Alerts to Adversaries — Capstone Report

Student Name: Marty Schneider (marty.schneider@gmail.com)
Date: 10/20/25
Host(s) Investigated: Asgard-Wrkstn, Wakanda-Wrkstn, Earth-DC

Scenario Overview -Chronological

Initial Access (Asgard-Wrkstn, ~16:34 UTC, user panther): Attacker likely gained access via phishing, using mshta.exe to execute cmd.exe and download/run receipt.hta (phishing payload) from Downloads folder. This triggered a living-off-the-land chain: powershell.exe to cmd.exe to mshta.exe (twice) to recursive powershell.exe running conhost.exe and dllhost.exe, likely for registry modification and payload staging.
Execution & Defense Evasion (Asgard-Wrkstn, ~16:33-16:37 UTC):

- ~16:33-16:37: PowerShell orchestrated automated script execution without human interaction.
- ~16:36: win-svc.exe (illegitimate) created Cobalt Strike named pipes (MSSE-1380-server, mojo) via dllhost.exe for C2 and obfuscation.
- ~16:36: rundll32.exe (PID 7884) made 100 rapid connections to internal IPs (172.19.146.215:47873 ↔ 172.19.152.7:19455), indicating C2 beaconing or data exfiltration.
- ~16:37: Rubeus v1.0 executed via PowerShell for Kerberos ticket theft/forgery (T1558.001), enabling privilege escalation.

Privilege Escalation (Asgard-Wrkstn, post-16:37 UTC): Kerberos exploitation via Rubeus provided elevated credentials (transition to user thor), setting up for lateral movement.
Lateral Movement (Wakanda-Wrkstn → Asgard-Wrkstn, ~09:13-09:43 local / ~14:13-14:43 UTC, user thor):

- ~09:13 local: From Wakanda, svchost.exe injected into wsmprovhost.exe (-embedding flag) for process hiding.
- ~09:43 local: PowerShell remoted from Wakanda (thor) to Asgard, spawning powershell.exe to conhost.exe/dllhost.exe; reciprocated to Wakanda (panther), running cmd.exe to conhost.exe to wevutil.exe (event log manipulation) for obfuscation.

Persistence (Wakanda-Wrkstn, post-lateral): WMI event subscription (namespace /root/subscription via svchost.exe) created twice: "A2A-Per" trigger 30-90s post-boot to execute rmm.exe from Temp folder for backdoor persistence (T1546.003).

Objective: Domain Compromise (Earth-DC, post-persistence): Elevated thor accessed DS objectserver on domain controller (Earth-DC.marvel.local), enabling DCSync (credential dumping).

Technical Details

Investigated Alerts

Alert Name: Non-Standard Network Connections

Host Investigated: Asgard-Wrkstn.marvel.local

MITRE ATT&CK Tactic / Technique: Defense Evasion / T1218

Observation:

Over the course of approximately 17 minutes, rundll32.exe process makes a network connection 100 times between the following IPs starting at 2025-10-09T16:36:22.0150000Z

172.19.146.215:47873

172.19.152.7:19455

PID: 7884

Classification:

True Positive: While rundll32.exe making a network connection is itself not suspicious, it is suspicious for it to be done repeatedly over a short period of time.

Notes:

Alert Name: Remote Thread Creation

Host Investigated: Asgard-Wrkstn.marvel.local

MITRE ATT&CK Tactic / Technique: T1059.001 – Command and Scripting Interpreter: Powershell / T1059.003 – Windows Command Shell / T1218.010 – Mshta

Living off the land

Observation:

At 2025-10-09T16:33:57.7090000Z over the course of about 4 minutes, user panther ran powershell.exe to use cmd.exe which then executed mshta.exe twice. Mshta.exe then executes powershell.exe and powershell.exe executes conhost.exe and dllhost.exe. Powershell.exe then executes itself and executes conhost.exe again. Likely to modify registry.

Classification:

True Positive – Chain of attacks orchestrated with powershell and leveraging cmd.exe and mshta suggest a living off the land attack. Quick execution without any human input suggests an automated script.

Notes:

Alert Name: mshta executions

Host Investigated: Asgard-Wrkstn.marvel.local

MITRE ATT&CK Tactic / Technique: T1218.010 – mshta

Observation:

At 2025-10-09T16:34:10.0380000Z: user panther executes mshta.exe to execute cmd.exe to execute receipt.hta. the next event is similar where mshta.exe executes cmd.exe to download receipt.hta file into downloads. Highly suspicious and highly likely malicious.

Classification:

Label your conclusion (e.g., True Positive, Benign, False Positive, Informational) and justify it with reasoning or supporting data.

True Positive: receipts.hta file looks like phishing and is downloaded to downloads folder.

Notes:

Alert Name: Cobalt Strike Named Pipes

Host Investigated: Asgard-Wrkstn.marvel.local

MITRE ATT&CK Tactic / Technique: T1059.003 – Windows Command Shell / T1134.001 – Access Token Manipulation / T1027.002 – Obfuscated Files / T1570 – lateral tool Transfer

Observation:

At 2025-10-09T16:36:19.7100000Z, user panther executes win-svc.exe (not legitimate) to create Named Pipe MSSE-1380-server. The next event uses dllhost.exe to create named pipe mojo.5688.8052.18389493978708887759.

Classification:

True Positive: Uses illegitimate win-svc.exe to create named pipes with random suffixes to hide activity.

Notes:

Alert Name: Rubeus executed via .NET

Host Investigated: Asgard-Wrkstn.marvel.local

MITRE ATT&CK Tactic / Technique: T1558.001 / Steal or Forge Kerberos Tickets

Observation:

At 2025-10-09T16:37:42.4300000Z, user panther, Rubeus version 1.0 is executed via powershell.exe.

Classification:

Label your conclusion (e.g., True Positive, Benign, False Positive, Informational) and justify it with reasoning or supporting data.

True Positive: Rubeus is a well known Kerberos exploitation.

Notes:

Alert Name: Potential Lateral Movement

Host Investigated: Wakanda-Wrkstn.marvel.local

MITRE ATT&CK Tactic / Technique: T1559.001

Observation:

At Oct 9, 2025 9:13:11 AM local time, user thor, initiates svchost.exe which in turn creates a new wsmprovhost.exe process with -embedding flag suggesting an injection.

Classification:

True Positive: The -embedding flag shows malicious intent by trying to hide newly created process. We also see another workstation involved showing lateral movement.

Notes:

Alert Name: Remote thread creation

Host Investigated: Asgard-Wrkstn.marvel.local and Wakanda-Wrkstn.marvel.local

MITRE ATT&CK Tactic / Technique: T1021.006 – Remote services

Observation:

At Oct 9, 2025 9:43:01 AM local time, user thor, uses powershell.exe to execute powershell on “asgard” which in turn creates a new event where powershell executes conhost.exe and then another event where powershell executes dllhost.exe. This then leads user panther to execute powershell.exe on a separate host “wakanda” that runs cmd.exe. cmd.exe then runs conhost.exe and then wevutil.exe.

Classification:

True Positive: Clear lateral movement between two workstations and two users running new threads as evidenced above.

Alert Name: WMI Event Subscription

Host Investigated: Wakanda-Wrkstn.marvel.local

MITRE ATT&CK Tactic / Technique: T1546.003 – Event Triggered Execution

Observation:

Twice an event is subscribed to from namespace /root/subscription using svchost.exe. The event is set to trigger between 30-90 seconds after boot up and runs rmm.exe from the Temp folder. Highly suspicious!

Classification:

True Positive: An event is subscribed to called A2A-Per (short for Alerts to Adversaries – Persistence :P)

Notes:

Alert Name: Possible DCSync

Host Investigated: Earth-DC.marvel.local

MITRE ATT&CK Tactic / Technique: T1003.006 – OS Credential dump

Observation:

User thor access an object on a third machine DS objectserver

Classification:

True Positive: An event is subscribed to called A2A-Per (short for Alerts to Adversaries – Persistence :P)

Notable Activity (Non-Alerted Findings)

I left this blank as I was unable to get any KQL query to work on my own. Not sure what was happening but Advanced hunting just ran my queries and returned nothing even when I know for a fact that at least one thing should have come back.

A basic PID query for a PID I found above simply returned nothing.

Attack Name:

Host Investigated:

MITRE ATT&CK Tactic / Technique:

Observation:

Summarize suspicious or malicious activity you uncovered outside of alerts (e.g., persistence, credential access, log tampering, lateral movement).

KQL Query:

Include the query you used to find this telemetry.

Notes:

Record investigative context, supporting events, correlations to other stages, or recommendations for new detections.

Additional Notes

Unclear exactly where the hta file was downloaded from although its possibly from one of the two IPs at the beginning of the chain.

Containment Strategy

Remove internet access from the affected machines.
Go into registry and delete the event persistence mechanisms that are allowing the malicious processes to run after bootup.
Delete the hta file that introduced the malicious processes.
Blacklist the IPs that the systems were trying to reach.
Reset passwords for affected users.