VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: m1601251936.EXE
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 6416aea2fba47de333668c25f804fe7f87b32a00
MD5: d3a0fb2bb6aec45d25cc857a15fb5c48
First Seen Date: 2016-01-25 16:07:38 UTC
Number of Clients Seen: 3
Last Analysis Date: 2016-01-25 16:07:38 UTC
Human Expert Analysis Date: 2016-02-01 16:13:15 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2016-01-25 16:07:38 UTC	Malware
Static Analysis Overall Verdict	2016-01-25 16:07:38 UTC	Highly Suspicious
Dynamic Analysis Overall Verdict	2016-01-25 16:07:38 UTC	Highly Suspicious
Human Expert Analysis Overall Verdict	2016-02-01 16:13:15 UTC	Malware
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
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Based on the sections entropy check! file is possibly packed	Clean
Timestamp value suspicious	Clean
Header Checksum is zero!	Suspicious
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean
Packer detection on signature database	Unknown
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	
Opens a file in a system directory	
Modifies Windows Service Keys	
Has no visible windows	
Uses a function clandestinely	

Behavioral Information

QueryFilePath

C:\sample

ReadRegisteryKey

SessionMerging
CreateUriCacheSize
DisplayName
AutoDetect
ProxyHttp1.1
SendTimeOut
ServerInfoTimeout
EnableHttp1_1
InstallDate
ComputerName
SecureProtocols
DisableNTLMPreAuth
FrameTabWindow
SystemSetupInProgress
SavedLegacySettings
WpadDecisionTime
DnsCacheTimeout
SendExtraCRLF
FrameMerging
DisableFalseStartBlocklist
TcpAutotuning
AutoProxyDetectType
DontUseDNSLoadBalancing
WpadExpirationDays
ProxyServer
UseFirstAvailable
WpadDetectedUrl
ClientAuthBuiltInUI
EnforceP3PValidity
DnsCacheEntries
AdminTabProcs
ConnectTimeOut
WpadDhcp
EnableSpdyDebugAsserts
MaxConnectionsPer1_0Server
CertCacheNoValidate
LeashLegacyCookies
WarnOnPost
WpadDecisionReason
ConnectRetries
ScavengeCacheFileLifeTime
DisableReadRange
WpadSearchAllDomains
DisableBranchCache
ScavengeCacheFileLimit
SqmHttpStreamRandomUploadPoolSize
IdnEnabled
CombineFalseStartData
DefaultConnectionSettings

WarnOnBadCertRecving
DisableBasicOverClearChannel
MaxConnectionsPerProxy
PreResolveLimit
WarnOnZoneCrossing
WpadDecision
FEATURE_CLIENTAUTHCERTFILTER
SocketReceiveBufferLength
WpadDns
ShareCredsWithWinHttp
TabProcGrowth
KeepAliveTimeout
DisableSecuritySettingsCheck
WarnOnHTTPSToHTTPRedirect
DisplayVersion
FtpDefaultExpiryTimeSecs
FromCacheTimeout
EnableNegotiate
BadProxyExpiresTime
ScavengeCacheLowerBound
WpadOverride
SocketSendBufferLength
HttpDefaultExpiryTimeSecs
WarnAlwaysOnPost
AutoConfigURL
MaxConnectionsPerServer
EnablePunycode
ProxyOverride
DisableKeepAlive
DnsCacheEnabled
AlwaysDrainOnRedirect
USERNAME
CacheMode
ReceiveTimeOut
DuoProtocols
SyncMode5
WarnOnPostRedirect
CurrentVersion
PreConnectLimit
MaxHttpRedirects
ProxyEnable

CreateRegisteryKey

52-54-00-12-35-02
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Software\Microsoft\Windows\CurrentVersion\Internet Settings
{69DC4768-446B-4F82-A6B0-63966A243064}
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

CreateFile

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

OpenRegisteryKey

Fontcore
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Microsoft\Internet Explorer\Security
FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608
SchedulingAgent
Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
FEATURE_SCH_SEND_AUX_RECORD_KB_2618444
FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545
Software\Microsoft\Windows NT\CurrentVersion
Software\Policies
FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266

{E2B51919-207A-43EB-AE78-733F9C6797C3}
IEData
FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477
WIC
Software
FEATURE_COMPAT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2151543
FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOWNLOAD_KB843289
{69DC4768-446B-4F82-A6B0-63966A243064}
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
Software\Microsoft\Internet Explorer\Main\FeatureControl
SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
SYSTEM\CurrentControlSet\services\Avg\SystemValues
FEATURE_DISALLOW_NULL_IN_RESPONSE_HEADERS
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_MIME_HANDLING
FEATURE_IGNORE_MAPPINGS_FOR_CREDPOLICY
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Content
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
Software\Policies\Microsoft\Internet Explorer\Main
MobileOptionPack
History
SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_ENABLE_PROXY_CACHE_REFRESH_KB2983228
Connection Manager
{929FBD26-9020-399B-9A7A-751D61F0B942}
FEATURE_BUFFERBREAKING_818408
Software\Microsoft\Internet Explorer\Main
FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
DirectDrawEx
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
SOFTWARE\Microsoft\Windows NT\CurrentVersion
FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615
IE5BAKEX
FEATURE_PERMIT_CACHE_FOR_AUTHENTICATED_FTP_KB910274
FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}
FEATURE_PRESERVE_SPACES_IN_FILENAMES_KB952730
Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
System\Setup
FEATURE_USE_CNAME_FOR_SPN_KB911149
Software\Policies\Microsoft\Internet Explorer
FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_KB936611
Oracle VM VirtualBox Guest Additions
Volatile Environment
IE40
FEATURE_LOCALMACHINE_LOCKDOWN
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Cookies
RETRY_HEADERONLYPOST_ONCONNECTIONRESET
Software\Policies\Microsoft\PeerDist\Service
FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
AddressBook
IE4Data
FEATURE_SKIP_POST_RETRY_ON_INTERNETWRITEFILE_KB895954
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
FEATURE_DIGEST_NO_EXTRAS_IN_URI
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
FEATURE_INCLUDE_PORT_IN_SPN_KB908209

CreateMutex

Local\ZonesLockedCacheCounterMutex
Local\ZonesCacheCounterMutex

LoadLibrary

api-ms-win-downlevel-advapi32-l2-1-0.dll
imm32.dll
IPHLPAPI.DLL
CRYPTSP.dll

ole32.dll
shlwapi.dll
CRYPTBASE.dll
CRYPT32.dll
Secur32.dll
OLEAUT32.dll
DNSAPI.dll
advapi32.dll
USERENV.dll
SHELL32.dll
shell32.dll
Comctl32.dll
user32.dll
urlmon.dll
winhttp.dll
WS2_32.dll
C:\Windows\system32\ws2_32
wininet.dll
ADVAPI32.dll
dhcpcsvc.DLL
api-ms-win-downlevel-shlwapi-l2-1-0.dll
ntdll.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2016-01-25 16:40:33 UTC
Analysis End Date: 2016-02-01 16:13:15 UTC
File Upload Date: 2016-01-25 16:39:13 UTC
Human Expert Analyst Feedback: TrojWare.Win32.Dridex
Verdict: Malware
Malware Family: TrojWare.Win32.Dridex
Malware Type: Trojan Generic

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x566837E0 [Wed Dec 9 14:17:04 2015 UTC]
Entry Point	0x402038 (.text)
File Size	91648
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	e05e7e987b99c751cbe984e691124b5276131460547b8a28bb44f5214a49b0c3

File Paths

FILE PATH ON CLIENT	SEEN COUNT
6416aea2fba47de333668c25f804fe7f87b32a00	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xdcc0	0xde00	6.094911	-
.rdata	0xf000	0x5fe0	0x6000	7.146203[SUSPICIOUS]	-
.data	0x15000	0x1c7c	0x1e00	5.822219	-
.data1	0x17000	0x40	0x200	0.779425[SUSPICIOUS]	-
.reloc	0x18000	0x38c	0x400	4.486180	-