SOFTWARE

Home > Software > esentutl

esentutl

esentutl is a command-line tool that provides database utilities for the Windows Extensible Storage Engine.[1]

ID: S0404

ⓘ Associated Software: esentutl.exe

ⓘ Type: TOOL

ⓘ Platforms: Windows

Contributors: Edward Millington; Matthew Demaske, Adaptforward

Version: 1.3

Created: 03 September 2019

Last Modified: 28 September 2023

Version Permalink

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1005		Data from Local System	esentutl can be used to collect data from local file systems.[2]
Enterprise	T1006		Direct Volume Access	esentutl can use the Volume Shadow Copy service to copy locked files such as `ntds.dit`.[3][4]
Enterprise	T1564	.004	Hide Artifacts: NTFS File Attributes	esentutl can be used to read and write alternate data streams.[3]
Enterprise	T1105		Ingress Tool Transfer	esentutl can be used to copy files from a given URL.[3]
Enterprise	T1570		Lateral Tool Transfer	esentutl can be used to copy files to/from a remote share.[3]
Enterprise	T1003	.003	OS Credential Dumping: NTDS	esentutl can copy `ntds.dit` using the Volume Shadow Copy service.[3][4]

Groups That Use This Software

ID	Name	References
G0114	Chimera	[5]
G1032	INC Ransom	[6][7]
G0045	menuPass	[8]

References

1. Microsoft. (2016, August 30). Esentutl. Retrieved September 3

5. Jansen, W . (2021, January 12). Abusing cloud services to fly