

T1027 Obfuscated PowerShell Execution

Incident Report: [HIGH] - T1027 Obfuscated PowerShell Execution

Analyst: Shewag Bhattarai

Date: February 13, 2026

Status: True Positive / Resolved

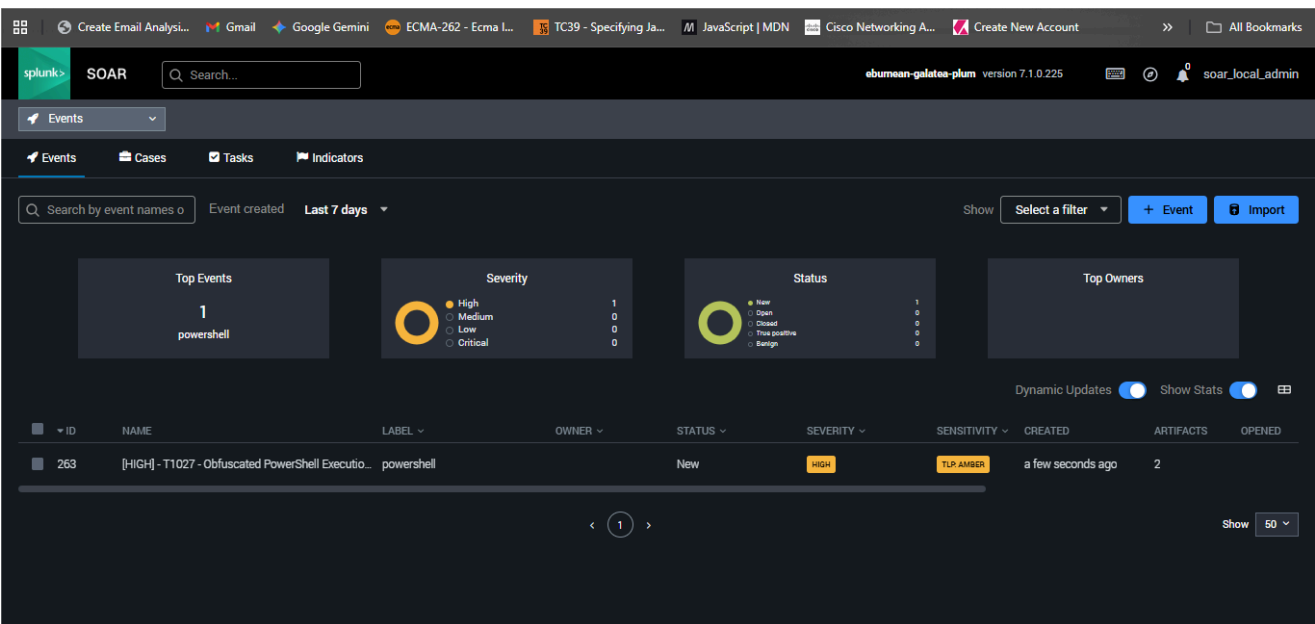
1. Executive Summary

On February 13, 2026, a high-severity alert was triggered via the Splunk SIEM identifying obfuscated PowerShell execution on a Windows endpoint. Investigation confirmed that an attacker (emulated via Atomic Red Team) utilized Base64 encoding to mask administrative reconnaissance commands. The incident was successfully triaged in Splunk SOAR, and the host was verified for containment.

2. Detection & Telemetry (The Identification Phase)

The attack was captured using **Sysmon Event ID 1 (Process Creation)**.

- **Extraction:** The Wazuh agent forwarded the logs to Splunk.
- **Detection Logic:** A scheduled Splunk search identified the `-EncodedCommand` flag.
- **SOAR Ingestion:** Data was mapped to CEF fields and pushed to Splunk SOAR for triage.



3. Technical Analysis (The Investigation Phase)

The primary artifact was an encoded string:

```
bgBlAHQAIABsAG8AYwBhAGwAZwByAG8AdQBwACAAAYQBkAG0AaQBuAGkAcwB0AHIAIYQB0AG8AcgBzAA==.
```

Analysis Steps:

1. **Field Extraction:** Extracted the Encoded string artifact in SOAR.
2. **Decoding:** Utilized CyberChef with a From Base64 and Decode text (UTF-16LE) recipe to strip null bytes.
3. **Findings:** The decoded command was `net localgroup administrators.`

The screenshot shows the Splunk SOAR interface. The top navigation bar includes the Splunk logo, 'SOAR', a search bar, and the user 'soar_local_admin'. The main header indicates the investigation is titled '[HIGH] - T1027 - Obfuscated PowerShell Execution (Base64)' with a severity of 'HIGH'. The left sidebar shows 'Recent Activity' with events from 'soar_local_admin'. The main panel displays the artifact details for ID 550, including its name, label, source ID, start time, and a list of fields: Encoded string, Executed Command, .originating_search, destinationUserName, rid, sid, and tag. The 'Encoded string' field contains the Base64-encoded command.

The screenshot shows the CyberChef web interface. The 'Recipe' panel on the left includes a 'From Base64' step with the alphabet 'A-Za-z0-9+/' and checkboxes for 'Remove non-alphabet chars' and 'Strict mode'. Below it is a 'Decode text' step with the encoding 'UTF-16LE (1200)'. The 'Input' panel on the right shows the encoded string. The 'Output' panel at the bottom displays the decoded command: `net localgroup administrators|`.

4. MITRE ATT&CK Mapping

- **Execution:** T1059.001 (Command and Scripting Interpreter: PowerShell)
- **Defense Evasion:** T1027 (Obfuscated Files or Information)
- **Discovery:** The activity also maps to Local Group Discovery (T1087.002) based on the intent to identify administrators.

5. Timeline & Closure

- **15:40:** Alert triggered in Splunk and ingested into SOAR.
- **15:44:** Analyst assigned and moved ticket to Open .
- **15:52:** Payload decoded; confirmed malicious intent to discover admin groups.
- **15:56:** Incident closed as **True Positive**.