November 27, 2023

Presentation

Volatile Memory Forensic

Jeremy Julian - 2501998845

Johanes - 2501983736

Immanuel Billy C.S - 2540132723

Richard Tan - 2502008952

CHAPTER I

The importance of volatile memory analysis in detecting fileless malware and other advanced threats.

The Importance of Volatile Memory Analysis

Nowadays, more and more people use their laptop or PC as their main device for work, school, study, play games, etc. With the increase of activity that involves the internet, more and more cyber threat emerges, an example is malware. Our devices can be infected easily by simply clicking a button on the internet, the bad news is, that this malware evolves every year, they may start weak and can be detected, but they may evolve to a malware that can’t be detected by antivirus software, called fileless malware.

What happened in 2020?

Because the pandemic, many people lock themselves inside their house, which mean the increase of daily computer and internet user, not only regular people, but some business was also forced to operate online , which lead to...

50% increase in Cyber Attack @Online Business

900% increare in fileless Malware spotting

The Part of Volatile Memory

Volatile memory such as RAM (Random Access Memory) holds a very valuable forensic data, especially in stuff like fileless malware since important data like running process, file fragment/artifacts, and network connections are stored here.

Moreover, RAM allows the extraction of obscured information in an unencrypted, readily available format

CHAPTER II

The Challenge of collecting and analyzing Volatile Memory

First Step: Memory Aquisition

In order to uncover the malware on a system, we first need to acquire the volatile memory stored in the system, as an Investigator, we can do acquisition in many different access level according to our needs, we can do it in Kernel, Hypervisor, System management or Asynchronous Device level, with various Memory types such as, Kernel Drivers, Crash Dump Files, Hibernation Files, Debuggers, Hypervisor, BIOS-Level, Direct Memory Access, etc

Tools that investigator use to do memory Aquisition

Access Level	Type	Tool Name	Pre-Incident	Post-Incident	Terminating	Non-Terminating
Kernel Level	Kernel Drivers	Pmem [14] LiME [15] ProcDump [16]		x		x
	Crash Dump Files	Built in	x		x	
	Hibernation Files	Built in	x		x	
	Debuggers	GNU Project Debugger [19] WinDbg [20] Visual Studio [21]	x	x		x
Hypervisor Level	Hypervisor	VMWare [22] LibVMI [23]	x			x
	Hypervisor	Hypersleuth [24] Vis [25] Cheng et al. [26]		x		x
System Management Level	BIOS-level	SmmBackdoor [27]	x			x
Asynchronous Device Level	Direct Memory Access	PCILeech [28] Inception [29]		x		x
	Hardware Thread Control Block	Snipsnap [30]	x			x
	Cold Boot	Built in	x		x	

Second Step: Memory Analysis

After we get the Memory we need, for example, a volatile memory, we can use Memory analysis tools like **Volatility3** to analyze the memory. Then we can do either signature Scanning or Heuristic Scanning to figure out the malware that infected the victim, there is another way, however, If we manage to quarantine the malware and extract it, we can simulate the behavior using Sandbox and gather the data from the running sandbox, for example, there is Any.run and Cuckoo

CHAPTER III

Overview of currently available tools for Volatile Memory Forensic

Memory analysis Tooling

Several memory analysis tools have been created that allow a user to parse memory dumps for useful artifacts. The open source examples of such tools include Volatility and Rekall, and some commercial tools include Cellebrite Inspector, FireEye Redline, Magnet AXIOM, and WindowsSCOPE.

volatility Tools

Volatility is capable of analyzing memory dumps from Windows, Linux, or Macintosh machines, supports many different types of file dump formats, and has an extensible application program interface (API). Volatility has emerged as the largest and best-supported framework because of its large base of contributors and independently authored plugins, many of which are geared toward platform-specific forensics. That’s why Almost all research methods make use of the Volatility software, and most commercial solutions expose or leverage Volatility within their product.

Comparison of tools

Tool Name	First Author	Year	Sandbox Analysis	Scanning Method	ML Method	Utilizes Volatility	Live Detection	Automated
	Graziano	2012	x			x		
YARA		2013		x				x
	Aghaeikheirabady	2014			x	x		
AMAL	Mohaisen	2015	x	x				x
	Tien	2017	x			x	x	
	Cohen	2017		x		x		x
	Fowler	2017		x				x
	Xu	2017			x		x	x

Tool Name	First Author	Year	Sandbox Analysis	Scanning Method	ML Method	Utilizes Volatility	Live Detection	Automated
MemScrimper	Brengel	2018		x				x
	Murthaja	2019			x	x		x
USIM Toolkit	Pendergrass	2019		x				x
SpeakEasy		2020	x					
	Lashkari	2021			x	x		
	Bozkir	2021			x	x		x
	Arfeen	2022			x	x		x

CHAPTER IV

Future Work and Conclusion

Future Work

There is a continuing need for research in the space of volatile memory acquisition and analysis. The further development of memory acquisition tools, particularly tools that reside in the system management level, is needed to develop atomic, efficient, and secure tools. The further research and validation of memory forensic methods utilizing machine learning algorithms is needed to confirm the effectiveness of those methods.

Conclusions

The landscape of volatile memory acquisition and analysis research is evolving quickly as it has proven to be a valuable forensic method. A variety of memory acquisition tools have been created for the major operating systems, but these tools vary in their accuracy, speed, and practicality.

Memory forensic methods can be classified as dynamic analysis from within a sandbox, a scanning method, or a machine learning approach. Scanning methods are fast to implement and already widely used in commercial software, but they fail to identify previously unseen malware and provide only a limited view of the behavior of the malware.

Shylock
Memory Analysis

Image Info of Shylock

./vol2 -f target.vmem imageinfo

```
┌──(mewz㉿Mewz)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./vol2 -f target.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/mewz/Downloads/volatility_2.6_lin64_standalone/target.vmem
)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545b60L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2011-09-30 00:26:30 UTC+0000
     Image local date and time : 2011-09-29 20:26:30 -0400
```

Proccess Analysis of Shylock

./vol2 -f target.vmem pslist

pslist akan melakukan analisa running process yang ada di memorinya.

```
┌──(mewz㉿Mewz)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./vol2 -f target.vmem pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------
0x819cc830 System                     4      0     60      209 ------      0
0x818efda0 smss.exe                 384      4      3       19 ------      0 2011-09-26 01:33:32 UTC+0000
0x81616ab8 csrss.exe                612    384     12      473      0      0 2011-09-26 01:33:35 UTC+0000
0x814c9b40 winlogon.exe             636    384     16      498      0      0 2011-09-26 01:33:35 UTC+0000
0x81794d08 services.exe             680    636     15      271      0      0 2011-09-26 01:33:35 UTC+0000
0x814a2cd0 lsass.exe                692    636     24      356      0      0 2011-09-26 01:33:35 UTC+0000
0x815c2630 vmacthlp.exe             852    680      1       25      0      0 2011-09-26 01:33:35 UTC+0000
0x81470020 svchost.exe              868    680     17      199      0      0 2011-09-26 01:33:35 UTC+0000
0x818b5248 svchost.exe              944    680     11      274      0      0 2011-09-26 01:33:36 UTC+0000
0x813a0458 MsMpEng.exe             1040    680     16      322      0      0 2011-09-26 01:33:36 UTC+0000
0x816b7020 svchost.exe             1076    680     87     1477      0      0 2011-09-26 01:33:36 UTC+0000
0x817f7548 svchost.exe             1200    680      6       81      0      0 2011-09-26 01:33:37 UTC+0000
0x8169a1d0 svchost.exe             1336    680     14      172      0      0 2011-09-26 01:33:37 UTC+0000
0x813685e0 spoolsv.exe             1516    680     14      159      0      0 2011-09-26 01:33:39 UTC+0000
0x818f5cd0 explorer.exe            1752   1696     32      680      0      0 2011-09-26 01:33:45 UTC+0000
0x815c9638 svchost.exe             1812    680      4      102      0      0 2011-09-26 01:33:46 UTC+0000
0x8192d7f0 VMwareTray.exe          1876   1752      3       84      0      0 2011-09-26 01:33:46 UTC+0000
0x818f6458 VMwareUser.exe          1888   1752      9      245      0      0 2011-09-26 01:33:47 UTC+000
0x8164a020 msseces.exe             1900   1752     11      205      0      0 2011-09-26 01:33:47 UTC+000
0x81717370 ctfmon.exe              1912   1752      3       93      0      0 2011-09-26 01:33:47 UTC+000
0x813a5b28 svchost.exe             2000    680      6      119      0      0 2011-09-26 01:33:47 UTC+000
0x81336638 vmtoolsd.exe             200    680      5      234      0      0 2011-09-26 01:33:47 UTC+000
0x81329b28 VMUpgradeHelper          424    680      5      100      0      0 2011-09-26 01:33:48 UTC+000
0x812d6020 wscntfy.exe             2028   1076      3       63      0      0 2011-09-26 01:33:55 UTC+000
0x812c1718 TPAutoConnSvc.e         2068    680      5       99      0      0 2011-09-26 01:33:55 UTC+000
0x812b03e0 alg.exe                 2272    680      7      112      0      0 2011-09-26 01:33:55 UTC+000
0x81324020 TPAutoConnect.e         3372   2068      3       90      0      0 2011-09-26 01:33:59 UTC+000
0x814e7b38 msiexec.exe             2396    680      5      127      0      0 2011-09-26 01:34:45 UTC+000
0x814db608 cmd.exe                 3756   1752      3       56      0      0 2011-09-30 00:20:44 UTC+000
0x812f59a8 cmd.exe                 3128    200      0 --------      0      0 2011-09-30 00:26:30 UTC+000
30 00:26:30 UTC+0000
```

Network Activity of Shylock

dari connscan kita bisa melihat bahwa ada address yang terkoneksi dari malware ini

```
┌──(mewz㉿Mewz)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./vol2 -f target.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address           Pid
----------  -------------------------  -------------------------  ---
0x014f6ab0 10.0.0.109:1072            209.190.4.84:443           1752
0x01507380 10.0.0.109:1073            209.190.4.84:443           1752
0x016c2b00 10.0.0.109:1065            184.173.252.227:443        1752
0x017028a0 10.0.0.109:1067            184.173.252.227:443        1752
0x01858cb0 10.0.0.109:1068            209.190.4.84:443           1752
```

Commandline of Shylock

./vol2 -f shylock.vmem cmdline

```
┌──(mewz㉿Mewz)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./vol2 -f shylock.vmem cmdline
Volatility Foundation Volatility Framework 2.6
**************************************************************************
System pid:     4
**************************************************************************
smss.exe pid:    384
Command line : \SystemRoot\System32\smss.exe
**************************************************************************
csrss.exe pid:    612
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 Server
ation,2 ProfileControl=Off MaxRequestThreads=16
**************************************************************************
winlogon.exe pid:    636
Command line : winlogon.exe
**************************************************************************
services.exe pid:    680
Command line : C:\WINDOWS\system32\services.exe
**************************************************************************
lsass.exe pid:    692
Command line : C:\WINDOWS\system32\lsass.exe
**************************************************************************
vmacthlp.exe pid:    852
Command line : "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
**************************************************************************
svchost.exe pid:    868
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
**************************************************************************
svchost.exe pid:    944
Command line : C:\WINDOWS\system32\svchost -k rpcss
**************************************************************************
MsMpEng.exe pid:   1040
Command line : "c:\Program Files\Microsoft Security Essentials\MsMpEng.exe"
**************************************************************************
svchost.exe pid:   1076
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
**************************************************************************
svchost.exe pid:   1200
Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService
**************************************************************************
svchost.exe pid:   1336
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
**************************************************************************
spoolsv.exe pid:   1516
Command line : C:\WINDOWS\system32\spoolsv.exe
**************************************************************************
explorer.exe pid:   1752
Command line : C:\WINDOWS\Explorer.EXE
**************************************************************************
svchost.exe pid:   1812
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
**************************************************************************
VMwareTray.exe pid:   1876
Command line : "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
**************************************************************************
VMwareUser.exe pid:   1888
Command line : "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
**************************************************************************
msseces.exe pid:   1900
Command line : "C:\Program Files\Microsoft Security Essentials\msseces.exe" -hide -runkey
**************************************************************************
ctfmon.exe pid:   1912
Command line : "C:\WINDOWS\system32\ctfmon.exe"
**************************************************************************
svchost.exe pid:   2000
Command line : C:\WINDOWS\system32\svchost.exe -k imgsvc
**************************************************************************
vmtoolsd.exe pid:    200
Command line : "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
**************************************************************************
VMUpgradeHelper pid:    424
Command line : "C:\Program Files\VMware\VMware Tools\VMUpgradeHelper.exe" /service
**************************************************************************
wscntfy.exe pid:   2028
Command line : C:\WINDOWS\system32\wscntfy.exe
**************************************************************************
TPAutoConnSvc.e pid:   2068
Command line : "C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe"
**************************************************************************
alg.exe pid:   2272
Command line : C:\WINDOWS\System32\alg.exe
**************************************************************************
TPAutoConnect.e pid:   3372
Command line : TPAutoConnect.exe -q -i vmware -a COM1 -F 30
**************************************************************************
msiexec.exe pid:   2396
Command line : C:\WINDOWS\system32\msiexec.exe /V
**************************************************************************
cmd.exe pid:   3756
Command line : "C:\WINDOWS\system32\cmd.exe"
**************************************************************************
cmd.exe pid:   3128
```

Malfind Analysis of Shylock

./vol2 -f shylock.vmem malfind

malfind menemukan file executeable yang melakukan modification di memorynya.

```
Process: explorer.exe Pid: 1752 Address: 0×3380000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Process: VMwareTray.exe Pid: 1876 Address: 0×f40000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Process: VMwareUser.exe Pid: 1888 Address: 0×2070000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Process: cmd.exe Pid: 3756 Address: 0×10000000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Process: ctfmon.exe Pid: 1912 Address: 0×10000000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Process: wscntfy.exe Pid: 2028 Address: 0×10000000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Process: TPAutoConnect.e Pid: 3372 Address: 0×10000000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Process: msseces.exe Pid: 1900 Address: 0×1220000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 612 Address: 0×7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6
```

```
Process: winlogon.exe Pid: 636 Address: 0×177a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

Dlldump on Malicious PID

./vol2 -f shylock.vmem dlldump -p <PID> -D ./ --output=<name_output>

dari hasil malfind, kita melakukan dlldump ke PID yang kami curigai, dan kami melakukan SHA256SUM kepada semua dll yang kami dump dari exe yang kami curigai, dari hasil ini kami mendapat beberapa SHA256SUM yang terflag sebagai malicious di virus total yaitu:

[cmd.exe] 8dfd506fa7936045995b63f53ccad9580f19d0ffd1aabcd1989017150d683232
[Explorer.EXE] b9352b0f0025a3fe6a8c41573b4c4869849e387733293a702d4cae13f980b286
[ctfmon.exe] 797e85ee3dd626a83a94ae93279188eddcb817d88e52951f0c22d6469cb1aeff
[vmwareuser.exe] 7f49879dfccb74cc79c8670958c907be7017e1d94f9db80ac8b60d30eeb99082
[winlogon.exe] 89133bf8330f416c14d1181b74fb9ac0a16069dbc986c14607c7938a5bd69d1d
[winlogon.exe] c078d81346771fb932a8fbd2d5b1f3a0fe36fcf2a7ad0167fac7fd1a67bf8b49
[winlogon.exe] 0fbdef6a682ac98cf2cffd3d4e092211d9aaa05ac5b0b8de79a9f3cc7235fdb6

Virus Total

cmd.exe

8dfd506fa7936045995b63f53ccad9580f19d0ffd1aabcd1989017150d683232

Sign in | Sign up

8 / 72

Community Score

8 security vendors and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

8dfd506fa7936045995b63f53ccad9580f19d0ffd1aabcd1989017150d683232

executable.3756.exe

peexe | detect-debug-environment | checks-user-input

Size: 380.00 KB

Last Analysis Date: 26 days ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 1

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

Popular threat label: trojan.

Threat categories: trojan

Security vendors' analysis

Do you want to automate checks?

Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_60% (W)
Google	Detected	Ikarus	Trojan.Win32.Tiggre
MaxSecure	Trojan.Malware.8328450.susgen	McAfee	Artemis!BCAA96209C38
Rising	Trojan.Generic@AI.94 (RDML:10M5yNX0...	Skyhigh (SWG)	BehavesLike.Win32.Dropper.fz
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected

Virus Total

Explorer.exe

b9352b0f0025a3fe6a8c41573b4c4869849e387733293a702d4cae13f980b286

Sign in | Sign up

3 / 72

Community Score

3 security vendors and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

b9352b0f0025a3fe6a8c41573b4c4869849e387733293a702d4cae13f980b286

EXPLORER.EXE

peexe

Size: 1009.50 KB

Last Analysis Date: 28 days ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 3

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

Security vendors' analysis

Do you want to automate checks?

Cynet	Malicious (score: 100)	Google	Detected
Ikarus	Trojan-Dropper.Agent	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected

Virus Total

ctfmon.exe

797e85ee3dd626a83a94ae93279188eddcb817d88e52951f0c22d6469cb1aeff

Sign in | Sign up

3 / 71

Community Score

3 security vendors and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

797e85ee3dd626a83a94ae93279188eddcb817d88e52951f0c22d6469cb1aeff

executable.1912.exe

peexe | idle | detect-debug-environment

Size: 15.00 KB

Last Analysis Date: 6 months ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

CrowdStrike Falcon	Win/malicious_confidence_60% (W)	MaxSecure	Trojan.Malware.300983.susgen
Trapmine	Suspicious.low.ml.score	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected

Virus Total

vmwareuser.exe

7f49879dfccb74cc79c8670958c907be7017e1d94f9db80ac8b60d30eeb99082

Sign in | Sign up

3 / 72

Community Score

3 security vendors and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

7f49879dfccb74cc79c8670958c907be7017e1d94f9db80ac8b60d30eeb99082

executable.1888.exe

peexe | checks-user-input | idle | detect-debug-environment

Size: 1.05 MB

Last Analysis Date: 28 days ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 1

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

Security vendors' analysis

Do you want to automate checks?

Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Bkav Pro	W32.AIDetectMalware	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected

Virus Total

winlogon.exe

89133bf8330f416c14d1181b74fb9ac0a16069dbc986c14607c7938a5bd69d1d

Sign in | Sign up

4 / 71

Community Score

4 security vendors and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

89133bf8330f416c14d1181b74fb9ac0a16069dbc986c14607c7938a5bd69d1d

executable.636.exe

peexe | detect-debug-environment

Size: 496.00 KB

Last Analysis Date: 6 months ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 1

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

Popular threat label: trojan.

Threat categories: trojan

Security vendors' analysis

Do you want to automate checks?

Google	Detected	Ikarus	Trojan.Win32.Spy
MaxSecure	Trojan.Malware.300983.susgen	Rising	Trojan.Generic@AI.95 (RDML:QFGmPqlUI...
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected

Virus Total

winlogon.exe

c078d81346771fb932a8fbd2d5b1f3a0fe36fcf2a7ad0167fac7fd1a67bf8b49

Sign in | Sign up

1 / 58

Community Score

1 security vendor and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

c078d81346771fb932a8fbd2d5b1f3a0fe36fcf2a7ad0167fac7fd1a67bf8b49

module.636.16c9b40.7c800000.dll

pedll

Size: 966.50 KB

Last Analysis Date: 6 years ago

DLL

DETECTION | DETAILS | COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

CrowdStrike Falcon	Malicious_confidence_100% (D)	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	AVware	Undetected
Baidu	Undetected	BitDefender	Undetected

Virus Total

winlogon.exe

0fbdef6a682ac98cf2cffd3d4e092211d9aaa05ac5b0b8de79a9f3cc7235fdb6

Sign in | Sign up

2 / 59

Community Score

2 security vendors and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

0fbdef6a682ac98cf2cffd3d4e092211d9aaa05ac5b0b8de79a9f3cc7235fdb6

module.636.16c9b40.7c900000.dll

pedll

Size: 698.00 KB

Last Analysis Date: 6 years ago

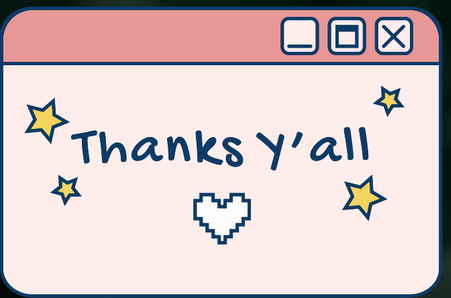
DLL

DETECTION | DETAILS | COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

CrowdStrike Falcon	Malicious_confidence_65% (D)	Qihoo-360	HEUR/QVM40.1.0000.Malware.Gen
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	AVware	Undetected

THANK YOU!