

3CORESec / MAL-CL

Public

Notifications

Fork 43

Star 308

<> Code

Issues

Pull requests

Actions

Security

Insights

Files

master

Go to file

Descriptors

Antivirus

NirSoft Utilities

Other

AdFind

Advanced IP Scanner

Advanced Port Scanner

AnyDesk

CleanWipe

README.md

Defender Control

Defender Exclusion Tool (AKA ...

IntelliAdmin Network Administ...

LaZagne

NBTscan

PAExec

Radmin

Rclone

SoftPerfect Network Scanner

TPAR

Winrar

Sysinternals

Windows 2000 Resource Kit Tools

Windows

Images

Template

LICENSE

README.md

MAL-CL / Descriptors / Other / CleanWipe

nasbench

Update "Versions History" and "File Metadata"

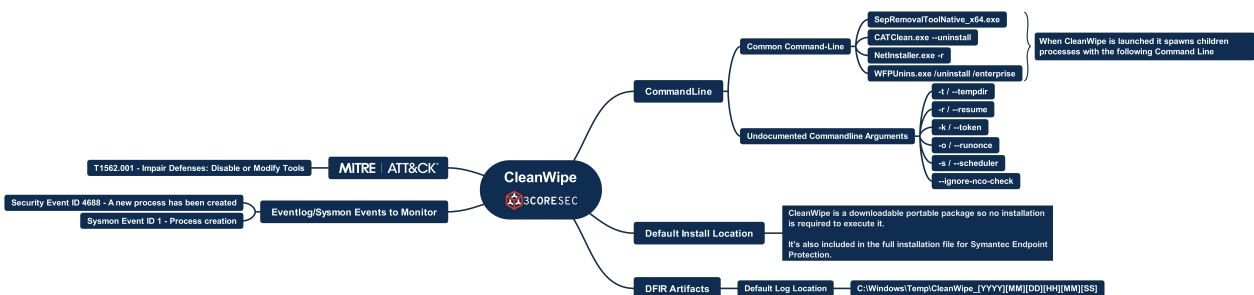
992ad41 · 3 years ago

History

Name	Last commit message	Last commit date
..		
README.md	Update "Versions History" and "File Metad...	3 years ago

README.md

CleanWipe



```
graph LR
    CW((CleanWipe  
3CORESEC)) --- CL[CommandLine]
    CW --- DIL[Default Install Location]
    CW --- DFI[DFIR Artifacts]
    CL --- CCL[Common Command-Line]
    CL --- UCA[Undocumented Commandline Arguments]
    CCL --- SPT[SepRemovalToolNative_x64.exe]
    CCL --- CAT[CATClean.exe --uninstall]
    CCL --- NI[NetInstaller.exe -r]
    CCL --- WPU[WPUUnins.exe /uninstall /enterprise]
    UCA --- T1[T /-tempdir]
    UCA --- T2[T /-resume]
    UCA --- T3[X /-token]
    UCA --- T4[Y /-runonce]
    UCA --- T5[Z /-scheduler]
    UCA --- T6[-ignore-rico-check]
    DIL --- DIL_N1[CleanWipe is a downloadable portable package so no installation is required to execute it.]
    DIL --- DIL_N2[It's also included in the full installation file for Symantec Endpoint Protection.]
    DFI --- DFL[Default Log Location]
    DFL --- DFL_PATH[C:\Windows\Temp\CleanWipe_[YYYY][MM][DD][HH][MM][SS]]
    T1562[T1562.001 - Impair Defenses: Disable or Modify Tools] --- MITRE[MITRE / ATT&CK]
    SEID[Security Event ID 4688 - A new process has been created] --- SEID1[Symon Event ID 1 - Process creation]
    SEID --- ESM[Eventlog/Symon Events to Monitor]
    SEID1 --- ESM
    ESM --- CW
```

Table of Contents

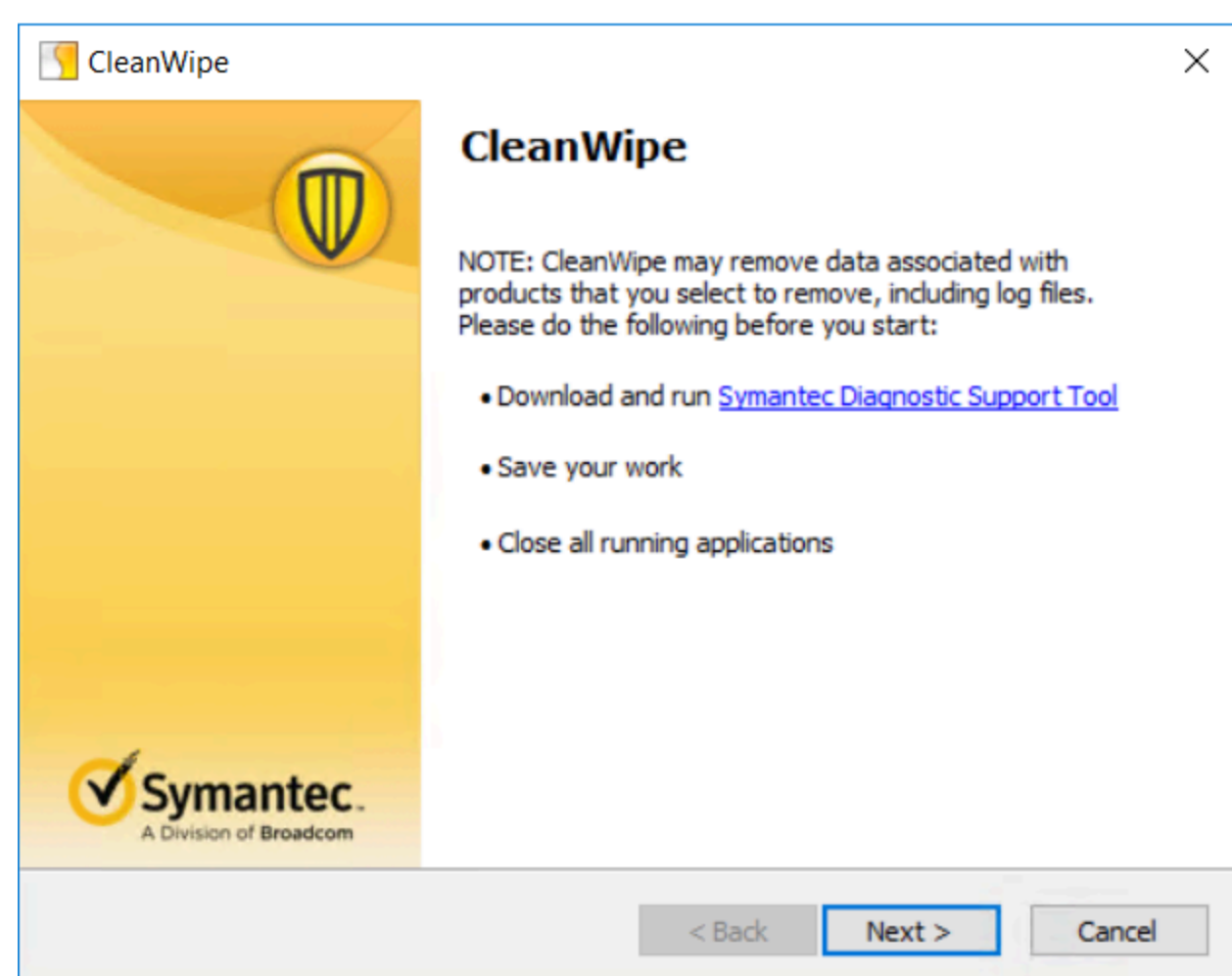
- CleanWipe
 - Table of Contents
 - Acknowledgement(s)
 - Description
 - Versions History
 - File Metadata
 - Common CommandLine
 - Threat Actor Ops (TAOps)
 - Common Process Trees
 - Default Install Location
 - DFIR Artifacts
 - Examples In The Wild
 - Documentation
 - Blogs / Reports References
 - ATT&CK Techniques
 - Telemetry
 - Detection Validation
 - Detection Rules
 - LOLBAS / GTFOBins References

Acknowledgement(s)

- 3CORESec - @3CORESec
- Nasreddine Bencherchali - @nas_bench

Page 1 of 4

Description



Symantec CleanWipe removal tool is a utility that removes any Symantec software, such as Symantec Endpoint Protection

Versions History

Version	SHA1	VT
14.3.5413.3000	cd16723f9c218c543c0c44cab8163714342f167d	LINK

File Metadata

- This metadata information is based on the latest version available as of this writing (14.3.5413.3000):

Attribute	Value
Copyright	Copyright (c) 2021 Broadcom. All Rights Reserved.
Product	Symantec Install Component
Description	CleanWipe
Original Name	CleanWipe.exe
Internal Name	CleanWipe

Common CommandLine

- When CleanWipe is launched it spawns children processes with the following Command Line

```
SepRemovalToolNative_x64.exe

CATClean.exe --uninstall

NetInstaller.exe -r

WFPUnins.exe /uninstall /enterprise
```

- Undocumented Commandline arguments

```
-t / --tempdir
-r / --resume
-k / --token
-o / --runonce
-s / --scheduler
--ignore-nco-check
```



Threat Actor Ops (TAOps)

- TBD

Common Process Trees

- TBD

Default Install Location

- CleanWipe is a downloadable portable package so no installation is required to execute it. It's also included in the full installation file for Symantec Endpoint Protection.

DFIR Artifacts

- Default Log Location

```
C:\Windows\Temp\CleanWipe_[YYYY][MM][DD][HH][MM][SS]
```



Examples In The Wild

- [ANY.RUN - CleanWipe \(SymantecUninstaller\).zip](#)

Documentation

- [Broadcom Techdocs - Download the CleanWipe removal tool to uninstall Endpoint Protection](#)

Blogs / Reports References

- TBD

ATT&CK Techniques

- [T1562.001 - Impair Defenses: Disable or Modify Tools](#)

Telemetry

- [Security Event ID 4688 - A new process has been created](#)
- [Sysmon Event ID 1 - Process creation](#)
- [PsSetCreateProcessNotifyRoutine/Ex](#)
- [ETW - Microsoft-Windows-Kernel-Process - Event ID 1 - ProcessStart](#)

Detection Validation

- TBD

Detection Rules

- TBD

LOLBAS / GTFOBins References

- None