VALKYRIE

PUA
Valkyrie Final Verdict

File Name: IESettings.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 767aced039df5d01c9fb2f5fca285f5b4686aede
MD5: b91d5b4a2f0f92e27b2500d18e93bed0
First Seen Date: 2017-12-17 05:16:44 UTC
Number of Clients Seen: 6
Last Analysis Date: 2018-08-07 15:25:48 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2018-11-04 09:29:41 UTC	PUA
Static Analysis Overall Verdict	2018-08-07 15:25:48 UTC	No Threat Found
Precise Detectors Overall Verdict	2018-08-07 15:25:48 UTC	No Match
File Certificate Validation		Vendor is Gray Listed

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

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	Suspicious
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Creates a child process	!
Uses a function clandestinely	!
Reads memory of another process	!
Opens a file in a system directory	!
Has no visible windows	!

Behavioral Information

QueryFilePath

C:\IESettings.exe
C:\Windows\system32\DUser.dll
C:\Windows\system32\cryptnet.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Windows\System32\msxml6.dll
C:\Windows\syswow64\CRYPT32.dll
C:\Windows\system32\PROPSYS.dll
C:\Windows\syswow64\shlwapi.DLL
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll

LowerChar

http
Map
map
Email
email
Translate
translate
Internet Explorer\User Preferences!DefaultScopeMigrationTime
internet explorer\user preferences!defaultscopemigrationtime
selection
document
link
Internet Explorer\SearchScopes!ProtectSilently
internet explorer\searchscopes!protectsilently
.EXE
.exe
program
file

CreateProcess

"C:\Program Files\Internet Explorer\IEXPLORE.EXE" http://search.searchffr.com/?source=bing&uid=2b537d4c-37fc-4f73-9cef-e355bf2abcfd&uc=20171215&ap=appfocus63&i_id=recipes_spt__1.30

ReadFile

C:\IESettings.exe
C:\Users\win7\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico
C:\Windows\Fonts\staticcache.dat

OpenMutex

Local\MSCTF.Asm.MutexDefault1

WriteFile

C:\IESettings.exe
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\ECF3006D44DA211141391220EE5049F4
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C46E7B0F942663A1EDC8D9D6D7869173_6043FC604A395E1485AF7AC16D16B7CE
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\40C68D5626484A90937F0752C8B950AB
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EA618097E393409AFA316F0F87E2C202_F63C4FD203F6454721A6574A3D8B1274
C:\Users\win7\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico
C:\Users\win7\AppData\Roaming\{28e56cfb-e30e-4f66-85d8-339885b726b8}\Uninstall.exe
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C46E7B0F942663A1EDC8D9D6D7869173_DF4CA81DC775CDA9B3214BDB5B55900E
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EA618097E393409AFA316F0F87E2C202_6A2C13C9B1F727E64CC0EE73EA440D77

CreateMutex

<NULL>
{5312EE61-79E3-4A24-BFE1-132B85B23C3A}
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

LoadLibrary

OLEACCRC.DLL
api-ms-win-core-synch-l1-2-0
kernel32
api-ms-win-core-fibers-l1-1-1
api-ms-win-core-localization-l1-2-1
API-MS-Win-Security-LSALookup-L1-1-0.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
ADVAPI32.dll
CRYPTBASE.dll
OLEAUT32.dll
USERENV.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
CRYPTSP.dll
USER32.dll
ncrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
SensApi.dll
SHLWAPI.dll
profapi.dll
api-ms-win-appmodel-runtime-l1-1-1
ext-ms-win-kernel32-package-current-l1-1-0
kernel32.dll
comctl32.dll
api-ms-win-core-sysinfo-l1-2-1
api-ms-win-downlevel-shlwapi-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
C:\Windows\System32\msxml6r.dll
urlmon.dll
CRYPT32.dll
RPCRT4.dll
ole32.dll
C:\Users\win7\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico
WINTRUST.dll
WINTRUST.DLL
C:\Windows\syswow64\CRYPT32.dll
imagehlp.dll
bcrypt.dll
SHELL32.dll
propsys.dll
ntmarta.dll
Secur32.dll
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
winhttp.dll
WS2_32.dll
SspiCli.dll
ntdll.dll
DUser.dll
C:\Windows\system32\DUser.dll

user32.dll
DNSAPI.dll
UxTheme.dll
dwmapi.dll
C:\Windows\system32\xmllite.dll
imageres.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
api-ms-win-downlevel-advapi32-l2-1-0.dll
IPHLPAPI.DLL
dhcpcsvc.DLL

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise Trojan Detector 5	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise Trojan Detector 7	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise Trojan Detector 2	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2018-08-07 15:25:41 UTC	No Match		NotDetected
Static Precise Trojan Detector 10	2018-08-07 15:25:42 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2018-08-07 15:25:42 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2018-08-07 15:25:42 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Gray Listed

[+] SpringTech Ltd

Status	Not Valid

Certificate Validation - Success

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5A2FE11C [Tue Dec 12 14:01:00 2017 UTC]
Debug Artifacts	
Entry Point	0x43aad6 (.text)
Exifinfo	
File Size	3179600
File Type Enum	6
Imphash	04dfbd3d8452222364d6c71f8a772e50
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Copyright (C) 2017 SpringTech Ltd.
Internal Name	IESettings
File Version	4, 2, 0, 12
Company Name	SpringTech Ltd.
Product Name	IESettings
Product Version	4, 2, 0, 12
File Description	IESettings
Original Filename	IESettings
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	1c596d79af49102d6ebb8a3f54d53a57ba24f269a96bfab09d8768ac59394a5e
Ssdeep	
Trid	42.7,Win32 Executable (generic),19.2,OS/2 Executable (generic),18.9,Generic Win/DOS Executable,18.9,DOS Executable Generic

File Paths

FILE PATH ON CLIENT	SEEN COUNT
IESettings.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x109bab	0x109c00	6.58059111462	0ac3f771a8708f9e06a22b63d7ff0a06
.rdata	0x10b000	0x34800	0x34800	4.90180255224	290bc867c20f1a72b16d38c782c46bb3
.data	0x140000	0x7e4c	0x6a00	4.66415601879	233f8865deeb9a6913815c326bcfea54
.AESeal	0x148000	0x1ed0	0x2000	5.90367144476	fef694449aed503a8cb6ff056df3097d
.rsrc	0x14a000	0x1b2548	0x1b2600	6.24778006185	09fc89c4fc810fc4c57964e3e0c26738
.reloc	0x2fd000	0xd994	0xda00	6.600615927	08bbe49c4bb41572f6c25c87e2457f53