Report #13637

Creation Date: Sept. 11, 2021, 12:36 a.m.
Last Update: Sept. 11, 2021, 12:40 a.m.
File:
m0kdzueblmmlav.dll
Results:

Binary

DLL	**True**
Size	116.50KB
trid	**46.1%** Win64 Executable **21.8%** Windows screen saver **10.9%** Win32 Dynamic Link Library **7.5%** Win32 Executable **3.3%** OS/2 Executable
type	PE
wordsize	32
Subsystem	Windows CLI

Hashes

md5	ba15f2f9f59bcaeabbb41c890bef4e2f
sha1	ab06d93f3df6a483a87c384c4539570b203e74cb
crc32	0xbd7976a6
sha224	99d395e1a6f38dfb71150fc4536841f2ed393759aec1c1adebd0fb0a
sha256	7518f79fddbf51df7f43045a55c1dfd8bbafa8f87d21b573ee2c13bbc1e616c0
sha384	db9ae55ead385ff2b950ab3457945b80d0912308717743764bb3bde8cef838da5664d046d37014e14a7ba75659ac18c8
sha512	9479913429521387778a47e7023843b01c85cb83e36f4632f434e6431045e5e013c857f72e7d93d8458015242017863eafc57ea388ae24384d6e7d026bf3d4b4
ssdeep	3072:9J3rhEXVJrS+ip0VIzwmYpt/iG5jXschdtHq9mp:ZElJr/iimSRTccVHRp

Community

Google	**False**
HashLib	**False**

YARA

Matches	IsDLL, domain, contentis_base64, HasOverlay, IsPacked, IsConsole, IsPE32
Suspicious	**True**

Imports

pdh.dll	PdhGetDataSourceTimeRangeW, PdhGetFormattedCounterValue, PdhOpenLogA, PdhComputeCounterStatistics, PdhMakeCounterPathA, PdhVbAddCounter, PdhSetCounterScaleFactor, PdhLookupPerfIndexByNameA
mscms.dll	OpenColorProfileW, GetCMMInfo, DeleteColorTransform, CreateMultiProfileTransform, OpenColorProfileA, DisassociateColorProfileFromDeviceW
MSVCRT.dll	exit, system, _getch
MSVFW32.dll	DrawDibDraw, ICSeqCompressFrameStart, DrawDibEnd
AVIFIL32.dll	AVIStreamRead, AVISaveVW
KERNEL32.dll	GetStdHandle, VirtualProtect, SetConsoleCursorPosition

Strings

List

MSVFW32.dll
MSACM32.dll
AVIFIL32.dll
5r844e8n9.dll
MAPI32.dll
pdh.dll
mscms.dll
%EiQdl2
N fDa
<requestedPrivileges>
VirtualProtect
edc6dA
system
<requestedExecutionLevel level='asInvoker' uiAccess='false' />
T3|9ICkp
78gTa@.Y
:\S+do1gr
,:?-w.oE
7$k/YoUL
Ic?EzMel

Tfs.ak_}
3 : Exit
%pXD5Yf%
</assembly>
IP[a(ti
`.rdata
2 : Play with O
'at3P
2di?O
@tY9e=
OR"'P
ERL$>G
[RB&E
li@t+Zr
YrO\;
<5h:o
Xcodpesoemflc
Your Turn :>
"e/wt)
1 : Play with X
*dGai$
@.data
AB_H>m
.an\D
#_heV
d_WO*
#HUt]
L|UOP
GEED>
$^tme
d77oH
E0sag1
k CmMFOHtEAc
of&nl
wykGtc)
fiWd$
gdRn,r `{s
C VItWo
1HNf,c
@0gMTr
pRCWQNO
HpRbaFN
Player Wins
Game Draw
349+[
#dE"
ESTHA
MEDUL
`@he
1St*w
8g&S"h
|YrT3-
I3ObC
4EeYw
IH6E
OW0D
_getch
>=[%21
a0Kdl

hwin5
9PoE
oL4PHd
atg3
r);hd
,?)^]
#==<;
>eFt
~YHE
=ACH
"CTSD
NGCI
FNGA
eMrO
=tDo
HefrY
sguLK
mHo:
NMi,
MaL#
lYr.

Foremost

Matches	0.dll, 12 KB
Suspicious	**True**

Heuristics

IPs	**hasIPs**: **False** **Allowed** **Suspicious** **hasAllowed**: **False** **hasSuspicious**: **False**
URLs	**Allowed** **hasURLs**: **False** **Suspicious** **hasAllowed**: **False** **hasSuspicious**: **False**
Files	**Allowed**: MAPI32.dll, AVIFIL32.dll, 5r844e8n9.dll, USER32.dll, pdh.dll, MSVFW32.dll, MSACM32.dll, MSVCRT.dll, mscms.dll, KERNEL32.dll **hasFiles**: **True** **Suspicious** **hasAllowed**: **True** **hasSuspicious**: **False**

Binary

Sizes

RVA
RVA: 16
Suspicious: False
Code
Size: 9216
Suspicious: False
Image
Address: 268435456
Suspicious: False
Stack
Stack: 4096
Suspicious: False
Headers
Headers: 1024
Suspicious: False
Suspicious: False

Symbols

Number
Number: 0
Suspicious: True
Pointer
Pointer: 0
Suspicious: True
Directories
Number: 16
Suspicious: False

Checksum

Value: 0
Suspicous: True

Sections

Allowed: .text, .rdata, .data, .rsrc
Suspicious
hasAllowed: True
hasSections: True
hasSuspicious: False

Versions

OS
Version: 6
Suspicious: False
Image
Version: True
Suspicious: 6
Linker
Version: 14.16
Suspicious: False
Subsystem
Version: 6.0
Suspicious: False
Suspicious: False

EntryPoint

Address: 0
Suspicious: True

Anomalies	**Anomalies**: The export table TimeDateStamp and the file header TimeDateStamp do not march., The header checksum and the calculated checksum do not match. **hasAnomalies**: True
Libraries	**Allowed**: mapi32.dll, avifil32.dll, user32.dll, pdh.dll, msvfw32.dll, msacm32.dll, msvcrt.dll, mscms.dll, kernel32.dll **hasLibs**: True **Suspicious**: 5r844e8n9.dll **hasAllowed**: True **hasSuspicious**: True
Timestamp	**Past**: False **Valid**: True **Value**: 2021-03-23 01:06:21 **Future**: False
Compilation	**Packed**: False **Missing**: False **Packers** **Compiled**: True **Compilers**: Microsoft Visual C++ vx.x DLL
Obfuscation	**XOR**: False **Fuzzing**: False

PEDetector

Matches	None
Suspicious	False

Disassembly

hasTricks	False
Tricks	

AVclass

File

Trace	

10/9/2021 - 23:45:43.106	now n	1 9 6	C:\Windows\SysWO W64\rundll32.exe	C:\Windows
10/9/2021 - 23:45:43.106	Unk now n	2 1 9 6	C:\Windows\SysWO W64\rundll32.exe	C:\Monitor
10/9/2021 - 23:45:43.106	Unk now n	2 1 9 6	C:\Windows\SysWO W64\rundll32.exe	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b 64144ccf1df_5.82.7601.18837_none_ec86b8d6858ec0bc
10/9/2021 - 23:45:43.106	Unk now n	2 1 9 6	C:\Windows\SysWO W64\rundll32.exe	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b 64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
10/9/2021 - 23:45:43.200	Unk now n	2 4 7 6	C:\Windows\Syste m32\rundll32.exe	C:\Monitor

Process

Trace

10/9/2021 - 23:45:43.1 06	Terminat e	247 6	C:\Windows\System32\rundll32. exe	219 6	C:\Windows\SysWOW64\rundll32. exe

Analysis

Reason	Finished
Status	Sucessfully Executed
Results	1

Registry

Trace

File Summary

Created **Identified**: False

Deleted **Identified**: False

Process Summary

Created **Identified**: False

Deleted **Identified**: True

Registry Summary

Proxy **Identified**: False

AutoRun **Identified**: False

Created **Identified**: False

Deleted **Identified**: False

Browsers **Identified**: False

Internet **Identified**: False

DNS

Query

Response

TCP

Info

UDP

Info

HTTP

Info

Summary

DNS	**False**
TCP	**False**
UDP	**False**
HTTP	**False**

Results

BINARY

NFS 2.0 (Threshold = 0.8)
confidence: 56.88%
suspicious: **True**

NFS 3.0 (Threshold = 0.75)
confidence: 67.33%
suspicious: **True**

Decision Tree (NFS-BRMalware)
confidence: 100.00%
suspicious: **True**

MalConv (Ember: Raw Bytes, Threshold=0.5)
confidence: 99.67%
suspicious: **True**

Random Forest (100 estimators, NFS-BRMalware)
confidence: 59.00%
suspicious: **False**

Non-Negative MalConv (Ember: Raw Bytes, Threshold=0.35)
confidence: 73.55%
suspicious: **True**

LightGDM (Ember: File Characteristics, Threshold=0.8336)
confidence: 98.35%
suspicious: **True**