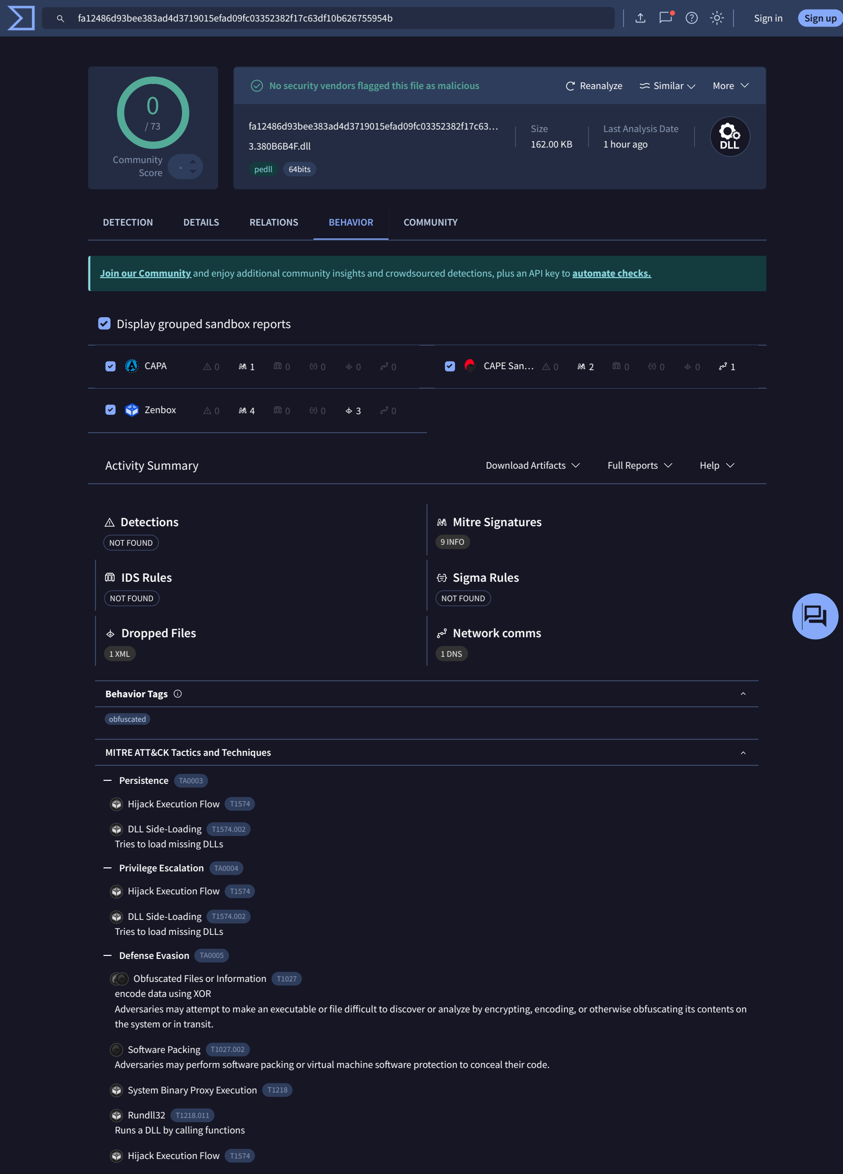

fa12486d93bee383ad4d3719015efad09fc03352382f17c63df10b626755954b

0
/ 73

Community Score

No security vendors flagged this file as malicious

fa12486d93bee383ad4d3719015efad09fc03352382f17c63…
3.380B6B4F.dll

pedll 64bits

Size
162.00 KB

Last Analysis Date
1 hour ago

DLL

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

☑ Display grouped sandbox reports

☑ CAPA ⚠ 0 · 1 · 0 · 0 · 0 · 0
☑ CAPE San… ⚠ 0 · 2 · 0 · 0 · 0 · 1
☑ Zenbox ⚠ 0 · 4 · 0 · 0 · 3 · 0

Activity Summary

Detections
NOT FOUND

Mitre Signatures
9 INFO

IDS Rules
NOT FOUND

Sigma Rules
NOT FOUND

Dropped Files
1 XML

Network comms
1 DNS

Behavior Tags

obfuscated

MITRE ATT&CK Tactics and Techniques

— **Persistence** TA0003
- Hijack Execution Flow T1574
- DLL Side-Loading T1574.002
  Tries to load missing DLLs

— **Privilege Escalation** TA0004
- Hijack Execution Flow T1574
- DLL Side-Loading T1574.002
  Tries to load missing DLLs

— **Defense Evasion** TA0005
- Obfuscated Files or Information T1027
  encode data using XOR
  Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.
- Software Packing T1027.002
  Adversaries may perform software packing or virtual machine software protection to conceal their code.
- System Binary Proxy Execution T1218
- Rundll32 T1218.011
  Runs a DLL by calling functions
- Hijack Execution Flow T1574

DLL Side-Loading `T1574.002`
Tries to load missing DLLs

— **Discovery** `TA0007`

System Information Discovery `T1082`
Reads software policies
Queries the volume information (name, serial number etc) of a device

Software Discovery `T1518`

Security Software Discovery `T1518.001`
AV process strings found (often used to terminate AV products)
May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)

— **Command and Control** `TA0011`

Application Layer Protocol `T1071`
Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic.

Malware Behavior Catalog Tree

— **Anti-Behavioral Analysis** `OB0001`

Software Packing `F0001`

— **Anti-Static Analysis** `OB0002`

Obfuscated Files or Information `E1027`
Encoding - Standard Algorithm `E1027.m02`

Software Packing `F0001`

— **Command and Control** `OB0004`

— **Defense Evasion** `OB0006`

Obfuscated Files or Information `E1027`
Encoding - Standard Algorithm `E1027.m02`

Software Packing `F0001`

— **Impact** `OB0008`

Denial of Service `B0033`

— **Data** `OC0004`

Encode Data `C0026`
XOR `C0026.002`

— **Communication** `OC0006`

HTTP Communication `C0002`

Capabilities

— **Load-Code**
Resolve function by parsing PE exports

— **Data-Manipulation**
Encode data using XOR

Network Communication ⓘ

DNS Resolutions

telemetry-incoming.r53-2.services.mozilla.com

Memory Pattern Domains

upx.sf.net

Memory Pattern Urls

http://upx.sf.net

Behavior Similarity Hashes ⓘ

CAPA	068a629543aa4569d7e5390c36023837
CAPE Sandbox	31133e83c5b119b82307f19d0359559e
Zenbox	ce9b83997e54f4f10ebf704d81c4ad94

File system actions ⓘ

Files Opened

- C:\Users\<USER>\Desktop\3.380B6B4F.dll
- C:\Users\<USER>\Desktop\3.380B6B4F.dll.123.Manifest
- C:\Users\<USER>\Desktop\3.380B6B4F.dll.124.Manifest
- C:\Users\<USER>\Desktop\3.380B6B4F.dll.2.Manifest
- C:\Users\<USER>\Desktop\3.380B6B4F.dll.manifest
- C:\Program Files (x86)\Common Files\Oracle\Java\java8path
- C:\Program Files (x86)\Common Files\Oracle\Java\java8path\
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
- C:\Program Files\dotnet
- C:\Program Files\dotnet\
- C:\ProgramData\Microsoft\
- C:\ProgramData\Microsoft\Windows\
- C:\ProgramData\Microsoft\Windows\WER
- C:\ProgramData\Microsoft\Windows\WER\
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC03F.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC03F.tmp.dmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC04E.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC04E.tmp.dmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0DC.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0DC.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0EC.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0EC.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC199.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC199.tmp.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1A6.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1D6.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC2C1.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC33F.tmp.txt
- C:\ProgramData\chocolatey\bin
- C:\ProgramData\chocolatey\bin\
- C:\Users\user\AppData\Local\DBG\config.xml
- C:\Users\user\AppData\Local\Dbg\EngineExtensions
- C:\Users\user\AppData\Local\Dbg\Visualizers\
- C:\Users\user\AppData\Local\Microsoft\WindowsApps
- C:\Users\user\AppData\Local\Microsoft\WindowsApps\
- C:\Users\user\AppData\Local\Programs\Python\Python39
- C:\Users\user\AppData\Local\Programs\Python\Python39\
- C:\Users\user\AppData\Local\Programs\Python\Python39\Scripts
- C:\Users\user\AppData\Local\Programs\Python\Python39\Scripts\
- C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\AppContainerUserCertRead
- C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\
- C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\
- C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\
- C:\Users\user\Desktop\3.380B6B4F.dll
- C:\Users\user\Desktop\3.380B6B4F.dll.123.Manifest
- C:\Users\user\Desktop\3.380B6B4F.dll.124.Manifest
- C:\Users\user\Desktop\3.380B6B4F.dll.2.Manifest
- C:\Windows\AppPatch\sysmain.sdb
- C:\Windows\Globalization\Sorting\sortdefault.nls
- C:\Windows\SYSTEM32
- C:\Windows\SYSTEM32\
- C:\Windows\SYSTEM32\Visualizers\
- C:\Windows\SYSTEM32\WINXP
- C:\Windows\SYSTEM32\XmlLite.dll
- C:\Windows\SYSTEM32\aepic.dll
- C:\Windows\SYSTEM32\apphelp.dll
- C:\Windows\SYSTEM32\dbgeng.dll
- C:\Windows\SYSTEM32\dbgmodel.dll
- C:\Windows\SYSTEM32\en-US\apphelp.dll.mui
- C:\Windows\SYSTEM32\en-US\ntdll.dll.mui

```
C:\Windows\SYSTEM32\en-US\tzres.dll.mui
C:\Windows\SYSTEM32\msvcp110_win.dll
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\SYSTEM32\ntmarta.dll
C:\Windows\SYSTEM32\ole32.dll
C:\Windows\SYSTEM32\policymanager.dll
C:\Windows\SYSTEM32\pri
C:\Windows\SYSTEM32\sfc.dll
C:\Windows\SYSTEM32\sfc_os.DLL
C:\Windows\SYSTEM32\tzres.dll
C:\Windows\SYSTEM32\winext
C:\Windows\SYSTEM32\winext\arcade
C:\Windows\SYSTEM32\winxp\triage.ini
C:\Windows\System32\
C:\Windows\System32\FlightSettings.dll
C:\Windows\System32\KERNEL32.DLL
C:\Windows\System32\KERNELBASE.dll
C:\Windows\System32\OpenSSH
C:\Windows\System32\OpenSSH\
C:\Windows\System32\RMCLIENT.dll
C:\Windows\System32\RPCRT4.dll
C:\Windows\System32\WINHTTP.dll
C:\Windows\System32\Wbem
C:\Windows\System32\Wbem\
C:\Windows\System32\WindowsPowerShell\v1.0
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\bcd.dll
C:\Windows\System32\bcryptPrimitives.dll
C:\Windows\System32\combase.dll
C:\Windows\System32\en-US\KERNEL32.DLL.mui
C:\Windows\System32\en-US\KERNELBASE.dll.mui
C:\Windows\System32\en-US\RPCRT4.dll.mui
C:\Windows\System32\en-US\combase.dll.mui
C:\Windows\System32\en-US\shcore.dll.mui
C:\Windows\System32\en-US\user32.dll.mui
C:\Windows\System32\imagehlp.dll
C:\Windows\System32\msvcrt.dll
C:\Windows\System32\shcore.dll
C:\Windows\System32\twinapi.appcore.dll
C:\Windows\System32\ucrtbase.dll
C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms
C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17134.1304_none_d3fbe61b7c93d9f0
C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17134.1304_none_d3fbe61b7c93d9f0\Comctl32.dll
C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17134.1304_none_d3fbe61b7c93d9f0\comctl32.DLL
C:\Windows\system32
C:\Windows\system32\
C:\Windows\system32\CRYPTBASE.dll
C:\Windows\system32\CRYPTSP.dll
C:\Windows\system32\DSREG.DLL
C:\Windows\system32\IMM32.DLL
C:\Windows\system32\NETAPI32.dll
C:\Windows\system32\SSPICLI.DLL
C:\Windows\system32\Secur32.dll
C:\Windows\system32\XmlLite.dll
C:\Windows\system32\bcrypt.dll
C:\Windows\system32\conhost.exe
C:\Windows\system32\dbgcore.DLL
C:\Windows\system32\dbghelp.dll
C:\Windows\system32\drivers\
C:\Windows\system32\dwmapi.dll
C:\Windows\system32\en-US\WerFault.exe.mui
C:\Windows\system32\en-US\conhost.exe.mui
C:\Windows\system32\en-US\faultrep.dll.mui
C:\Windows\system32\en-US\rundll32.exe.mui
C:\Windows\system32\en-US\wer.dll.mui
```

- C:\Windows\system32\faultrep.dll
- C:\Windows\system32\loaddll64.exe
- C:\Windows\system32\msvcp110_win.dll
- C:\Windows\system32\rpcss.dll
- C:\Windows\system32\rsaenh.dll
- C:\Windows\system32\rundll32.exe
- C:\Windows\system32\uxtheme.dll
- C:\Windows\system32\uxtheme.dll.Config
- C:\Windows\system32\verifier.dll
- C:\Windows\system32\version.dll
- C:\Windows\system32\wer.dll
- C:\Windows\system32\wer.dll.3.Manifest
- MountPointManager
- PhysicalDrive0
- c:\windows\system32\
- c:\windows\system32\loaddll64.exe

Files Written

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC03F.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
parent command line	C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC03F.tmp.dmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
parent command line	C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC04E.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC04E.tmp.dmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0DC.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0DC.tmp.WERInternalMetadata.xml

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0EC.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
parent command line	C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0EC.tmp.WERInternalMetadata.xml

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
parent command line	C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC199.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC199.tmp.xml

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

Files Deleted

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC03F.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
parent command line	C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1

— C:\ProgramData\Microsoft\Windows\WER\Temp\WERC03F.tmp.dmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
parent command line	C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1

- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC04E.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC04E.tmp.dmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0DC.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0EC.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
parent command line	C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1

- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC199.tmp

command line	C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
parent command line	C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"

Files Dropped

- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0DC.tmp.WERInternalMetadata.xml

sha256	6368c7180943ce872c790026b33648cd84e749ab0023c93922c018969aae9ed8
type	XML
process name	C:\Windows\System32\WerFault.exe

- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0EC.tmp.WERInternalMetadata.xml

sha256	a44031ec5913df1569302bbb0940b70bb570db76df40e3fabf655971b7e42c4d
type	XML
process name	C:\Windows\System32\WerFault.exe

- C:\ProgramData\Microsoft\Windows\WER\Temp\WERC199.tmp.xml

sha256	90407544069df81a22e1b100e081c0d33580745a82e6087f5fb71436b0ae1c20
type	XML
process name	C:\Windows\System32\WerFault.exe

Registry actions

Registry Keys Opened

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppModel\Lookaside\Packages
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsSelfHost\FIDs\ByFID
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsSelfHost\FIDs\Unknown
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap

Registry Keys Set

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug\ExceptionRecord

  ```
  05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 98 12 C3 63 00 00 00 00 02 00 00 00 00 00 00 00 00 0
  ```

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\Debug
- \REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\PermissionsCheckTestKey
- \REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\loaddll64.exe|f3d72086358f9008
- \REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\loaddll64.exe|f3d72086358f9008\BinFileVersion
- \REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\loaddll64.exe|f3d72086358f9008\BinProductVersion
- \REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\loaddll64.exe|f3d72086358f9008\BinaryType

pe64_amd64

— \REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\loaddll64.exe|f3d72086358f9008\FileId

0000f232e0decd548852fa6089e195431b73e94ed0bd

— \REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\loaddll64.exe|f3d72086358f9008\IsOsComponent

0

— \REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\loaddll64.exe|f3d72086358f9008\IsPeFile

1

Registry Keys Deleted

\REGISTRY\A\{4ef1dd23-2ee8-a970-e25d-6939ef1da50a}\Root\InventoryApplicationFile\PermissionsCheckTestKey

Process and service actions ⓘ

Processes Created

"C:\Windows\sysnative\rundll32.exe" "C:\Users\<USER>\Desktop\3.380B6B4F.dll",#1
C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152
C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
C:\Windows\System32\cmd.exe cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1
C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"
C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1

Processes Terminated

C:\Windows\System32\WerFault.exe
C:\Windows\System32\cmd.exe

Processes Tree

6612 - "C:\Windows\sysnative\rundll32.exe" "C:\Users\<USER>\Desktop\3.380B6B4F.dll",#1
7540 - C:\Windows\System32\loaddll64.exe loaddll64.exe "C:\Users\user\Desktop\3.380B6B4F.dll"
↳ 7548 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
↳ 7588 - C:\Windows\System32\cmd.exe cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1
  ↳ 7608 - C:\Windows\System32\rundll32.exe rundll32.exe "C:\Users\user\Desktop\3.380B6B4F.dll",#1
    ↳ 7716 - C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7608 -s 252
↳ 7708 - C:\Windows\System32\WerFault.exe C:\Windows\system32\WerFault.exe -u -p 7540 -s 152

Synchronization mechanisms & Signals ⓘ

Mutexes Created

\Sessions\1\BaseNamedObjects\Global\AmiProviderMutex_InventoryApplicationFile
\Sessions\1\BaseNamedObjects\Global\e5b9915f-9061-487a-837d-cd660323e9e3
\Sessions\1\BaseNamedObjects\Global\f1dd6682-f7fb-43a8-ad6b-8080b0b8ba4f
\Sessions\1\BaseNamedObjects\Local\WERReportingForProcess7540
\Sessions\1\BaseNamedObjects\Local\WERReportingForProcess7608