GRC TECHNICAL RISK REPORT

Case Study : Post-Breach Windows Forensics with MITRE ATT&CK & D3FEND
Report ID : CTF2025-WIN-REDTEAM
Date : 25 July 2025
Prepared by: Divyanshu Kumar
Confidentiality Level: Internal / Adversary Emulation Report

1. Executive Summary

This report analyses an adversary emulation exercise simulating an advanced, stealthy attack on a Windows endpoint. The attacker disabled security controls, patched memory protections, manipulated boot configurations, and removed forensic evidence to avoid detection. Splunk SIEM was used for log analysis, while the MITRE ATT&CK and D3FEND frameworks guided technique identification and defensive mapping. This case underscores the need for resilient, defense-in-depth approaches and proactive blue team training for real-world readiness.

2. Incident Description

- **Attack Vector:** Multi-step attack involving privilege escalation, security feature disablement, and forensic artifact suppression.
- **Target:** Windows workstation/server, critical for business operations.
- **Impact:** Loss of conventional logs and system silence hindered real-time detection; incident reconstruction required advanced forensic methods.
- **Bypassed Controls:** Windows Defender, AMSI, event logging, and PowerShell history.

Attack Timeline

1. **Registry Modification – LSA Protection Disabled**

   The attacker modified the Local Security Authority (LSA) registry key, weakening system credential protection and paving the way for tools like Mimikatz.

   - **Registry Path:** `HKLM\SYSTEM\CurrentControlSet\Control\LSA`
   - **MITRE Technique:** Modify Registry (T1112)

2. **Windows Defender Disabled**

   A crafted PowerShell command disabled key Defender modules, reducing antivirus visibility for files, emails, and new threats.

   - **Command:** `Set-MpPreference -DisableIOAVProtection $true -DisableEmailScanning $true -DisableBlockAtFirstSeen $true`
   - **MITRE Technique:** Disable or Modify System Security (T1562.001)

3. **AMSI Bypass Patch Injected**

   The adversary employed an in-memory PowerShell patch on the AMSI (AmsiScanBuffer), allowing malicious scripts to bypass security scanning.

   - **Patched Function:** AmsiScanBuffer
   - **MITRE Technique:** AMSI Bypass (T1562.001)

4. **System Reboot into Safe Mode**

   The attacker restarted the host in Safe Mode with Networking, disabling most AV/EDR protections and facilitating persistence.

   - **Command:** `bcdedit.exe /set safeboot network`
   - **MITRE Technique:** Boot or Logon Initialization Scripts (T1547.001)

5. **PowerShell Command History Wiped**

   Forensic PowerShell history was erased, further inhibiting traceability of attacker activity.

   - **Command:** `Set-PSReadlineOption -HistorySaveStyle SaveNothing`
   - **MITRE Technique:** Indicator Removal on Host (T1070)

3. MITRE ATT&CK Mapping (TTP Breakdown)

Tactic	Technique	ID	Description
Credential Access	Modify Registry	T1112	LSA protection disabled for credential dumping
Defense Evasion	Disable Security Tools (PowerShell)	T1562.001	Windows Defender modules turned off
Defense Evasion	AMSI Bypass via PowerShell patch	T1562.001	Hooked AmsiScanBuffer for stealthy script execution
Persistence/Evasion	Safe Mode Boot	T1547.001	AV/EDR evasion by Secure Boot manipulation
Indicator Removal	PowerShell History Wipe	T1070	Set-PSReadlineOption disables command history

4. MITRE ATT&CK & D3FEND Defense Control Mapping

Framework	Control Reference	Title/Requirement
MITRE ATT&CK	T1112	Modify Registry (LSA protection disabled)
MITRE ATT&CK	T1562.001	Impair Defenses: Disable/Modify System Security
MITRE ATT&CK	T1547.001	Boot or Logon Initialization Scripts
MITRE ATT&CK	T1070	Indicator Removal on Host
D3FEND	D3-PSA	PowerShell Activity Analysis
D3FEND	D3-HCI	Host Configuration Integrity
D3FEND	D3-EDR	Endpoint Detection & Response
D3FEND	D3-BIV	Boot Policy Integrity Validation
D3FEND	D3-ALH	Audit Log Hardening and Retention

5. D3FEND Defensive Mapping

Defense Category	Capability	ID	Purpose
Command-Line Analysis	PowerShell Activity Analysis	D3-PSA	Detect suspicious scripting activity
Configuration Monitoring	Host Configuration Integrity	D3-HCI	Detect registry and boot config changes
Endpoint Monitoring	Endpoint Detection & Response	D3-EDR	Track tool execution and evasion attempts
Boot Security	Boot Policy Integrity Validation	D3-BIV	Alert/block on malicious boot state changes
Logging & Audit	Audit Log Hardening	D3-ALH	Ensure event and command retention is enforced

6. Key Observations & Lessons Learned

- Attackers effectively used "living-off-the-land" (LOLBins), blending in with administrative activity.
- AMSI patching and PowerShell-based evasion can neutralize traditional antivirus.
- Silence in logs can itself indicate attacker activity.
- Splunk plus MITRE ATT&CK enables granular post-breach forensic reconstruction.
- Robust, protected PowerShell logging is a must-have control.

7. Recommendations (Tactical & Strategic)

- **Implement Defender Tamper Protection** to prevent adversary changes to host security.
- **Enable ScriptBlock & Transcription Logging** for PowerShell, forwarding logs to a central, immutable store.
- **Deploy Device Guard/Application Control** to restrict and monitor script/tool execution.
- **Audit registry and boot configuration changes regularly**; alert on LSA, Defender, and Safe Boot edits.
- **Enhance blue team readiness** with continuous MITRE ATT&CK/D3FEND-based drills and training—don't rely solely on alerts.

8. Conclusion

This emulation and post-breach investigation demonstrates how modern adversaries can evade standard controls yet remain traceable by well-prepared defenders. Integration of MITRE ATT&CK and D3FEND frameworks, combined with SIEM-based visibility and blue team process maturity, is essential for detecting, analyzing, and countering advanced post-exploitation activities.