35c22725a92d5cb1016b09421c0a6cdbfd860fd4778b3313669b057d4a131cb7

Sign in Sign up

1 / 60
Community Score

1/60 security vendor flagged this file as malicious

Reanalyze Similar More

35c22725a92d5cb1016b09421c0a6cdbfd860fd4778b3313669…
BatLocked (not safe).bat
shell

Size 219 B

Last Analysis Date 7 months ago

DETECTION DETAILS BEHAVIOR COMMUNITY 1

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

Display grouped sandbox reports

VirusTotal… 0 0 0 0 0 0

Zenbox 0 3 0 1 0 0

Activity Summary

Download Artifacts Full Reports Help

Detections
NOT FOUND

Mitre Signatures
6 INFO

IDS Rules
NOT FOUND

Sigma Rules
1 LOW

Dropped Files
NOT FOUND

Network comms
NOT FOUND

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002
+ Defense Evasion TA0005
+ Discovery TA0007

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 0 LOW 1

Matches rule Files And Subdirectories Listing Using Dir by frack113 at Sigma Integrated Rule Set (GitHub)
↳ *Detects usage of the "dir" command that's part of windows batch/cmd to collect information about directories*

Behavior Similarity Hashes

VirusTotal Jujubox	8b98ffaf790599cb98a1ac747fe1df99
Zenbox	ad2184c04253581f0be78cec9612c5c6

File system actions

Files Opened

C:\Users
C:\Users\
C:\Users\<USER>\

C:\Users\<USER>\Downloads\35c22725a92d5cb1016b09421c0a6cdbfd860fd4778b3313669b057d4a131cb7.vbs
C:\Users\<USER>\Downloads\35c22725a92d5cb1016b09421c0a6cdbfd860fd4778b3313669b057d4a131cb7.vbs\
C:\Users\azure
C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.18837_none_a4d981ff711297b6
C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.18837_none_a4d981ff711297b6\COMCTL32.dll

Files Written

C:\Users\user\Desktop\BPMLNOBVSB.jpg10750.batlocked
C:\Users\user\Desktop\BatLocked (not safe).bat10750.batlocked
C:\Users\user\Desktop\FENIVHOIKN.png10750.batlocked
C:\Users\user\Desktop\JSDNGYCOWY.png10750.batlocked
C:\Users\user\Desktop\KZWFNRXYKI.jpg10750.batlocked
C:\Users\user\Desktop\KZWFNRXYKI.xlsx10750.batlocked
C:\Users\user\Desktop\NWTVCDUMOB.docx10750.batlocked
C:\Users\user\Desktop\WKXEWIOTXI.mp310750.batlocked
\Device\ConDrv\\Connect

Registry actions

Registry Keys Opened

HKEY_CLASSES_ROOT\.vbs
HKEY_CLASSES_ROOT\.vbs\0x0
HKEY_CLASSES_ROOT\VBSFile\ScriptEngine
HKEY_CLASSES_ROOT\VBSFile\ScriptEngine\0x0
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\TrustPolicy
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\IgnoreUserSettings

Registry Keys Set

+ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.60.3.1!7\Name
+ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.60.3.2!7\Name
+ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.60.3.3!7\Name
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.60.3.1!7
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.60.3.2!7
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.60.3.3!7

Process and service actions

Processes Tree

7812 - C:\Windows\System32\cmd.exe C:\Windows\system32\cmd.exe /c ""C:\Users\user\Desktop\BatLocked (not safe).bat" "
↳ 4072 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
↳ 7880 - C:\Windows\System32\cmd.exe C:\Windows\system32\cmd.exe /c dir /b /s
↳ 7928 - C:\Windows\System32\certutil.exe certutil -encode "C:\Users\user\Desktop\BatLocked (not safe).bat" "C:\Users\user\Desktop\BatLocked (not safe).bat10750.batlocked"
↳ 7984 - C:\Windows\System32\certutil.exe certutil -encode "C:\Users\user\Desktop\BPMLNOBVSB" "C:\Users\user\Desktop\BPMLNOBVSB10750.batlocked"
↳ 7948 - C:\Windows\System32\certutil.exe certutil -encode "C:\Users\user\Desktop\BPMLNOBVSB.jpg" "C:\Users\user\Desktop\BPMLNOBVSB.jpg10750.batlocked"

↳ 3192 - C:\Windows\System32\certutil.exe certutil -encode "C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx" "C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx10750.batlocked"

↳ 7640 - C:\Windows\System32\certutil.exe certutil -encode "C:\Users\user\Desktop\KZWFNRXYKI.jpg" "C:\Users\user\Desktop\KZWFNRXYKI.jpg10750.batlocked"

↳ 2732 - C:\Windows\System32\certutil.exe certutil -encode "C:\Users\user\Desktop\KZWFNRXYKI.xlsx" "C:\Users\user\Desktop\KZWFNRXYKI.xlsx10750.batlocked"

Modules loaded

Runtime Modules

- ADVAPI32.dll
- API-MS-Win-Security-LSALookup-L1-1-0.dll
- C:\Windows\system32\CRYPT32.dll
- C:\Windows\system32\advapi32.dll
- C:\Windows\system32\rsaenh.dll
- C:\Windows\system32\scrobj.dll
- C:\Windows\system32\vbscript.dll
- C:\Windows\system32\wshext.dll
- CLBCatQ.DLL
- CRYPTBASE.dll

Highlighted actions

Calls Highlighted

- GetSystemMetrics
- GetTickCount