DEVELOPING AND IMPLEMENTING AN EFFECTIVE ENDPOINT SECURITY STRATEGY

Kurtis Armour
October 2, 2018
New talk - Who dis?

- whoami
  - Kurtis Armour
  - @S3Ns3

- I do security stuff
  - 7 years in the security space
  - Penetration Testing, Endpoint Security, Vulnerability Management

- Interested in security research around attacking and defending environments
Introduction

- The goal of this talk
- Types of attacks that target the endpoint
- Endpoint security overview
Introduction

- The goal of this talk
- Types of attacks that target the endpoint
- Endpoint security overview
- Endpoint maturity model
- Hardening corporate environments
What are we trying to protect?

- Data
  - Workstations
  - Servers
  - Users

- Essentially want to give clients the ability to prevent or detect and respond to security events that happen on any endpoints within the environment
How are endpoints being compromised?

- Insufficient security controls
- Lack of user education
- Lack of patch management
- Lack of environment hardening
- Least privilege is not being enforced
Threat Landscape

- What is the end goal of threat actors?
- What are the main ways to execute code?
  - Binary Executables (.exe, .dll, .msi)
  - Scripts (.js, .vba, .vbe, .wsf, .ps)
  - Shellcode
  - Exploitation
Droppers

- HTML / HTA
- JS
- ZIP / 7ZIP / RAR
- EXE / DLL / MSI
- Macros (DOCM, XLSM, POTX)
- PS
- VBA / VBS / VBE
- PDF
- SCT
Types of Attacks that Lead to Compromise

(External) What type of attacks are targeting the users in our customers organization?
- Exploitation – Malvertising, Exploit Kits, Drive-by Downloads
- Social Engineering – Phishing (credential harvesting and malware execution)
- Infected USBs

(Internal) What types of attacks are targeting customers internally after compromise?
- Credential Harvesting and Re-Use
- Active Directory and Protocol Attacks
- Application and OS Exploitation
Endpoint Security Overview
What does the endpoint security stack look like?

- EPP
- EDR
- Application Whitelisting / Process Whitelisting
- Privilege Management and Local Admin
- Vulnerability Management, Patch Management
- OS Hardening
- Deceptive Technique Alerting
- Central Alerting and Monitoring
Security Stack Overview - EPP

- EPP (Endpoint Protection Platform)
  - Anti-Malware component
  - Focused on preventing code execution
  - Static and behavioral analysis are key components
  - Memory protection (preventing exploitation of vulnerabilities)
  - Can include pre-execution and post-execution analysis and prevention
  - Can incorporate multiple components such as encryption, DLP, device control and other forms of security
Security Stack Overview - EDR

- EDR (Endpoint Detection and Response)
  - Records system level behavior
  - Provides detection capabilities through IOCs or IOAs
  - Data search and investigations
  - Suspicious activity detection
  - Response capabilities and host isolation
  - Forensic data acquisition processes
Security Stack Overview - Whitelisting

- Application Whitelisting
  - Utilized to stop unapproved software applications from executing
  - One of the strongest methods to prevent file based malicious code execution
  - Complex to implement in dynamic environments

- Process Whitelisting
  - Utilized to stop unapproved process creation and execution
  - Parent child relationships of process execution
  - Trusted binary execution protection (abusing trusted binaries)
Security Stack Overview – Privilege Management

- Privilege Management
  - Used to limit the ability for password compromise and re-use
  - Central server that can provide authentication validation via TFA/MFA is strong
  - Enforces the requesting user to validate who they are
  - Can cover network based authentication, local authentication or SaaS based authentication

- Local Admin Control
  - Limiting admin access can prevent code execution
  - Randomization of local admin password prevents re-use of credentials
Security Stack Overview – Vulnerability and Patching

- **Vulnerability Management**
  - Utilized to identify known vulnerabilities within a corporate environment
  - Active and passive components can provide details about all hosts supported within an environment
  - Authenticated scanning provides privileged access to vulnerabilities present on the internal system

- **Patch Management**
  - Utilized to remediate known vulnerabilities within an environment
  - Clients should have a consistent patch policy for all components of their infrastructure (network infrastructure, workstations, servers, etc)
Security Stack Overview – OS Hardening

- OS Hardening
  - Native controls are available to harden systems
  - Controls specific to Linux, Windows and Mac can reduce the attack surface
  - Hardening takes time and is specific to each corporate environment
  - Legacy components in corporate environments are generally the weakest link
Security Stack Overview – Deception Technology

- Deceptive Technique Alerting
  - Honey pots
  - Honey tokens
  - Honey credentials
  - Honey networks
  - Honey database tables
Security Stack Overview – Central Logging

- Central Alerting and Monitoring
  - Clients need the ability to ingest alerts across their infrastructure
  - Visibility into alerts within your environment from a central location is key to responding in a timely fashion
  - Aggregate raw events from multiple security controls and implement effective correlation
  - Utilize technology that is able to interpret events to provide meaningful use case detection
Endpoint Maturity Model
Endpoint Maturity Model

- How much are you willing to spend?
- How many controls are you willing to implement?
- Do you have buy in to change operational habits?
Endpoint Maturity Model

- How much are you willing to spend?
- How many controls are you willing to implement?
- Do you have buy in to change operational habits?
- Do you have trained resources internally to support deployed technologies?
- What is your risk tolerance?
Endpoint Maturity Model

- Levels of endpoint maturity based on security controls
  - The key is the visibility and ability to prevent and action on detected content
  - The more technology and coverage from a security perspective makes you better able to protect and respond to security events your organization

- Different levels of maturity on the endpoint
  - Novice 1 – 2 security controls (AV and Vuln Management)
  - Intermediate 3 – 4 security controls (AV, EDR, Least Privilege, Vuln Management)
  - Mature 5 – 6+ security controls (Above controls + Monitored centrally 24/7)
Endpoint Maturity Model

**Deployment**
- Needs to cover your entire environment (Know your assets!)
- Internal and external assets need to be covered
- Policies and configuration specific to each business unit
- Windows, Linux and MacOS

**Implementation**
- Utilize as many capabilities as possible based on product offering
- Utilize trained professionals to implement solutions and third party validation
- Use a wide pool of test hosts across business units during testing
Endpoint Maturity Model

- Continuous testing
  - Validation of deployed technology is the best way to keep detection and prevention current
  - Don’t be sold to a technology or solution until you POC a competitor
  - Don’t just believe what vendors tell you. Test it yourself!
  - Have a standardized testing plan for whatever security control you are looking to test or implement
  - Integration and consolidation can be a big win
Hardening Corporate Environments
Hardening Corporate Environments

- Protecting against initial code execution (stopping droppers)
  - Do not allow employees to have local administrator on machines
  - Restrict macro execution (office 2016 or other software)
  - Limit the execution of script content (WSH)
  - Ensure you are utilizing Powershell v5
    - Constrained language is best way to control PS
    - Or block the Powershell interpreter
  - Run a layered endpoint defense strategy
  - Block common dropper formats via email gateway
Hardening Corporate Environments

- Protecting against password based attacks
  - Deploy Microsoft LAPS across the environment
  - Ensure there is no one in an elevated group who shouldn’t be
  - Disabled LLMNR and NetBios-NS
  - Create an entry for WPAD to deweaponize poisoning
  - Disable WDigest and caching of cleartext credentials on Windows
  - Enforce complex passwords especially on domain admin accounts (28 characters or longer) 6 month rotation (passphrases work well)
  - Limit use of privileged accounts to only manage explicit privileged machines
Hardening Corporate Environments

- Protecting against lateral movement attacks
  - Ensure SMB Signing is enabled across organization
  - Disable all occurrences of SMBv1 within your environment
  - Ensure you are patching all vulnerabilities identified
  - Segregate outdated machines that are running legacy technology
  - Prevent code execution via endpoint hardening
  - Implementing proper least privilege within an environment makes it hard to move laterally
Protecting Corporate Environments – Advanced Clients

- MITRE ATT&CK Framework is awesome
- Map protection and detection mechanisms to the below chart and test!

```plaintext
<table>
<thead>
<tr>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Execution</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Token</td>
<td>Access Token</td>
<td>Account Manupulation</td>
<td>Account Discovery</td>
<td>Application Deployment Software</td>
<td>Command Line Interface</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
<td></td>
</tr>
<tr>
<td>AppCert DLLs</td>
<td>Accessibility Features</td>
<td>Binary Padding</td>
<td>Brute Force</td>
<td>Application Window Discovery</td>
<td>Distributed Component Object Model</td>
<td>Dynamic Data Exchange</td>
<td>Automated Collection</td>
<td>Data Compressed</td>
<td></td>
</tr>
<tr>
<td>AppInit DLLs</td>
<td>AppCert DLLs</td>
<td>Bypass User Control</td>
<td>Credential Dumping</td>
<td>File and Directory Discovery</td>
<td>Exploitation of Vulnerability</td>
<td>Execution through API</td>
<td>Browser Extensions</td>
<td>Data Encrypted</td>
<td></td>
</tr>
<tr>
<td>Application Shimming</td>
<td>AppInit DLLs</td>
<td>Code Signing</td>
<td>Credentials in Files</td>
<td>Network Service Scanning</td>
<td>Logon Scripts</td>
<td>Execution through Module Load</td>
<td>Clipboard Data</td>
<td>Data Transfer Size Limits</td>
<td>Custom Command and Control Protocol</td>
</tr>
<tr>
<td>Authentication Package</td>
<td>Application Shimming</td>
<td>Component Firmware</td>
<td>Exploitation of Vulnerability</td>
<td>Network Share Discovery</td>
<td>Pass the Hash</td>
<td>Graphical User Interface</td>
<td>Data Staged</td>
<td>Exfiltration Over Alternative Protocol</td>
<td>Custom Cryptographic Protocol</td>
</tr>
</tbody>
</table>
```

- [https://attack.mitre.org/wiki/Main_Page](https://attack.mitre.org/wiki/Main_Page)
Protecting Corporate Environments – Advanced Clients

- The security community is awesome!

- Atomic Red Team - https://github.com/redcanaryco/atomic-red-team


- Metta - https://github.com/uber-common/metta

- Know your risk and test your stack!
Creating unparalleled client experiences through technology transformation