VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: tmpF57E.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: fcf68ce7332517f3dac88d335fcda26648127f79
MD5: 95492cebd656f106ee20b3f5c1038a40
First Seen Date: 2016-12-21 07:43:09 UTC
Number of Clients Seen: 3
Last Analysis Date: 2016-12-21 07:43:09 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	2016-12-21 07:43:09 UTC	Malware	
Static Analysis Overall Verdict	2016-12-21 07:43:09 UTC	Highly Suspicious	
Dynamic Analysis Overall Verdict	2016-12-21 07:43:09 UTC	Highly Suspicious	
File Certificate Validation		Not Applicable	

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	Clean	
TLS callback functions array detected	Clean	

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Creates a child process	!
Writes to address space of another process	!
Uses a function clandestinely	!
Reads memory of another process	!
Downloads a file via network	!
Opens a file in a system directory	!
Has no visible windows	!

Behavioral Information

QueryFilePath

C:\Windows\SysWOW64\svchost.exe
C:\tmpF57E.exe

LoadLibrary

urlmon.dll
user32.dll
shell32.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
Secur32.dll
SHELL32.dll
ADVAPI32.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
WS2_32.dll
winhttp.dll
IPHLPAPI.DLL
OLEAUT32.dll
DNSAPI.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
ole32.dll
comctl32.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
CRYPTBASE.dll
dhcpcsvc.DLL

ReadRegisteryKey

CacheOk
CreateUriCacheSize
EnablePunycode
FrameTabWindow
FrameMerging
SessionMerging
AdminTabProcs
TabProcGrowth
<NULL>
Compatible
Version
Platform
ConnectTimeOut
SendTimeOut
ReceiveTimeOut
SyncMode5
FEATURE_CLIENTAUTHCERTFILTER
FromCacheTimeout
SecureProtocols
DisableKeepAlive
IdnEnabled
PreConnectLimit

PreResolveLimit
SqmHttpStreamRandomUploadPoolSize
CacheMode
EnableHttp1_1
ProxyHttp1.1
EnableNegotiate
DisableBasicOverClearChannel
ClientAuthBuiltInUI
DisableReadRange
SocketSendBufferLength
SocketReceiveBufferLength
KeepAliveTimeout
MaxHttpRedirects
MaxConnectionsPerServer
MaxConnectionsPer1_0Server
MaxConnectionsPerProxy
ServerInfoTimeout
ConnectRetries
DisableNTLMPreAuth
ScavengeCacheLowerBound
CertCacheNoValidate
ScavengeCacheFileLifeTime
ScavengeCacheFileLimit
HttpDefaultExpiryTimeSecs
FtpDefaultExpiryTimeSecs
LeashLegacyCookies
SendExtraCRLF
WpadSearchAllDomains
DontUseDNSLoadBalancing
ShareCredsWithWinHttp
DnsCacheEnabled
DnsCacheEntries
DnsCacheTimeout
WarnOnPost
WarnAlwaysOnPost
WarnOnZoneCrossing
WarnOnBadCertRecving
WarnOnPostRedirect
AlwaysDrainOnRedirect
WarnOnHTTPSToHTTPRedirect
TcpAutotuning
BadProxyExpiresTime
AutoProxyDetectType
WpadOverride
DisableBranchCache
UseFirstAvailable
CombineFalseStartData
DisableFalseStartBlocklist
EnforceP3PValidity
DuoProtocols
EnableSpdyDebugAsserts
DefaultConnectionSettings
DisableSecuritySettingsCheck
SystemSetupInProgress
ProxyEnable
ProxyServer
ProxyOverride
AutoConfigURL
AutoDetect
SavedLegacySettings
EnableUTF8
WpadDecision
WpadDecisionTime
WpadExpirationDays

CreateRegisteryKey

Software\Microsoft\DownloadManager
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad

CreateFile

C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
\\.\Nsi
C:\Windows\system32\rsaenh.dll

OpenRegisteryKey

Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
Software\Microsoft\Internet Explorer\Main\FeatureControl
FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
FEATURE_MIME_HANDLING
Software\Microsoft\Internet Explorer\Main
Software\Policies\Microsoft\Internet Explorer\Main
PROTOCOLS\Name-Space Handler\
PROTOCOLS\Name-Space Handler\http\
PROTOCOLS\Name-Space Handler*\
FEATURE_BROWSER_EMULATION
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent
Software\Policies
Software
Microsoft\Windows\CurrentVersion\Internet Settings\User Agent
Pre Platform
Post Platform
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
RETRY_HEADERONLYPOST_ONCONNECTIONRESET
FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_KB936611
FEATURE_IGNORE_MAPPINGS_FOR_CREDPOLICY
FEATURE_INCLUDE_PORT_IN_SPN_KB908209
FEATURE_BUFFERBREAKING_818408
FEATURE_SKIP_POST_RETRY_ON_INTERNETWRITEFILE_KB895954
FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOWNLOAD_KB843289
FEATURE_USE_CNAME_FOR_SPN_KB911149
FEATURE_PERMIT_CACHE_FOR_AUTHENTICATED_FTP_KB910274
FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
FEATURE_DISALLOW_NULL_IN_RESPONSE_HEADERS
FEATURE_DIGEST_NO_EXTRAS_IN_URI
FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608
FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477
FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545
FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615
FEATURE_PRESERVE_SPACES_IN_FILENAMES_KB952730
FEATURE_ENABLE_PROXY_CACHE_REFRESH_KB2983228
Software\Policies\Microsoft\Internet Explorer
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266
FEATURE_COMPAT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2151543
FEATURE_SCH_SEND_AUX_RECORD_KB_2618444
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
FEATURE_MAXCONNECTIONSPERSERVER
FEATURE_MAXCONNECTIONSPER1_0SERVER
Software\Policies\Microsoft\PeerDist\Service
Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
FEATURE_URLMON_IQDA_SIZE
SOFTWARE\Microsoft\Windows\CurrentVersion\UrlMon Settings
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Microsoft\Internet Explorer\Security
System\Setup
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
FEATURE_LOCALMACHINE_LOCKDOWN
FEATURE_USE_IETLDLIST_FOR_DOMAIN_DETERMINATION
SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\users\S-1-5-21-3979321414-2393373014-2172761192-1000
Content
Cookies
History

{69DC4768-446B-4F82-A6B0-63966A243064}

CreateMutex

Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

CreateProcess

QueryProcessAddress

URLDownloadToFileW
ShellExecuteW

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	0x58014FCD [Fri Oct 14 21:36:13 2016 UTC]
Entry Point	0x4047bd (.text)
File Size	71899
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	451f3390a9758a206ad0577ffbf47164cee69443ad7aa6d355ac89b9499d2f10

File Paths

FILE PATH ON CLIENT	SEEN COUNT
fcf68ce7332517f3dac88d335fcda26648127f79	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x10998	0x10a00	5.356172	-
.data	0x12000	0x3b0	0x400	1.004700	-
.rsrc	0x13000	0x530	0x600	4.592926	-