602f4ae507fa8de57ada079adff25a6c2a899bd25cd092d0af7e62cdb619c93c

Sign in Sign up

53
/ 70
Community Score

53/70 security vendors flagged this file as malicious

Reanalyze Similar More

602f4ae507fa8de57ada079adff25a6c2a899bd25cd092d0...
popup.sed

Size
226.59 KB

Last Analysis Date
9 months ago

EXE

peexe overlay checks-user-input detect-debug-environment long-sleeps checks-cpu-name

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

☑ Display grouped sandbox reports

☑ C2AE	0	0	0	0	1	0	☑ CAPA	0	5	0	0	0	0
☑ Microsoft ...	0	0	0	0	18	2	☑ VirusTotal...	0	0	6	0	1	0
☑ VirusTotal...	0	0	0	0	1	0	☑ VirusTotal...	0	0	0	0	0	0
☑ Zenbox	0	5	0	0	5	2							

Activity Summary

Download Artifacts Full Reports Help

Detections
NOT FOUND

Mitre Signatures
22 INFO

IDS Rules
2 MEDIUM 4 LOW

Sigma Rules
NOT FOUND

Dropped Files
21 OTHER 1 TEXT 1 PE_EXE

Network comms
2 DNS 2 IP

Behavior Tags ⓘ

checks-cpu-name checks-user-input detect-debug-environment long-sleeps

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002
+ Defense Evasion TA0005
+ Credential Access TA0006
+ Discovery TA0007
+ Collection TA0009

Malware Behavior Catalog Tree

+ Anti-Static Analysis

+ Defense Evasion OB0006

+ Discovery OB0007

+ Execution OB0009

+ File System OC0001

+ Process OC0003

+ Data OC0004

+ Cryptography OC0005

+ Communication OC0006

+ Operating System OC0008

Capabilities

Open in CAPA explorer

+ Host-Interaction

+ Data-Manipulation

+ Executable

+ Linking

+ Communication

+ Collection

+ Anti-Analysis

Crowdsourced IDS rules

⚠ Matches rule PROTOCOL-ICMP Unusual PING detected at Snort registered user ruleset
↳ *successful-recon-limited*

⚠ Matches rule PROTOCOL-ICMP traceroute at Snort registered user ruleset
↳ *attempted-recon*

⚠ Matches rule (eth) truncated ethernet header at Snort registered user ruleset
↳ *misc-activity*

⚠ Matches rule PROTOCOL-ICMP PING at Snort registered user ruleset
↳ *misc-activity*

⚠ Matches rule PROTOCOL-ICMP Echo Reply at Snort registered user ruleset
↳ *misc-activity*

⚠ Matches rule PROTOCOL-ICMP Destination Unreachable Network Unreachable at Snort registered user ruleset
↳ *misc-activity*

See all

Network Communication

DNS Resolutions

fp2e7a.wpc.2be4.phicdn.net

+ fp2e7a.wpc.phicdn.net

IP Traffic

TCP 20.99.133.109:443
TCP 192.229.211.108:80 (fp2e7a.wpc.phicdn.net)

Behavior Similarity Hashes

C2AE	ce7a0baf559dccaeb611c88da111a91d
CAPA	bc9eafc9b52390b76fc898df4f2f456c
Microsoft Sysinternals	[illegible]
VirusTotal Cuckoofork	494200a4ae747f8f322cf0b11bf3d1a2
VirusTotal Jujubox	d487b6fc52f07aa0d50a0fb9a6054361

Sign in Sign up

File system actions

Files Opened

- C:\602f4ae507fa8de57ada079adff25a6c2a899bd25cd092d0af7e62cdb619c93c
- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\popup.sed
- C:\Documents and Settings\<USER>\Local Settings\Temp\3.tmp
- C:\Documents and Settings\<USER>\Local Settings\Temp\3.tmp\1.bat
- C:\Documents and Settings\<USER>\Local Settings\Temp\4.tmp
- C:\WINDOWS\system32\iexpress.exe
- C:\WINDOWS\system32\makecab.exe
- CONIN$
- nul
- ~%TargetName%.DDF

Files Written

- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\popup.sed
- C:\Documents and Settings\<USER>\Local Settings\Temp\3.tmp\1.bat
- nul
- ~%TargetName%.DDF
- C:\Users\<USER>\AppData\Local\Temp\3380.tmp\1.bat
- C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser
- C:\Users\user\AppData\Local\Temp\C3BD.tmp
- C:\Users\user\AppData\Local\Temp\C3BD.tmp\1.bat
- C:\Users\user\AppData\Local\Temp\C3CE.tmp
- C:\Users\user\AppData\Local\Temp\popup.sed

Files Deleted

- C:\ProgramData\Microsoft\Windows\WER\Temp\WER268E.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER2759.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER2798.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER3499.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A9.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER34AA.tmp.txt
- C:\Windows\System32\spp\store\2.0\cache\cache.dat
- C:\Documents and Settings\<USER>\Local Settings\Temp\3.tmp
- C:\Users\<USER>\AppData\Local\Temp\3380.tmp
- C:\Users\user\AppData\Local\Temp\C3BD.tmp

Files Copied

+ C:\602f4ae507fa8de57ada079adff25a6c2a899bd25cd092d0af7e62cdb619c93c

Files Dropped

+ %TEMP%\popup.sed

%USERPROFILE%\AppData\Local\Temp\E975.tmp

%USERPROFILE%\AppData\Local\Temp\E975.tmp\1.bat

%USERPROFILE%\AppData\Local\Temp\E976.tmp

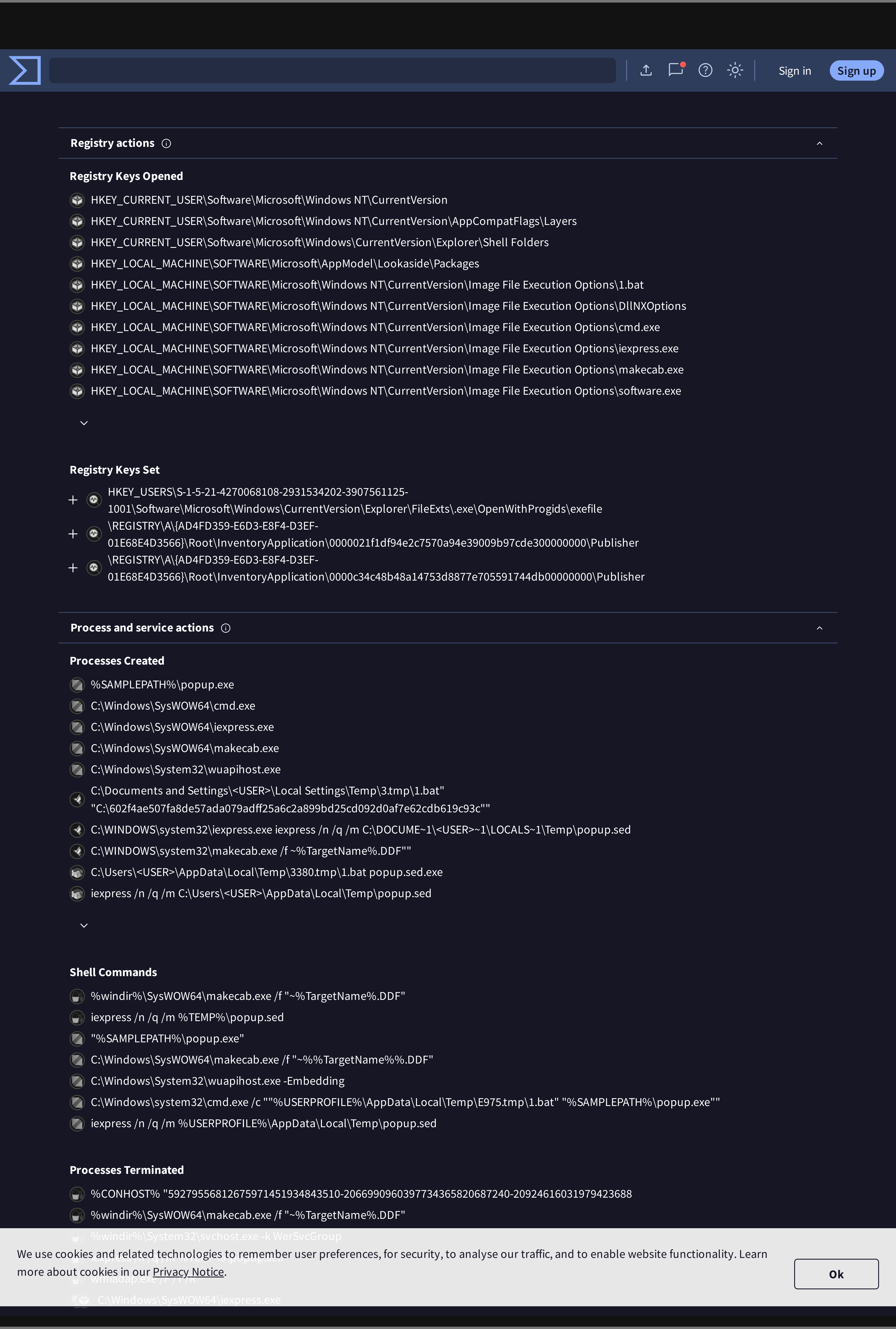
%USERPROFILE%\AppData\Local\Temp\popup.sed

C:\ProgramData\Microsoft\Windows\WER\Temp\WER268E.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WER268E.tmp.WERInternalMetadata.xml

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2759.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2759.tmp.csv



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\Windows NT\CurrentVersion\Image File Execution Options\1.bat
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\iexpress.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\makecab.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\software.exe

Registry Keys Set

- + HKEY_USERS\S-1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\OpenWithProgids\exefile
- + \REGISTRY\A\{AD4FD359-E6D3-E8F4-D3EF-01E68E4D3566}\Root\InventoryApplication\0000021f1df94e2c7570a94e39009b97cde300000000\Publisher
- + \REGISTRY\A\{AD4FD359-E6D3-E8F4-D3EF-01E68E4D3566}\Root\InventoryApplication\0000c34c48b48a14753d8877e705591744db00000000\Publisher

Process and service actions ⓘ

Processes Created

- %SAMPLEPATH%\popup.exe
- C:\Windows\SysWOW64\cmd.exe
- C:\Windows\SysWOW64\iexpress.exe
- C:\Windows\SysWOW64\makecab.exe
- C:\Windows\System32\wuapihost.exe
- C:\Documents and Settings\<USER>\Local Settings\Temp\3.tmp\1.bat" "C:\602f4ae507fa8de57ada079adff25a6c2a899bd25cd092d0af7e62cdb619c93c""
- C:\WINDOWS\system32\iexpress.exe iexpress /n /q /m C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\popup.sed
- C:\WINDOWS\system32\makecab.exe /f ~%TargetName%.DDF""
- C:\Users\<USER>\AppData\Local\Temp\3380.tmp\1.bat popup.sed.exe
- iexpress /n /q /m C:\Users\<USER>\AppData\Local\Temp\popup.sed

Shell Commands

- %windir%\SysWOW64\makecab.exe /f "~%TargetName%.DDF"
- iexpress /n /q /m %TEMP%\popup.sed
- "%SAMPLEPATH%\popup.exe"
- C:\Windows\SysWOW64\makecab.exe /f "~%%TargetName%%.DDF"
- C:\Windows\System32\wuapihost.exe -Embedding
- C:\Windows\system32\cmd.exe /c ""%USERPROFILE%\AppData\Local\Temp\E975.tmp\1.bat" "%SAMPLEPATH%\popup.exe""
- iexpress /n /q /m %USERPROFILE%\AppData\Local\Temp\popup.sed

Processes Terminated

- %CONHOST% "59279556812675971451934843510-2066990960397734365820687240-20924616031979423688"
- %windir%\SysWOW64\makecab.exe /f "~%TargetName%.DDF"
- %windir%\System32\svchost.exe -k WerSvcGroup
- iexpress /n /q /m %TEMP%\popup.sed
- wmiadap.exe /F /T /R
- C:\Windows\SysWOW64\iexpress.exe

C:\Windows\System32\wuapihost.exe

C:\Users\<USER>\AppData\Local\Temp\3380.tmp\1.bat popup.sed.exe

Processes Tree

```
2204 - %windir%\System32\svchost.exe -k WerSvcGroup
2692 - %CONHOST% "59279556812675971451934843510-2066990960397734365820687240-20924616031979423688
2648 - %CONHOST% "333468326242449828-910471021550555212-20617934831352295882112652944290124525
2852 - wmiadap.exe /F /T /R
2580 - %SAMPLEPATH%
   ↳ 2664 - %ComSpec% /c ""%TEMP%\56A7.tmp\1.bat" %SAMPLEPATH%"
     ↳ 2672 - iexpress /n /q /m %TEMP%\popup.sed
       ↳ 2684 - %windir%\SysWOW64\makecab.exe /f "~%TargetName%.DDF"
2892 - %windir%\system32\wbem\wmiprvse.exe
3664 - %WINDIR%\explorer.exe
```

Synchronization mechanisms & Signals

Mutexes Created

ShimCacheMutex

Modules loaded

Runtime Modules

%SAMPLEPATH%\popup.exe

advapi32.dll

comctl32.dll

kernel32.dll

msimg32.dll

uxtheme.dll

version.dll

ADVAPI32.dll

C:\Users\<USER>\AppData\Local\Temp\3380.tmp\1.bat

Highlighted actions

Calls Highlighted

GetTickCount

Highlighted Text

"popup.sed.exe"