INCIDENT RESPONSE REPORT

Subject: LOLBins Abuse

Incident ID: IR-2025-1230-011

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 30, 2025

Incident ID	IR-2025-1230-011
Date	December 30, 2025
Severity	**High**
Status	Closed (Lab Simulation)

1. Project Overview and Goal

- This project demonstrates the detection of **"Living Off The Land" (LOLBins)** attacks, where adversaries use legitimate, pre-installed operating system tools to perform malicious actions. Specifically, the Windows binary `certutil.exe` was abused to download a simulated malicious payload from an external source.
- The goal was to engineer a behavioral detection rule in the Wazuh SIEM to identify this activity, even if the payload itself bypasses signature-based antivirus defenses.

2. Lab Architecture

- **Attacker Vector:** Local Command Execution (Simulated Insider/Compromised Host)
- **Victim System:** Windows 11 (Endpoint with Wazuh Agent)
- **Security Tools:** Microsoft Defender (EPP), Wazuh Manager (SIEM)
- **Detection Method:** Behavioral Analysis (Command Line Arguments)

3. Objectives:

- Simulate a file download attack using a trusted Microsoft binary (`certutil.exe`).

- Analyze how Endpoint Protection (Microsoft Defender) reacts to known abuse patterns.
- Create and validate a custom SIEM rule to detect the specific argument pattern (`-urlcache`, `-split`).
- Map the activity to the MITRE ATT&CK framework.

4.Malware Behavior Simulation

A command was executed to mimic a "dropper" downloading a payload from a C2 server.

- **Tool:** `certutil.exe` (Certificate Authority Utility)
- **Command:** `certutil.exe -urlcache -split -f https://www.google.com/robots.txt malicious_test_2.txt`
- **Behavior:** The command attempts to connect to the internet, fetch a file, and save it to the disk using the `-split` flag to handle the file content.

5. Detection & Analysis

The investigation revealed a multi-layered defense response:

Layer 1: Endpoint Protection (Microsoft Defender)

- Upon execution, Microsoft Defender immediately blocked the process.
- **Event ID:** 1116 (Malware Detection)
- **Threat Name:** `Trojan:Win32/Ceprolad.A`

- **Outcome:** The command failed with `Access is denied` and `ResourceUnavailable` errors in the terminal.

Layer 2: SIEM Detection (Wazuh)

- To validate SIEM visibility, Real-Time Protection was temporarily disabled to allow log generation.
- **Log Source:** Event ID 4688 (Process Creation)
- **Custom Rule Logic:** Detected the combination of `certutil.exe` with `urlcache` and `http` arguments.
- **Result:** High-Severity Alert generated in the Wazuh Dashboard.

6. MITRE ATT&CK Mapping

- **T1105** – Ingress Tool Transfer (Downloading the file)
- **T1218** – System Binary Proxy Execution (Using `certutil` to hide activity)

7. Incident Response & Remediation

- **Containment:** The endpoint was isolated (simulated) to prevent lateral movement.
- **Eradication:** The downloaded file `malicious_test_2.txt` was identified and deleted.

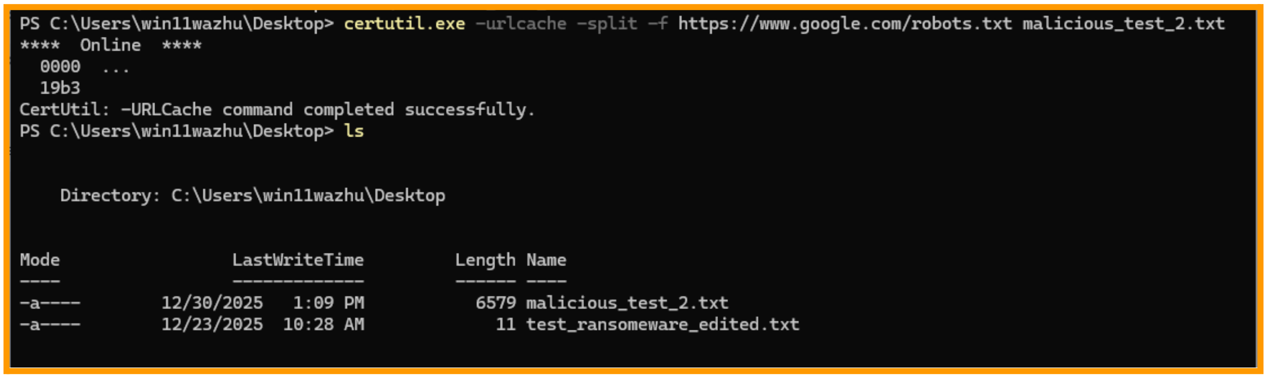
- **Tuning:** Validated that the custom Wazuh rule triggers only on the *combination* of internet flags to prevent false positives from legitimate certificate updates.

8. Conclusion

This project highlights the necessity of **Defense in Depth**. While signature-based AV (Defender) successfully caught the specific tool usage in this instance, sophisticated attackers often obfuscate commands to bypass these signatures.

The implementation of behavioral SIEM rules provides a critical safety net, ensuring that even if the "tool" is allowed, the "behavior" (downloading files from the web via certutil) is detected.

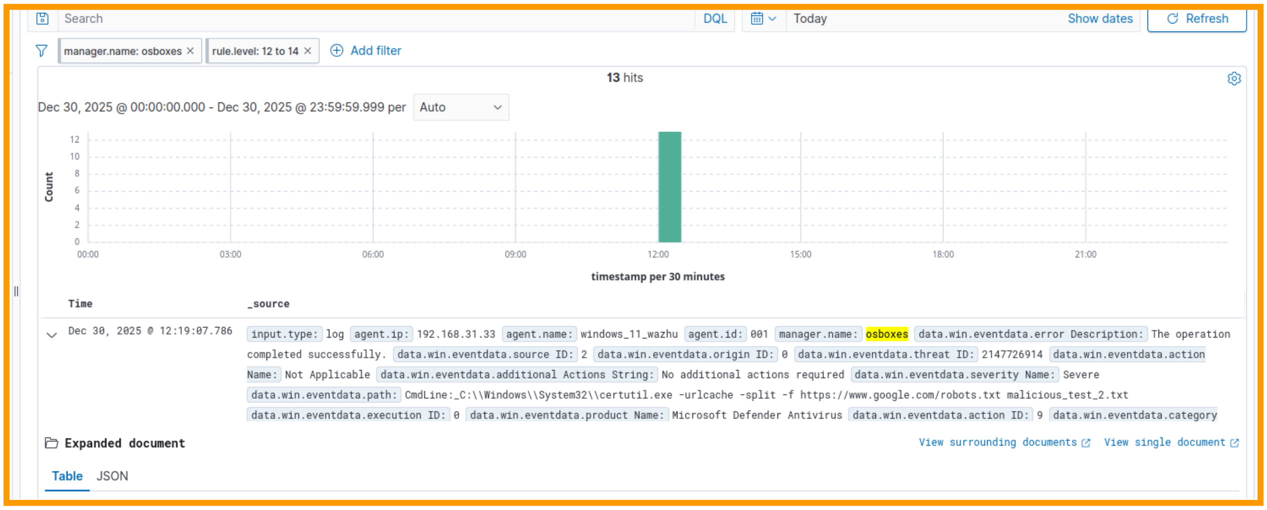
9. Evidence



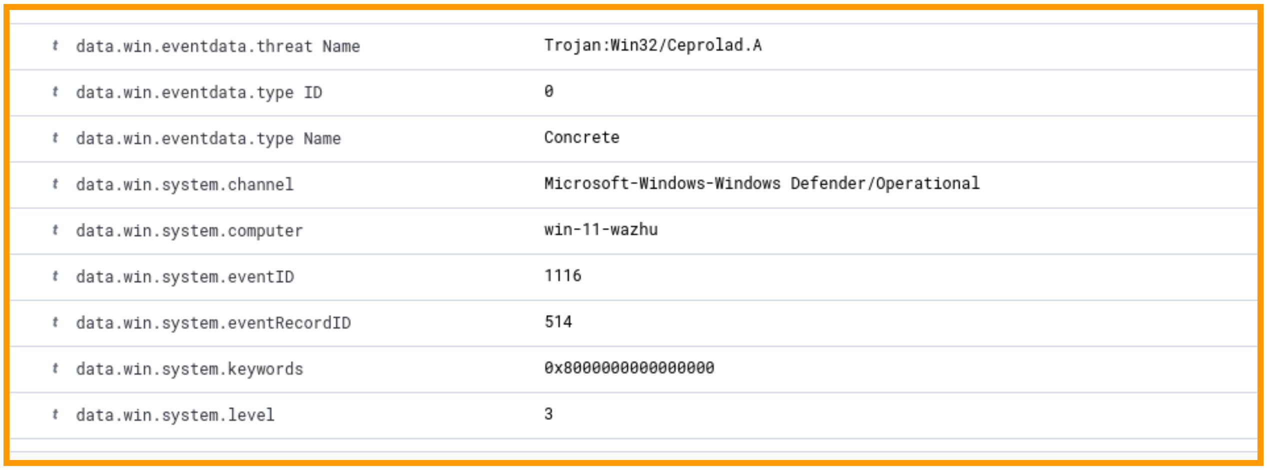
```
PS C:\Users\win11wazhu\Desktop> certutil.exe -urlcache -split -f https://www.google.com/robots.txt malicious_test_2.txt
****  Online  ****
  0000  ...
  19b3
CertUtil: -URLCache command completed successfully.
PS C:\Users\win11wazhu\Desktop> ls


    Directory: C:\Users\win11wazhu\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/30/2025   1:09 PM           6579 malicious_test_2.txt
-a----        12/23/2025  10:28 AM             11 test_ransomeware_edited.txt
```



```
Dec 30, 2025 @ 12:19:07.786   input.type: log agent.ip: 192.168.31.33 agent.name: windows_11_wazhu agent.id: 001 manager.name: osboxes data.win.eventdata.error Description: The operation
completed successfully. data.win.eventdata.source ID: 2 data.win.eventdata.origin ID: 0 data.win.eventdata.threat ID: 2147726914 data.win.eventdata.action
Name: Not Applicable data.win.eventdata.additional Actions String: No additional actions required data.win.eventdata.severity Name: Severe
data.win.eventdata.path: CmdLine:_C:\\Windows\\System32\\certutil.exe -urlcache -split -f https://www.google.com/robots.txt malicious_test_2.txt
data.win.eventdata.execution ID: 0 data.win.eventdata.product Name: Microsoft Defender Antivirus data.win.eventdata.action ID: 9 data.win.eventdata.category
```



t	data.win.eventdata.threat Name	Trojan:Win32/Ceprolad.A
t	data.win.eventdata.type ID	0
t	data.win.eventdata.type Name	Concrete
t	data.win.system.channel	Microsoft-Windows-Windows Defender/Operational
t	data.win.system.computer	win-11-wazhu
t	data.win.system.eventID	1116
t	data.win.system.eventRecordID	514
t	data.win.system.keywords	0x8000000000000000
t	data.win.system.level	3