Sign in

3CORESec / **MAL-CL** Public

Notifications | Fork 43 | Star 308

Code | Issues | Pull requests | Actions | Security | Insights

MAL-CL / Descriptors / Other / **CleanWipe** /

Name	Last commit message	Last commit date
..		
README.md		

README.md

CleanWipe

Table of Contents

Acknowledgement(s)

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

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