

Forum:[Hack Forums](#)

Thread: [Celesty Binder](#)

BPName - April 13, 2025, 1:08 pm

It is a powerful file binding software for the Windows operating system. This software is especially used by hackers to hack computers and laptops silently by binding their viruses and trojan inside other premium software. It allows you to merge multiple files together and you can also change the icon of your bound file through this

[deleted] [warn]

Bastille - April 14, 2025, 12:25 am

Thanks for the anaysis [mention=1441945] ! I'll take a deeper look when I can

I just took a couple of minutes to check the VT report and this is what I've noticed :

Decoded text

{'Lumma': {'C2': []}}

Probably a stealer as it has interactions with Telegram : 149.154.167.99:443 (t.me)

BPName - April 14, 2025, 5:45 am

(Apr 14, 2025 12:25 AM)Bastille Wrote: [\[CITE\]](#) Thanks for the anaysis [mention=1441945] ! I'll take a deeper look when I can

I just took a couple of minutes to check the VT report and this is what I've noticed :

Decoded text

{'Lumma': {'C2': []}}

Probably a stealer as it has interactions with Telegram : 149.154.167.99:443 (t.me)

Sorry I got it from github witout it analyze

(Apr 13, 2025 02:30 PM)m0hx Wrote: [\[CITE\]](#) DO NOT DOWNLOAD

file is being analyzed, will report back if i find anything and edit my post. but seeing initially that the file size is over 800mb unpacked is very sus.

Celesty Binder comes with DarkComet and pretty outdated anyways. I have clean version to compare it with.

be careful.

for reference og post is:

edit1: doesnt look good at all!

quick vt analysis:

<https://www.virustotal.com/gui/file/a16f1a84341084bfa09bc5d428b143c583a65bd44aa0ea9bbebd1ca35b734e7d?nocache=1>

edit2: vt behavioral analysis

Files written

C:\Users\<USER>\AppData\Local\Temp\643999\Del.com
C:\Users\<USER>\AppData\Local\Temp\643999\N
C:\Users\<USER>\AppData\Local\Temp\Accessing
C:\Users\<USER>\AppData\Local\Temp\CAB05552.TMP
C:\Users\<USER>\AppData\Local\Temp\Cancer.accde
C:\Users\<USER>\AppData\Local\Temp\Cheque.accde
C:\Users\<USER>\AppData\Local\Temp\Constant.accde
C:\Users\<USER>\AppData\Local\Temp\Council
C:\Users\<USER>\AppData\Local\Temp\Delivery
C:\Users\<USER>\AppData\Local\Temp\Fig.accde

Processes created

"C:\Users\<USER>\Desktop\celesty_binder_strpd.exe"
"C:\Windows\System32\cmd.exe" /c copy Fig.accde Fig.accde.bat & Fig.accde.bat
C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc
C:\Windows\System32\svchost.exe -k NetworkService -p
C:\Windows\system32\lsass.exe
C:\Windows\system32\services.exe
C:\Windows\system32\svchost.exe -k LocalService -s W32Time
C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Del.com N
choice /d y /t 5

Shell commands

"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc
"C:\Windows\System32\cmd.exe" /c copy Fig.accde Fig.accde.bat & Fig.accde.bat
C:\Windows\System32\cmd.exe /c copy Fig.accde Fig.accde.bat & Fig.accde.bat
C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc
C:\Windows\System32\svchost.exe -k NetworkService -p
C:\Windows\System32\svchost.exe -k netsvcs -p
C:\Windows\system32\lsass.exe
C:\Windows\system32\spssvc.exe
C:\Windows\system32\svchost.exe -k LocalService -s W32Time
C:\Windows\system32\svchost.exe -k UnistackSvcGroup

Processes terminated

findstr /I opssvc wrsa
tasklist
1184 - C:\Windows\system32\DeviceDisplayObjectProvider.exe -Embedding
3292 - C:\Windows\System32\slui.exe -Embedding
3304 - "C:\Windows\System32\cmd.exe" /c copy Fig.accde Fig.accde.bat & Fig.accde.bat
3680 - rundll32 C:\Windows\system32\GeneralTel.dll,RunInUserCxt oXVxnIBVmk+7vxDv.1.1.2
{DE4017EA-FD03-45B0-A72A-80F744F8BB21} {121A51A0-A642-35F0-CC22-F81735E3E318}
IsAdmin WAMAccountCount
3688 - tasklist
3728 - findstr /I "opssvc wrsa"

3788 - ping -n 188 127.0.0.1

Processes tree

3156 - "C:\Users\<USER>\Desktop\celesty_binder_strpd.exe"
7056 - "C:\Windows\System32\cmd.exe" /c copy Fig.accde Fig.accde.bat & Fig.accde.bat
3608 - tasklist
6308 - findstr /I "opssvc wrsa"
2564 - tasklist
5428 - findstr "SophosHealth bdservicehost AvastUI AVGUI nsWscSvc ekrn"
5292 - cmd /c md 643999
5552 - extrac32 /Y /E Cancer.accde
6652 - findstr /V "EXIST" Delivery
4344 - cmd /c copy /b 643999\Del.com + Mitsubishi + Ugly + Council + University + Find + Guild + Simpsons + Officers + Accessing 643999\Del.com

edit3: quick findings:

Archive Name: celesty_binder.rar.7z

Archive Hashes:

CRC32: E042DE4E

MD5: CF30837D14931E801922D76E66049710

SHA-1: 5ED85CDD995DFB9C5190652E03384094283647C9

Filename: celesty_binder.rar.exe

File Hashes:

CRC32: F45E7C46

MD5: FC6279A47D37C314FD1D68E056D2CE3A

SHA-1: 8AB6C406C76A731530C1E7C99E9710ECC40DD3F8

architecture: 32-bit (x86)

time-date-stamp: 2010-04-10 15:19:23 (Sat Apr 10 12:19:23 2010 (UTC))

size-of-image: 00136000

sections: 0005

type: GUI

Filesize: 862.33MiB

entry-point: 004033e9 (0x000033E9 (section[.text]))

Operation system: Windows(2000)[I386, 32-bit, GUI]

Installer: Nullsoft Scriptable Install System(2.46-Unicode)[lzma]

packed section: Section(4)['.rsrc']

pumped with: 00

actual file size: ~30.3 MB

Operation system: Windows(2000)[I386, 32-bit, GUI]

Linker: Microsoft Linker(9.00.30729)

Compiler: Microsoft Visual C/C++(15.00.30729)[C]

Language: C

Tool: Microsoft Visual Studio(2008)
Installer: Nullsoft Scriptable Install System(2.46-Unicode)[lzma]
Overlay: Binary
Data: NSIS data
packet sections: Section(4)['.rsrc'] / Overlay

manifest: Nullsoft.NSIS.exehead
entropy: 6.723
overlay: NullsoftInst..o...T...l... .

SUS strings:
00344594 GetProcessHeap
00344622 IsDebuggerPresent
0034B01D onecoreuap\base\appmodel\userdataaccess\objectmodels\poom\lib\folder.cpp

0034B2AD onecoreuap\base\appmodel\userdataaccess\objectmodels\poom\lib\emailrecipientinfo.cp
p
0034B21C onecoreuap\base\appmodel\userdataaccess\objectmodels\poom\lib\mail.cpp
00351156 (Either UserName or Password was missing.
00351181 No active transaction.
003516EF KeyEncryptionPassword is specified when DontCopyRemoteKeys switch is present.
Remove the KeyEncryptionPassword parameter if you don't wish to copy the remote keys.
Otherwise remove the DontCopyRemoteKeys switch if you wish to copy the remote keys.
00356729 Failed to instantiate {%ls} from debugger's image path.
003567E9 The version of SOS does not match the version of CLR you are debugging. Please
00358F35 RegSetValueExW
00358F47 RegGetValueW
0035904D LoadLibraryExW
00006CE4 SeShutdownPrivilege
00006D70 Error writing temporary file. Make sure your temp folder is valid.
00006ED0 Control Panel\Desktop\ResourceLocale
00007018 Software\Microsoft\Windows\CurrentVersion
0004BAE2 MS Shell Dlg
00163F2A wincredprovider
0016535B Software\Microsoft\Windows\CurrentVersion\Run
00165423 SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
00177EE0 bcdedit /store C:\DATA\BCD /enum ACTIVE
001A8AC1 Keyword.API
001A8ADD Keyword.SEND
001A8AFD Keyword.RECEIVE
001A8B21 Keyword.L3_CONNECT
001A8B4D Keyword.CLOSE
001A8B6D Keyword.SECURITY
001A8B95 Keyword.CONFIGURATION
001A8BC5 Keyword.GLOBAL
001A8BE9 Keyword.DROPPED
001A8C0D Keyword.PII_PRESENT
001A8C39 Keyword.PACKET
001A8C5D Keyword.ADDRESS

001A8C81 Keyword.CONTEXT_EVENT
001A8CB1 Keyword.STATE_TRANSITION
001AF340 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp
0020AD20 BATMETER.DLL
0021AA92 IP NAT Helper Client
00221DC2 Another app has a higher priority level, preventing this call from succeeding

edit4: its definitely malware/infected. there's too much indications, drops /opens a lot of files.
including bat / dlls.

In strings also found it uses proxy libraries , networking which shouldnt be used in a binder!! check
DNS Resolutions on virustotal too.

I don't have time to fully reverse and unpack each single thing, but I hope no one gets infected by
this... be careful.

note: if anyone who wants to analyze it further let me know.

Thank you for reading. ?

more sus stuff:

005FF9FF Local address: %1%n
005FFA29 Remote address: %2%n
005FFA9F Peer private address: %5%n
005FFFE7 Local address: %1%n
00600011 Remote address: %2%n
00600087 Peer private address: %5%n
00606478 o::LoadLibrary. Name: %s. Version: %s6MethodCall:
ICLRRuntimeInfo::GetProcAddress. Name: %S
00606860 1LegacyFunctionCall: GetFileVersion. Filename: %s1LegacyFunctionCall:
GetRealProcAddress. Proc: %S-LegacyFunctionCall: CorExitProcess. Code:
%d/LegacyFunctionCall: CoUninitializeEE. Flag: %d%LegacyFunctionCall:
CoUninitializeCor2LegacyFunctionCall: CorDllMainWorker. Flags: 0x%x
0061155A IP Address
00611572 IPv6 Address
0061158E IPv6 Tunnel Address
00AFB7FB Domain:%t%t%3%n%tLogon ID:%t%t%4%n%nNetwork Information:%t%n%tSource
Address:%t%t%5%n%tSource Port:%t%t%6%n%t%nShare Name:%t%t%t%7
00CCC447 HWAddress
00CCC4A7 NewHWAddress
00CCC64D HWAddress
014B3C0F not a valid IP address: %s
014E52C5 WalletLegacy_BusinessAddressStreet
014E530D WalletLegacy_BusinessAddressCity
005FFA29 Remote address: %2%n
005FFA79 Remote port: %4%n
00600011 Remote address: %2%n

00600061 Remote port: %4%n
006B32A9 SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\RemoteAccess\
00ABEDC3 Microsoft Remote Desktop Services Web Access Control
00E65897 Command that control remote event logging
00ECED15 remoteaddr
0110057A REMOTESERVERNAME=
018726A5 RemoteAddress
01C7FC56 remotedesktop
01C7FC72 remoteadmin
002EBE3A Failed to start the VM Host Agent service: 0x%x
0052614B Deleting element %08x blocked by seStart Session. Type ID: %d. Session ID: %s.
Global: %d. Existing: %d.OCLRSQM: End Session. Type ID: %d. Session ID: %s. Global: %d.
Existing: %d.#SEM_FAILCRITICALERRORS is set to %dMLaunching browser to download missing
.NET Framework version. FWLINK page: %s
00565E5F Windows.StartupTask
0064E28E Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup
00B900D7 %PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup
00B9014F %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup
00BA38B8 Disconnect the device, and click "Reset." If you click "Close," the port will not work until
you unplug it and restart your PC.oA USB device has malfunctioned and exceeded the power limits
of its hub port. You should disconnect the device.
00FAF43F Software\Microsoft\Windows\CurrentVersion\StartupNotify
00519037 PrivateKeyPassword
0089DDAD ReistryKey.
008BBC02 Software\Microsoft\Windows NT\CurrentVersion\DefaultProductKey
01174BD6 PrivateKeyPassword
01174BFC %windir%\system32\inetsrv\config\configEncKey.bak
01174EC4 KeyCollection
013A432A keyboardrepeat
013A434A mousekeys
that was advertising ... ^^
you have to click several times to download something

I uploaded the file myself to mega

<https://mega.nz/file/3ch2HJyY#UV4UkooByiT0UJDxBJFG8Pje59GpoiKo9iafV0RRQ-0>