Pudi Thrimurthi Sai Tarun - Senior Threat Hunter

Professional Summary

Senior Cyber Threat Hunter with Strong expertise in proactive Threat Detection, Anomaly based hunting, EDR Telemetry analysis, SIEM correlation and Intelligence-driven detection engineering.

Experienced in building detections from scratch, validating real world attacker tradecraft, documenting & communicating hunting outcomes to technical and leadership stakeholders.

Core Skills

- Threat Hunting
- Cyber Threat Intelligence (CTI)
- Detection Engineering
- CrowdStrike Falcon
- SIEM
- Endpoint Telemetry
- MITRE ATT&CK
- Network Traffic Analysis

Threat Hunt Case Study #1 Suspected RCE Exploitation on IIS / SharePoint via w3wp.exe (ZDV-2025-0708 | CVE-2025-53770)

Hypothesis

Adversaries may exploit a Remote Code Execution Vulnerability in IIS-hosted Sharepoint applications to execute arbitrary commands abusing the IIS worker process w3wp.exe Successful exploitation is expected to result in w3wp.exe spawning command interpreters or scripting engines to execute attacker-supplied payloads, often using encoded command lines to evade detection.

This behavior is inconsistent with normal IIS or SharePoint application execution and aligns with post-exploitation of RCE.

Telemetry Used

- CrowdStrike Falcon EDR process Telemetry
- Command line Execution Metadata
- Encoded PowerShell execution Indicators

Hunting Approach

The Hunt focused on identifying abnormal process execution chains originating from IIS worker processes.

- Queried for instances where w3wp.exe spawned command line interpreters (cmd.exe) or scripting engines.
- Analysis of child process command lines for encoded PowerShell execution, indicating obfuscation and payload staging.
- Performed command line decoding to identify obfuscated PowerShell payload execution, the activity originated from a web Application process rather than Admin Maintenance.
- Correlated observed behavior with known exploitation patterns through Threat Intel.

The observed execution chain showed w3wp.exe spawning cmd.exe, which in turn executed encoded PowerShell commands

Key Findings

The activity was blocked by CrowdStrike, preventing further execution. Analysis indicates a high-confidence malicious event consistent with successful RCE exploitation against an IIS / SharePoint server.

Based on decoded payload characteristics and execution intent, the suspected web shell capability included:

- Extraction of SharePoint machine keys
- Arbitrary command execution

Outcome

This hunt validated a critical attack path against internet-facing web infrastructure and reinforced the need for:

- Immediate patch Validation for the Critical Vulnerability
- Dedicated detection & enhanced alerting for encoded command execution originating from web server processes.

The hunting logic was retained for reuse and future detection hardening across SharePoint-hosting environments.

MITRE ATT&CK Alignment

- T1190 – Exploit Public-Facing Application
- T1059 – Command & Scripting Interpreter
- T1027 – Obfuscated/Encoded Files or Information

Threat Hunt Case Study #2 Detection of External reconnaissance against exposed Server.

Hypothesis

An Internet exposed DNS Service, port 53 on a client server can be leveraged by adversaries for Reconnaissance, pre-exploitation probing.

Hunt Trigger

- While reviewing Attack Surface Reduction reports, identify an open port on a Client managed node server. When initiated Port Scan for Internet facing subnet through Censys, uncovered no Access restriction for DNS service on this public facing server.
- Further uncovered that the port 53 is accessible for everyone through Internet.

Hunting Approach

- DNS traffic analysis through SIEM uncovered high volume DNS ANY queries & authentication requests pointing to the server IP, posing DNS poisoning risk.
- Correlated reconnaissance patterns across inbound DNS telemetry and identified repeated probing activity from multiple external sources
- Attempts patterns aligned with automated scanning frameworks which can pose potential risk to the Infra.

Detection Logic

Service = '53'

AND

Direction = 'Inbound'

AND

Dns.qtype = 'ANY'

| groupby ip.dst, ip.src

| having count(sessionid) > 100

Action Taken & Outcome

Immediately raised priority Security Advisory to inform respective stakeholders & leadership about the Security Misconfiguration and Attack Surface Risk. Implemented access control and firewall policy updates to limit DNS communication to authorized internal sources only.

- Reduced risk of exposed DNS Attack surface & prevented potential Multi-staging exploit on public facing servers.
- Integrated the Detection logic use-case into SIEM, detecting exposed DNS services across Infra Assets further.

MITRE ATT&CK Alignment

- T1595 – Active Scanning
- T1046 – Network Service Discovery
- T1590 – Gather Victim Network Information