Hardware-Enabled Zero Day Protection (HEZDP)

Def-Logix
Paul Rivera

9/5/2013
Team Profile

- Small Business founded in 2008
- Based out of San Antonio, Texas
- Primary focus on research and development of cyber security software solutions for government customers
- McAfee SIA Partner
• MS Windows is forcing malware authors to develop new sophisticated new tactics, reaching deep into OS internals.
• Bootkits like TDL4 arose from the need to circumvent Windows Patch Guard. DNS Changer infection showed the power of this technique.
• Worse is to come: BIOS malware will likely arise in response to Windows 8 secure boot.
• Proof of concept BIOS malware “Rakshasa” (Blackhat 2012) has the ability to infect multiple firmware, giving it the ability to survive HD format and BIOS flashing.

Source: McAfee Threats Report 2Q 2013
HEZDP in action

Platform Initialization

OS Boot

Runtime

Shimmix

Load UEFI Shell

EFI Driver Dispatcher

Boot Manager

OS Loader

Windows Kernel

Entrap

First Responder
First Responder responds to compromise and interfaces with enterprise security architectures.

Entrap prevents malicious code from hooking.

Shimmix takes firmware and system measurements, detects compromises and restores.

Windows 7 HEZDP Deployment

Host Layers

User Space
OS libraries and executables

Kernel Space
System and device drivers

UEFI Application
Firmware and BIOS

UEFI Drivers
NIC, SATA and graphic cards

Def-Logix Technologies

Full Spectrum Protection

Operating System

Preboot Environment

Hardware
First Responder responds to compromise and interfaces with enterprise security architectures. Shimmix takes firmware and system measurements, detects compromises and restores.
Approach

- Detection is at a lower level
- Involved with UEFI, Pre-Boot, and Firmware
- Takes pre-boot-time measurements
- Verifies system is in good standing
- Sends anomaly information to First Responder
Benefits

• HEZDP provides full-scale protection against a variety of malware and root kits aimed at the kernel, hypervisor, and firmware layers
• HEZDP provides end-to-end trust by enabling hardware to not only thwart attacks, but also be resilient to malware aftermath
• HEZDP has access to UEFI variables and the entire pre-boot process, giving a security capability lower on the host stack than any encroaching malware can reach
• HEZDP measures UEFI variables, system files, and firmware for verification every time the system boots
• Flexibility
• Can Detect Compromised Certificates
• Non-TPM based
• Non-Intel TXT based
Competition/Complimentary Technology (optional)

- UEFI Secureboot
- Intel Trusted Execution Technology (TXT)
- Microsoft Measuredboot
- McAfee DeepSafe
  - Based on Intel TXT technology
Next Steps

Phase 4 – Testing & Initial Release

Final Regression Testing

Phase 5 – Maintenance & Beta

Maintenance & Beta

11 Dec

Initial Release

11 Dec

User Guide/
Installation Guide
Release Notes

<table>
<thead>
<tr>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Contact Information

Mr. Paul A. Rivera
Office: (210) 702-3409
Mobile: (210) 478-1369
privera@def-logix.com