runs the Edge browser in isolation
- Limited to enterprise and education licenses
- Available summer 2017
Microsoft validation that **Bromium solves the problem!**

“Microsoft and Bromium are partnering on a series of joint security scenarios that use Virtualization Based Security and micro-virtualization as a means to hardware isolate apps. Microsoft Edge uses Windows Defender Application Guard to protect the device, apps, data, and networks from attacks launched through the browser. Bromium ships a robust full-featured solution to protect the endpoint from malicious documents, executables, attachments, downloads and sites.”
Processor based virtualization isolates critical system components and data and protects even in the event full system compromise.

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

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

Virtualization using a biometric for authentication increases the level of difficulty for an attacker to the highest level.
Device Guard uses micro-virtualization to hardware-isolate two Windows Services

- Credential Guard isolates credential hashes to reduce pass-the-hash attacks
- Hypervisor enforced Code Integrity enforces white-listing for applications and the OS kernel

Windows Defender Application Guard will isolate the Edge browser (in RS2)
Bromium isolates all external attack vectors and monitors the OS and every app.
Ransomware is now the **#1 security concern** for organizations

**Ransomware attack vectors**
- Weaponized e-mail attachments
- Embedded hyperlinks within emails
- Browser (drive-by) attacks
- Web application vulnerabilities
Defeating ransomware with Bromium and Microsoft

Isolates Edge

- Weaponized e-mail attachments
- Embedded hyperlinks within emails
- Browser (drive-by) attacks
- Web application vulnerabilities
Enterprise cyber resilience with Bromium

- Protection against Pass-the-hash attacks
- Kernel code integrity checks
- WDGA isolates Edge

- Protection & self-remediation for
  - Network-based attacks
  - File or data loss
  - Key-loggers & screen scrapers
  - Ransomware
  - Persistent APTs
  - Pass-the-hash attacks
  - All malicious execution

- Tamper-proof real-time monitoring (EDR) of isolated tasks and the Windows desktop

© Bromium
New Micro-VM per 'user task'
Protected

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

Isolated

- Websites
- Attachments
- USB / shares
- Untrusted networks
- Vulnerable Applications

BIOS Boot
(Windows 7, 8 upgrade)
Windows Defender Application Guard for Edge

1. Complete record of execution state (diffs, pcaps, files)

2. Fed to SOC for real-time analytics & hunting

Applications
- Windows 10 Kernel
- VBS (Hyper-V)
- Microvisor

3. Self-remediation
Enterprise cyber resilience with Bromium

- Sensor Network
- Threat Intelligence
- Self-defending Endpoints
- API and Threat Feeds
- Device & Policy Management
- Virtual SOC
Bromium is delivering enterprise security – today!

The power of VBS is available now and will support the upgrade journey from Windows 7 and 8 to Windows 10.

We isolate all threat vectors: malicious documents, executables, attachments, downloads, and sites.

The Sensor Network has isolation intelligence for post-breach, detection, investigation, and advanced threat response.

It's easy to deploy and you'll immediately start realizing value.
Bromium helps investment firm secure $236 billion using existing business assets

“The Bromium approach leverages our existing investments in endpoint and network security, providing unambiguous and actionable threat intelligence that we can use to quickly and systematically enhance our overall security posture.”

- Ken Pfeil, CISO Pioneer Investments
Microsoft validates that isolation is the way forward!

- WDAG a Microsoft implementation of virtualization-based security with limited applicability
- Windows 10 WDAG implementation is not available on all Win 10 machines.
  - New hardware required supporting UEFI-based Secure Boot
  - BIOS-booted Windows 10 machines are not supported
- Bromium supports Edge today with hardware-enforced isolation and complete Edge browser isolation is in development
- Bromium accelerates Windows 10 migration with hardware-enforced isolation for Windows 7, 8 and 10 today for all attack vectors
Gartner top security investments in 2016/2017

- Cloud Access Security Broker (CASB)
- Endpoint Detection & Remediation (EDR)
- Non-signature Approaches for EPP
- User and Entity Behavior Analytics (UEBA)
- Micro-segmentation & Visibility
- Security Testing for DevOps
- Intelligence Driven SOC
- Remote Browser
- Deception
- Pervasive Trust Services

Bromium satisfies 6 of the top 10 security investments
Learn more about us.

We have more for you in our TAG-Cyber download.