SOC Use Case Report

UC-030: CertUtil Download with VerifyCtl & Split Arguments

Author	Abishek V
Date	07 February 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Logs / Process Telemetry
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-030
Use Case Name	CertUtil Download with VerifyCtl & Split Arguments
Category	Living-off-the-Land / Defense Evasion
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	High

CertUtil can abuse the `-verifyctl` argument to download remote files while appearing to perform certificate trust list operations. Attackers commonly pair this with split arguments to evade detection.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User: `clair`
- Process observed: `certutil.exe`
- Activity: Remote file download using VerifyCtl

SOC risk point: VerifyCtl misuse is rarely legitimate on user endpoints and strongly indicates malicious staging.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs
- Process creation logs (4688)
- Network telemetry

Key Indicators

certutil.exe Execution	LOLBAS utility used
VerifyCtl Argument	Remote content retrieval
Split Arguments	Obfuscated command-line
Suspicious Output	File written to temp or user path

4. Detection Logic

Trigger when:

- `certutil.exe` executes with `-verifyctl` argument
- command-line shows argument splitting or obfuscation

5. SOC L1 Playbook

Phase A: Triage

1. Reconstruct full command-line execution

2. Identify remote source and output path
3. Confirm user and endpoint context

Phase B: Investigation

1. Validate destination URL reputation
2. Inspect downloaded file type and hash
3. Check for follow-on execution
4. Scope for similar CertUtil usage

6. Evidence Timeline

Time	Event ID	Process	Observation
16:02:13	4688	certutil.exe	VerifyCtl download command executed
16:02:28	–	network	External file retrieved
16:02:44	4688	powershell.exe	Execution attempt detected

Outcome: CertUtil VerifyCtl misuse detected. Classified as high-risk LOLBAS activity.

7. False Positive Checks

- legitimate certificate trust list updates
- approved PKI administrative scripts
- controlled lab or testing activity

8. Verdict Criteria

True Positive if:

- downloaded file is executable or script
- source is untrusted
- follow-on execution observed

9. SOC Response Actions

- quarantine downloaded file
- block destination URL/IP
- isolate endpoint if execution occurred
- escalate to incident response

10. Ticket Notes

Ticket: UC-030 CertUtil VerifyCtl Download Detected
Severity: High
Verdict: True Positive