SOC Use Case Report

UC-028: CertUtil with Decode Argument

Author	Abishek V
Date	06 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-028
Use Case Name	CertUtil with Decode Argument
Category	Living-off-the-Land / Defense Evasion
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium → High

CertUtil is a built-in Windows utility commonly abused by attackers to decode malicious payloads that were transferred in encoded form to evade detection.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User: `clair`
- Process observed: `certutil.exe`
- Activity: File decoded from Base64 format

SOC risk point: CertUtil decoding activity is rarely required in normal user workflows and is a common malware staging technique.

3. Telemetry and Evidence

Primary logs

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

Key Indicators

certutil.exe Execution	LOLBAS utility detected
Decode Argument	`-decode` or `-decodehex` used
Suspicious Output File	Executable or script created

4. Detection Logic

Trigger when:

- `certutil.exe` executes with decode arguments
- output file is written to user or temp directories

5. SOC L1 Playbook

Phase A: Triage

1. Review full command-line arguments
2. Identify input and output file paths
3. Confirm user and endpoint context

Phase B: Investigation

1. Determine origin of encoded file
2. Review decoded file type and hash
3. Check for follow-on execution
4. Scope for similar activity across environment

6. Evidence Timeline

Time	Event ID	Process	Observation
14:21:06	4688	certutil.exe	Decode command executed
14:21:10	–	filesystem	Payload file written to disk
14:21:18	4688	cmd.exe	Execution attempt observed

Outcome: Unauthorized CertUtil decode activity detected. Classified as suspicious payload staging.

7. False Positive Checks

- legitimate certificate troubleshooting
- approved administrative scripts
- controlled lab or testing activity

8. Verdict Criteria

True Positive if:

- decoded file is executable or script
- source of encoded data is untrusted
- follow-on execution is observed

9. SOC Response Actions

- quarantine decoded file
- block related hash or source
- isolate endpoint if execution occurred
- escalate to incident response

10. Ticket Notes

Ticket: UC-028 CertUtil Decode Detected
Severity: High
Verdict: True Positive