VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: 2
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 49a69d2915b2116161a9d7ec437ceae945a0b69c
MD5: dc0b3828159e9526a1f0b18f93dc372c
First Seen Date: 2016-06-24 05:51:27 UTC
Number of Clients Seen: 2
Last Analysis Date: 2016-06-24 05:51:27 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	2016-06-24 05:51:27 UTC	Malware	
Static Analysis Overall Verdict	2016-06-24 05:51:27 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2016-06-24 05:51:27 UTC	No Threat Found	
File Certificate Validation		Not Applicable	

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	
Opens a file in a system directory	!
Uses a function clandestinely	!
Has no visible windows	!

Behavioral Information

QueryFilePath

C:\sample
C:\Windows\system32\ODBC32.dll
C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\MSVCR90.dll

ReadRegisteryKey

Win31FileSystem
UninstallString
DisplayName
HWID

CreateFile

C:\
C:\Windows
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:\Windows\system32\EhStorShell.dll
\??\C:\Windows\system32\ntshrui.dll
C:\sample
C:\Users\win7\AppData\Local\Temp\HWID
C:\Windows\wcx_ftp.ini
C:\Users\win7\wcx_ftp.ini
C:\Users\win7\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\ProgramData\GHISLER\wcx_ftp.ini
C:\Users\win7\AppData\Local\GHISLER\wcx_ftp.ini
C:\Users\win7\AppData\Roaming\GlobalSCAPE\CuteFTP\sm.dat
C:\Users\win7\AppData\Roaming\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Users\win7\AppData\Roaming\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Users\win7\AppData\Roaming\CuteFTP\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\ProgramData\CuteFTP\sm.dat
C:\Users\win7\AppData\Local\GlobalSCAPE\CuteFTP\sm.dat
C:\Users\win7\AppData\Local\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Users\win7\AppData\Local\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Users\win7\AppData\Local\CuteFTP\sm.dat
C:\Users\win7\AppData\Roaming\FlashFXP\3\Sites.dat
C:\Users\win7\AppData\Roaming\FlashFXP\4\Sites.dat
C:\Users\win7\AppData\Roaming\FlashFXP\3\Quick.dat
C:\Users\win7\AppData\Roaming\FlashFXP\4\Quick.dat
C:\Users\win7\AppData\Roaming\FlashFXP\3\History.dat
C:\Users\win7\AppData\Roaming\FlashFXP\4\History.dat
C:\ProgramData\FlashFXP\3\Sites.dat
C:\ProgramData\FlashFXP\4\Sites.dat
C:\ProgramData\FlashFXP\3\Quick.dat
C:\ProgramData\FlashFXP\4\Quick.dat
C:\ProgramData\FlashFXP\3\History.dat
C:\ProgramData\FlashFXP\4\History.dat
C:\Users\win7\AppData\Local\FlashFXP\3\Sites.dat
C:\Users\win7\AppData\Local\FlashFXP\4\Sites.dat
C:\Users\win7\AppData\Local\FlashFXP\3\Quick.dat
C:\Users\win7\AppData\Local\FlashFXP\4\Quick.dat
C:\Users\win7\AppData\Local\FlashFXP\3\History.dat
C:\Users\win7\AppData\Local\FlashFXP\4\History.dat
C:\Users\win7\AppData\Roaming\FileZilla\sitemanager.xml
C:\Users\win7\AppData\Roaming\FileZilla\recentservers.xml

C:\Users\win7\AppData\Roaming\FileZilla\filezilla.xml
C:\ProgramData\FileZilla\sitemanager.xml
C:\ProgramData\FileZilla\recentservers.xml
C:\ProgramData\FileZilla\filezilla.xml
C:\Users\win7\AppData\Local\FileZilla\sitemanager.xml
C:\Users\win7\AppData\Local\FileZilla\recentservers.xml
C:\Users\win7\AppData\Local\FileZilla\filezilla.xml

OpenRegisteryKey

SOFTWARE\Microsoft\BidInterface\Loader
SOFTWARE\ODBC\ODBC.INI\ODBC
SYSTEM\CurrentControlSet\Control\FileSystem
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{050d4fc8-5d48-4b8f-8972-47c82c46020f}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{f65db027-aff3-4070-886a-0d87064aabb1}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}
Software\WinRAR
Software\Ghisler\Windows Commander
Software\Ghisler\Total Commander
Software\GlobalSCAPE\CuteFTP 6 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 6 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 7 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 7 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 8 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 8 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 9\QCToolbar
Software\FlashFXP\3
Software\FlashFXP
Software\FlashFXP\4
Software\FileZilla
Software\FileZilla Client
Software\VanDyke\SecureFX
Software\Opera Software
Opera.HTML\shell\open\command
Software\Mozilla

CreateMutex

<NULL>

OpenService

ProtectedStorage

LoadLibrary

imm32.dll
C:\Windows\system32\odbcint.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
ole32.dll
comctl32.dll
ADVAPI32.dll
SHELL32.dll
propsys.dll
ntmarta.dll

WindowsCodecs.dll
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ntshrui.dll
c:\windows\system32\imageres.dll
wsock32.dll
kernel32.dll
urlmon.dll
userenv.dll
user32.dll
advapi32.dll
wininet.dll
shlwapi.dll
crypt32.dll
shell32.dll
netapi32.dll
vaultcli.dll
msi.dll
pstorec.dll
rpcrt4.dll
C:\sample
SspiCli.dll

QueryProcessAddress

OpenProcess
CreateProcessA

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x576BD850 [Thu Jun 23 12:38:40 2016 UTC]
Entry Point	0x411f7b (.text)
File Size	159232
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	bed3a73572c129662abb800140dc778b1de2f004bb5943d443aacc9cb151b790

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x11594	0x11600	6.378695	-
.rdata	0x13000	0x1448c	0x14600	6.407408	-
.data	0x28000	0x658	0x400	4.286194	-
.tls	0x29000	0x9	0x200	0.000000	-
.rsrc	0x2a000	0x78c	0x800	4.506753	-