STRONTIC
Security. Automation. Analytics.

About xCyclopedia Github

Home / Xcyclopedia / Library / **stordiag.exe |**

stordiag.exe

>> File Path: `C:\Windows\SysWOW64\stordiag.exe`

>> Description:

Hashes

Type	Hash
MD5	`1F08FC87C373673944F6A7E8B18CD845`
SHA1	`EB78E97DEE03DC3C2F744A408087AD79FD067219`
SHA256	`B812162F140A347EC78756416302CBC9204EF484FEB7623C0FFF8FF7B4B3EC04`
SHA384	`5FFFDC39EDC75FD6AB1DA10CCA1CBEAD3FAD3A90C0A6105A59BB0165B40708C4C1A177EFD88713535B7B3744A9274793`
SHA512	`428CE4A0C9413D94EA1F9C041C6BA2282D017C6BDE36A28EC96679D439D8202A35AA7D652A78D8C710485C0006F7213E64C7D293BBA103FF3165E5298C804023`
SSDEEP	`1536:qwYYQyn8M801RXnItvNCl/iBeKiZfbOZE4RS8JRFahdqb3BuS:jY28M806enfbOZE4I8JRFEYb3BuS`
IMP	`F34D5F2D4577ED6D9CEEC516C1F5A744`
PESHA1	`A5E5500ACB8F0080F5C37EDDD4E326A39FF84A74`
PE256	`FA81CDCA613277A54823444E28467F1EAB38646AC9AE57FAAE496F1A289E70CF`

Runtime Data

Usage (stdout):

```
Collects storage and filesystem diagnostic logs and outputs them to a folder.

StorDiag [-collectEtw] [-out <PATH>]
-collectEtw                  Collect a 30-second long ETW trace if run from an elevated session
-collectPerf                 Collect disk performance counters
-collectStorageBreakdown     Collect system volume used space breakdown
-checkFSConsistency          Checks for the consistency of the NTFS file system
-diagnostic                  outputs a storage diagnostic report
-bootdiag                    output boot sectors of the disk
-driverdiag                  output avaliable storport and storahci logs
-out <PATH>                  Specify the output path. If not specified, logs are saved to %TEMP%\StorDiag
```

Child Processes:

conhost.exe

Open Handles:

Path
(R–) C:\Users\user\AppData\Local\Temp\StorDiag\PSLogs.txt
(R-D) C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.Management.Infrastructure\v4.0_1.0.0.0__31bf3856ad364e35\Microsoft.Management.Infrastructure.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Diagnostics\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Diagnostics.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Management\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Managemer

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Utility\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Utility.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.ConsoleHost\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.ConsoleHost.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Security\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Security.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.WSMan.Management\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.WSMan.Management.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Configuration.Install\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Configuration.Install.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Management.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.ServiceProcess\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.ServiceProcess.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.XML.dll

(R-D) C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll

(RW-) C:\Users\user

...\Cor_SxSPublic_IPCBlock

\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000002.db

\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000002.db

\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2

\BaseNamedObjects\Cor_Private_IPCBlock_v4_5348

\BaseNamedObjects\NLS_CodePage_1252_3_2_0_0

\BaseNamedObjects\NLS_CodePage_437_3_2_0_0

\Sessions\1\BaseNamedObjects\windows_shell_global_counters

Loaded Modules:

Path
C:\Windows\System32\KERNEL32.dll
C:\Windows\System32\KERNELBASE.dll
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\SysWOW64\stordiag.exe

Signature

- >> Status: Signature verified.
- >> Serial: `3300000266BD1580EFA75CD6D3000000000266`
- >> Thumbprint: `A4341B9FD50FB9964283220A36A1EF6F6FAA7840`
- >> Issuer: CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
- >> Subject: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

File Metadata

- >> Original Filename: stordiag.exe
- >> Product Name: Microsoft (R) Windows (R) Operating System

- Company Name: Microsoft Corporation
- File Version: 10.0.19041.1
- Product Version: 10.0.19041.1
- Language: Language Neutral
- Legal Copyright: Copyright (c) Microsoft Corporation. All rights reserved.
- Machine Type: 32-bit

File Scan

- VirusTotal Detections: 0/75
- VirusTotal Link: https://www.virustotal.com/gui/file/b812162f140a347ec78756416302cbc9204ef484feb7623c0fff8ff7b4b3ec04/detection

File Similarity (ssdeep match)

File	Score
C:\Windows\system32\stordiag.exe	91

Possible Misuse

*The following table contains possible examples of `stordiag.exe` being misused. While `stordiag.exe` is **not** inherently malicious, its legitimate functionality can be abused for malicious purposes.*

Source	Source File	Example	License
sigma	proc_creation_win_stordiag_execution.yml	`title: Execution via stordiag.exe`	DRL 1.0
sigma	proc_creation_win_stordiag_execution.yml	`description: Detects the use of stordiag.exe to execute schtasks.exe systeminfo.exe and fltmc.exe`	DRL 1.0
sigma	proc_creation_win_stordiag_execution.yml	`- https://strontic.github.io/xcyclopedia/library/stordiag.exe-1F08FC87C373673944F6A7E8B18CD845.html`	DRL 1.0
sigma	proc_creation_win_stordiag_execution.yml	`ParentImage|endswith: '\stordiag.exe'`	DRL 1.0
sigma	proc_creation_win_stordiag_execution.yml	`ParentImage|startswith: # as first is "Copy c:\windows\system32\stordiag.exe to a folder"`	DRL 1.0
sigma	proc_creation_win_stordiag_execution.yml	`- Legitimate usage of stordiag.exe.`	DRL 1.0
LOLBAS	Stordiag.yml	`Name: Stordiag.exe`	
LOLBAS	Stordiag.yml	`- Command: stordiag.exe`	
LOLBAS	Stordiag.yml	`Description: Once executed, Stordiag.exe will execute schtasks.exe systeminfo.exe and fltmc.exe - if stordiag.exe is copied to a folder and an arbitrary executable is renamed to one of these names, stordiag.exe will execute it.`	
LOLBAS	Stordiag.yml	`- Path: c:\windows\system32\stordiag.exe`	
LOLBAS	Stordiag.yml	`- Path: c:\windows\syswow64\stordiag.exe`	

FOLLOW: STRONTIC.COM TWITTER GITHUB INSTAGRAM LINKEDIN FACEBOOK EMAIL FEED