SECURITY INCIDENT REPORT

Sysmon + Splunk Detection Engineering Lab

Suspected Post-Exploitation Activity: Discovery, Credential Access & Persistence on SOC-Lab-Win11

Incident ID	LAB-2026-0804-01	**Severity**	Medium (Simulated)
Date Detected	August 4, 2026	**Status**	Closed - Simulated / Lab Exercise
Analyst	SOC Lab Project	**Affected Host**	SOC-Lab-Win11
Detection Source	Splunk (Sysmon + Windows Defender)	**MITRE Tactics**	Discovery, Credential Access, Persistence

1. Executive Summary

On August 4, 2026, detection logic built in Splunk identified a sequence of process activity on host SOC-Lab-Win11 consistent with a post-compromise attack chain spanning three MITRE ATT&CK tactics: Discovery, Credential Access, and Persistence. The activity began with system reconnaissance commands, progressed to an attempt to access cached credentials via the Windows Credential Manager, and concluded with the creation of two scheduled tasks configured to execute on user logon and system startup.

This activity was generated intentionally as part of a controlled home-lab exercise using the Atomic Red Team framework to simulate real adversary techniques against a Windows 11 virtual machine instrumented with Sysmon and forwarded to Splunk Enterprise. No real compromise occurred and no production systems were involved. The purpose of this report is to document the detection, investigation, and response process the way it would be handled against a genuine intrusion.

Separately, Windows Defender's real-time protection independently flagged and quarantined a number of process-injection and credential-dumping tools that were staged on disk during the exercise, before those specific techniques could execute. This is noted in the timeline as evidence of layered defense operating alongside SIEM-based detection.

2. Detection Summary

Detection Method: Custom SPL correlation searches against Sysmon (Process Create, EventCode 1) and Windows Defender Operational log telemetry, saved as reports in Splunk.

Data Sources: Sysmon EventCode 1 (Process Create); Windows Defender Operational log (EventCode 1116/1117); Windows Security Event Log.

Techniques Identified: T1082 (System Information Discovery), T1003.005 (Credential Dumping: Cached Domain Credentials), T1053.005 (Scheduled Task), T1055/T1003 (Process Injection / Credential Dumping tooling, blocked).

3. Timeline of Events

All times shown in local system time (host clock). Events are ordered chronologically as observed in Splunk.

Time	Technique	Event
09:47 AM	**T1082**	Process creation observed: powershell.exe spawns cmd.exe, which executes

Time	Technique	Event
		systeminfo and a registry query against HKLM\SYSTEM\CurrentControlSet\Services\Disk. Consistent with post-access environment reconnaissance.
10:55 AM	**T1003.005**	rundll32.exe executed with keymgr.dll,KRShowKeyMgr, spawned by powershell.exe. Opens the Windows Credential Manager UI, a technique used to surface cached credentials on the host.
11:06 AM	**T1053.005**	schtasks.exe /create executed twice via cmd.exe (parent: powershell.exe), registering two scheduled tasks: one on user logon, one on system startup running as SYSTEM. Consistent with establishing persistence beyond a single session.
Throughout	**T1055 / T1003 (blocked)**	Windows Defender real-time protection flagged and quarantined multiple process-injection and credential-dumping tools on disk (Event IDs 1116/1117) before they could execute, including signatures matching known offensive tooling (e.g. Mimikatz-related, Meterpreter-related).

4. Analysis

4.1 Discovery (T1082)

The activity opened with systeminfo.exe and a registry query targeting disk-related service keys, both launched from cmd.exe with a PowerShell parent process. This is a low-noise, high-value first step for an attacker: it establishes what OS version, patch level, and hardware configuration is in play, informing which follow-on techniques and exploits are viable. The specific registry path queried (Services\Disk) can also indicate an attacker checking for virtualization or sandbox artifacts before proceeding further, a common evasion pattern.

4.2 Credential Access (T1003.005)

Roughly one hour after the initial reconnaissance, rundll32.exe was invoked with the keymgr.dll,KRShowKeyMgr export, spawned directly from a PowerShell process. This is a 'living-off-the-land' technique: rundll32.exe is a legitimate, digitally-signed Windows binary, so this activity would not be flagged by simple allow-list or signature-based tooling. The result is the Windows Credential Manager interface, from which an attacker with local access can view or export stored credentials for websites, mapped drives, and applications. The use of a trusted system binary to reach sensitive credential material is precisely why process-lineage-based detection (parent-child relationships, not just the binary name) is necessary.

4.3 Persistence (T1053.005)

Approximately eleven minutes after the credential access attempt, two scheduled tasks were created via schtasks.exe, again spawned through a cmd.exe/PowerShell lineage. One task was configured to trigger on user logon; the second was configured to trigger on system startup and, notably, to run under the SYSTEM account rather than the current user context. A standard user account creating a SYSTEM-level scheduled task is a significant privilege-boundary violation and one of the strongest single indicators in this entire chain, since legitimate user activity rarely has cause to do this. Both tasks were configured to launch cmd.exe, which in a real intrusion would typically be swapped for a malicious payload or beacon.

4.4 Blocked Activity: Process Injection & Credential Dumping Tooling (T1055 / T1003)

Independent of the chain above, Windows Defender's real-time protection engine identified and quarantined a number of files matching known offensive-tooling signatures during the exercise, including detections consistent with Mimikatz-derived credential dumping utilities and Meterpreter-style injection tooling. These were blocked at the file

level before the associated Atomic Red Team tests could execute. This activity is included in this report because it demonstrates that endpoint defenses and SIEM-based detection are complementary layers: a mature security posture should not rely on either one alone, and correlating AV block events with attempted technique execution is valuable context for scoping the true extent of an intrusion.

5. Impact Assessment

This activity took place entirely within an isolated lab virtual machine with no connection to production systems, real user data, or external networks. As such, the realized impact is none.

Had this chain occurred against a real production endpoint, the potential impact would be assessed as Medium to High, on the following basis:

- Discovery activity alone provides an attacker with actionable intelligence but no direct impact.
- Successful credential access via Credential Manager could expose cached web, application, or network credentials, enabling lateral movement or account takeover.
- A SYSTEM-level scheduled task represents a durable foothold that would survive user logoff, password resets (unless the underlying account is disabled), and standard reboots, and would require deliberate task removal to fully remediate.
- The presence of process-injection and credential-dumping tooling on disk, even if blocked, suggests the actor's toolkit and intent extended beyond what ultimately executed successfully, and warrants a wider compromise assessment in a real incident.

6. Response Actions Taken (Simulated)

The following response actions were documented as though this were a live incident, for the purposes of this exercise:

- Isolated the affected host from the network to prevent potential lateral movement or C2 callback (simulated - lab VM was already isolated).
- Reviewed the two scheduled tasks created (T1053_005_OnLogon, T1053_005_OnStartup) and documented their configuration for removal.
- Captured and preserved the full Sysmon process-creation chain and Windows Defender detection log entries as evidence, exported from Splunk.
- Cross-referenced all identified techniques against MITRE ATT&CK to confirm tactic/technique mapping and to inform the recommendations below.
- Verified no successful outbound network connections were associated with the credential access or persistence activity (would be reviewed in DNS/proxy/firewall logs in a full deployment; not in scope for this lab's current data sources).

7. Recommendations

7.1 Detection Improvements

- Convert the four saved SPL searches used in this investigation into scheduled, alerting correlation searches (requires an Enterprise license; not available on the current Free/Trial license used in this lab).
- Add a dedicated detection for scheduled tasks created with /ru system by a non-SYSTEM parent process, since this specific pattern was the single strongest indicator in the chain and deserves its own high-confidence alert rather than a general schtasks.exe search.
- Extend log coverage to include DNS and network connection telemetry (e.g. via Zeek or Sysmon EventCode 3) to close the gap on command-and-control or exfiltration detection noted in Section 6.

7.2 Preventive Controls

- Restrict interactive use of rundll32.exe with uncommon DLL/export combinations via Windows Defender Application Control or AppLocker rules, where operationally feasible.
- Apply least-privilege task-creation policies so that standard user accounts cannot register scheduled tasks configured to run as SYSTEM.
- Continue leveraging Windows Defender's real-time protection as a first line of defense, and ensure detection engineering treats AV block events as a data source in their own right, not just a suppressor of alerts.

7.3 Process Improvements

- Document detection logic ordering carefully when using case()-style conditional logic in SPL: broader conditions listed before more specific ones can silently miscategorize events, as encountered while building the dashboard for this exercise.
- Maintain a living MITRE ATT&CK coverage map (technique to detection to test) to track and prioritize gaps, rather than building detections ad hoc.

8. Conclusion

This exercise successfully demonstrated an end-to-end detection and investigation workflow: generating realistic adversary behavior with Atomic Red Team, capturing it through Sysmon and Windows Defender telemetry forwarded into Splunk, building and debugging SPL detection logic, visualizing it on a live dashboard, and documenting it in the format expected of a SOC analyst investigating a real incident. The techniques covered (T1082, T1003.005, T1053.005, and the blocked T1055/T1003 activity) span three distinct MITRE ATT&CK tactics, reflecting a realistic, if compressed, attack progression from initial reconnaissance through to persistence.