Moving Target Defenses for Data Storage Devices

Donald E. Matthews
Founder and CEO
NexiTech, Inc.
Moving Target Defenses for Data Storage Devices

- **What** we do
  - Layers and fit
  - Foundational work

- **How** we do it
  - Technical attributes
  - Reference architecture

- **Why** does it matter to you?
What is Moving Target Defense?

- Increases the cost of the attacker’s efforts
- Reduces the attacker’s window of opportunity
Changing Multiple Dimensions of the Attack Surface
Multiple attack vectors are available

Multiple vendors protect most layers

NexiTech stands alone with comprehensive **Moving Target Defense** at the Data Storage Layer

**Data Storage Systems**
- Enclosures (power, cooling)
- Solid State Drives
- Data in Motion
- Data at Rest

**Storage Threat Layering**
- Identity Management
- VPN, SSO, Authentication
- Web Application Security/Content Filtering
- Application Memory
- Operating System
- Server Hardware
Storage Attack Surfaces

**Risks Include:**
- Alteration
- Compromise

**Risks Include:**
- Erasure
- Unavailability
- Performance Degradation
- Meltdown!

**Risks Include:**
- Alteration
- Compromise
Storage Attack Surfaces

- **Disk CONTROL Surface**: Risk: Online Data QoS Loss
- **Disk DATA Surface**: Risk: Online Data Loss or Compromise
- **Tape CONTROL Surface**: Risk: Backup Data Loss
- **Tape DATA Surface**: Risk: Backup Data Compromise
- **Enclosure CONTROL Surface**: Risk: Physical Damage
- **Enclosure DATA Surface**: Risk: Physical Damage
Market Landscape

Cyber Security Domain

Data Storage Domain

Flash Memory Summit 2019
Santa Clara, CA
Successful Customer Examples

Silicon Valley Innovation Program

2009
Flash Memory Summit 2019
Santa Clara, CA

2019
How It Works

An autonomous system that randomly changes multiple dimensions of the attack surface, making it unpredictable to adversaries.
Technical Solution

- **Isolate the device**
  - Change the device type from "disk" to "unknown" inside a storage appliance.
  - Create multiple abstractions of the device using storage virtualization.

- **Obfuscate the command set**
  - Change the command set for the device inside the appliance.
  - Makes it more difficult for an attacker to access the device, but not impossible.

- **Now introduce a Moving Target Defense (MTD)**
  - Change the communications channel from one command to the next.
  - Change the command set itself from one command to the next.

- **Statically link the interface library (optional)**
Technical Attributes

- Autonomous
- Multi-dimensional
- Uses randomization
- Unpredictable by adversaries
- Dynamic network configuration
- Gathers metrics and reports breaches
- Optionally may use a Honeypot (i.e. Decoy)
- Address Space Layout Randomization (ASLR) for DATA STORAGE
Technical Capabilities

- Dynamic Networks
  - Protocol Obfuscation
  - Network Address Space Randomization
  - End Point Route Mutation

- Protection of Legacy Systems and Devices
  - Obsolete/Unsupported OS (including Windows XP)
  - Embedded Systems Firmware
  - Real-time Embedded Systems
  - Kernel-mode device drivers for both Windows and Linux
Where Are We Headed?

- Evolving the technology (Patent Pending)
- Expanding market opportunities
- Forming a network of partnerships
- Exploring a broad range of additional use cases, including NVMe-oF
The Last Line Of Defense
Conclusion

- The core technology is adaptable
- It uniquely protects data-in-flight for the storage DATA surface and also the storage CONTROL surface
- Can exist in an appliance …
- Or can be embedded in the device itself
Let’s Start a Conversation!

Donald E. Matthews
Founder and CEO
matthews@nexitech.com
719-687-3225
www.nexitech.com