SOC Use Case Report

UC-029: CertUtil Download with URLCache & 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-029
Use Case Name	CertUtil Download with URLCache & Split Arguments
Category	Living-off-the-Land / Defense Evasion
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	High

Attackers abuse CertUtil with URLCache and split arguments to download payloads in a way that bypasses simple command-line detections and blends into legitimate administrative usage.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User: `clair`
- Process observed: `certutil.exe`
- Activity: File downloaded using URLCache and split arguments

SOC risk point: Split arguments are commonly used to evade static detection rules.

3. Telemetry and Evidence

Primary logs

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

Key Indicators

certutil.exe Execution	LOLBAS binary used
URLCache Argument	Remote file retrieval
Split Arguments	Obfuscated command-line structure
Suspicious Output	File written to temp or user path

4. Detection Logic

Trigger when:

- `certutil.exe` executes with URLCache-related arguments
- command-line shows argument splitting or obfuscation

5. SOC L1 Playbook

Phase A: Triage

1. Review full reconstructed command line
2. Identify source URL and output file path

3. Confirm user and endpoint context

Phase B: Investigation

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

6. Evidence Timeline

Time	Event ID	Process	Observation
15:09:44	4688	certutil.exe	URLCache download command executed
15:09:58	–	network	External payload retrieved
15:10:11	4688	cmd.exe	Execution attempt detected

Outcome: Obfuscated CertUtil download detected. Classified as high-risk LOLBAS activity.

7. False Positive Checks

- approved certificate management tasks
- trusted administrative scripts
- controlled lab or testing activity

8. Verdict Criteria

True Positive if:

- downloaded file is executable or script
- source URL 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-029 CertUtil URLCache Download Detected
Severity: High
Verdict: True Positive