Exceptional service in the national interest

SAND2014-15065C

Sandia National Laboratories

Endpoint Hardening with Micro-Virtualization (Bromium vSentry Pilot at Sandia)

Andres Georgieff

angeor@sandia.gov

John Montoya

jvmonto@sandia.gov

NLIT 2014

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

The Endpoint Problem

Sandia National Laboratories

- Zero day flaws in applications
  - Adobe (PDF, Flash)
  - Java
  - Web browsers
- Cross site scripting
- Office Macros

vSentry protects with isolation

What is Bromium?

Sandia National Laboratories

vSentry

- Hardware layer Micro-Virtualization used to isolate execution of **untrusted** tasks in the operating system.

Live Attack Visualization and Analysis (LAVA)

- Integrated within vSentry to monitor for malicious behavior and output it for forensic analysis.

Requirements

Sandia National Laboratories

- Intel virtualization technology (VT) provides hardware level isolation
  - Core i5, i7, and some i3 and Xeon processors
  - Minimum 4GB RAM
  - Minimum 30 gigabytes free disk space
  - Windows 7 x64
- Management Server
  - Policy distribution management
  - LAVA
- Supported applications
  - Internet Explorer
  - Microsoft Office
  - Acrobat Reader
  - Flash
  - Silverlight

How does Bromium vSentry work?

Sandia National Laboratories

- A separate micro-VM (uVM) container is created to host each untrusted website and file opened.
- Each Bromium uVM container isolates and restricts access to trusted resources.
- Persistent monitoring on each uVM takes places with LAVA.
- Malware running within the uVM is isolated from the host computer, network, and data.
- Upon closing the uVM, everything within it is destroyed.

Demonstration

Sandia National Laboratories

Pilot Evaluation Criteria

- Effectiveness
- Enterprise readiness
- Usability and stability
- End user experience

Communication Strategy

- Website teaser
- Direct Emails
- Sandia Daily News
- SharePoint site built for pilot participant solicitation, information and feedback

Pilot Deployment

Sandia National Laboratories

- Verified eligibility of volunteers
  - Used Bromium-provided BrPreCheck tool
  - SCCM query
- VT on processor remotely enabled via script
- Installer pushed silently with SCCM

Pilot Data

Sandia National Laboratories

- 107 pilot user group
- 30 days to run vSentry pilot
- 85 unique feedback items reported
- 32 support items opened during pilot
- LAVA detected 15 events, but were identified as false positives

Feedback

Sandia National Laboratories

- Customers desired data provenance
- Lack of reliable printing fidelity lead to undesirable trust behavior
- Performance impact on machines with ≤ 8GB of RAM
- Initialization and re-initialization occurred frequently, degrading performance
- Lack of supported applications and operating systems

Challenges

Sandia National Laboratories

- Determining eligible computers proved time consuming and laborious
- Initial deployment contained a vSentry bug, but was fixed overnight
- Flash 12 critical patch broke vSentry users, as it wasn't yet supported
- Policy management was handled through organizational units
- Hardware and application support limited the amount of qualified users for the pilot
- LAVA detected no organic malicious events, but had several false positives.

Upcoming Features

Sandia National Laboratories

- Mac OSX
- Windows 8.1
- Office 2013
- Acrobat Pro
- Firefox ESR
- Chrome
- Enterprise Scalability Improvements

Future of Bromium at SNL

- Phase 2 of the pilot will be conducted with targeted high-risk individuals

Questions

Sandia National Laboratories