Executive Summary: Ransomware Intrusion Investigation

Overview

This executive summary presents the findings of a threat hunting investigation conducted using Microsoft Defender for Endpoint telemetry. The investigation reconstructed a multi-stage ransomware attack across enterprise systems, identifying attacker behavior from reconnaissance through impact.

Key Findings

1. Ransomware payload identified as updater.exe
2. SHA256 hash: e609d070ee9f76934d73353be4ef7ff34b3ecc3a2d1e5d052140ed4cb9e4752b
3. Encryption activity began at 22:18:33 UTC
4. Shadow copies were deleted to prevent recovery
5. Evidence cleanup was performed via script-based deletion
6. Activity observed across hosts: AS-PC2 and AS-SRV

Attack Summary

1. Initial access via LOLBins for tool delivery
2. Network reconnaissance using scanning tools
3. Credential discovery targeting LSASS
4. Persistence established using AnyDesk
5. Data staging via archive creation
6. Ransomware deployment and execution
7. Backup destruction using shadow copy deletion
8. Post-execution cleanup of ransomware binary

Key Indicators of Compromise

Malware File: updater.exe

`SHA256: e609d070ee9f76934d73353be4ef7ff34b3ecc3a2d1e5d052140ed4cb9e4752b`

`Shadow Copy Deletion Command: vssadmin delete shadows /all /quiet`

`Credential Discovery Command: tasklist | findstr lsass`

Detection Opportunities

1. Monitor LOLBin usage (certutil, PowerShell, bitsadmin)
2. Detect credential discovery commands targeting LSASS
3. Alert on shadow copy deletion activity
4. Identify suspicious archive creation in staging directories
5. Correlate process execution with abnormal file activity

Conclusion

This investigation demonstrates how structured threat hunting using endpoint telemetry can reconstruct ransomware activity and identify early indicators of compromise.