VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: uninstaller.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: dc1e6c625399e9b840047a9182c5b5f36221d71d
MD5: 4a5cddb95a6d26a6df72e0434642915d
First Seen Date: 2017-03-28 21:05:12 UTC
Number of Clients Seen: 6
Last Analysis Date: 2017-03-28 21:05:12 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Valkyrie Automatic Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-03-28 21:05:12 UTC	No Match	?
Static Analysis Overall Verdict	2017-03-28 21:05:12 UTC	Highly Suspicious	!
Dynamic Analysis Overall Verdict	2017-03-28 21:05:12 UTC	Highly Suspicious	!
Precise Detectors Overall Verdict	2017-03-28 21:05:12 UTC	No Match	?
File Certificate Validation		Certificate and Vendor name are Not Valid	?

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	!

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	✓
Non-ascii or empty section names detected	Clean	✓
Illegal size of optional Header	Clean	✓
Packer detection on signature database	Unknown	?
Based on the sections entropy check! file is possibly packed	Clean	✓
Timestamp value suspicious	Clean	✓
Header Checksum is zero!	Clean	✓
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean	✓
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	✓
Anti-vm present	Clean	✓
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Suspicious	!
TLS callback functions array detected	Clean	✓

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	!

SUSPICIOUS BEHAVIORS

Operation successfully finished.

Behavioral Information

QueryFilePath

C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Au_.exe

CreateFile

C:\
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db
C:\Users\desktop.ini
C:\Users
C:\Users\win7
C:\Users\win7\AppData
C:\Users\win7\AppData\Local
C:\Users\win7\AppData\Local\Temp

LoadLibrary

SHFOLDER
ole32.dll
comctl32.dll
ADVAPI32.dll
propsys.dll
ntmarta.dll
SHELL32.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll

CreateMutex

<NULL>

DeleteFile

C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Fu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Gu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Hu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Iu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Ju_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Ku_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Lu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Mu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Nu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Ou_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Pu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Qu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Ru_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Su_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Tu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Uu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Vu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Wu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Xu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Yu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Zu_.exe

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Not Verified ✖

[+] null

Status	Not Valid ✖

Certificate Validation - FileNotSigned ✖

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x54336EBA [Tue Oct 7 04:40:26 2014 UTC]
Entry Point	0x40322e (.text)
File Size	496013
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	mozilla.org
File Version	55.0a1
Company Name	mozilla.org
Product Name	Nightly
Product Version	55.0a1
File Description	Nightly Helper
Original Filename	helper.exe
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	c9f1308b5e62ca6bf1f172098097570b42e046d83463168e0e8ed398e9eb8b54

File Paths

FILE PATH ON CLIENT	SEEN COUNT
dc1e6c625399e9b840047a9182c5b5f36221d71d	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x60ce	0x6200	6.469683	-
.rdata	0x8000	0x1460	0x1600	4.945965	-
.data	0xa000	0x2afb8	0x600	3.895316	-
.ndata	0x35000	0x17000	0x0	0.000000[SUSPICIOUS]	-
.rsrc	0x4c000	0x7078	0x7200	5.804786	-