VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: dulbchlabgha.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 43a50aecddc697e729bc600b162a74bc7ff1f8ce
MD5: dfea5046edf5fdbff8a31344b0ae98d1
First Seen Date: 2016-06-12 12:45:17 UTC
Number of Clients Seen: 5
Last Analysis Date: 2016-06-12 12:45:17 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	2016-06-12 12:45:17 UTC	Malware	
Static Analysis Overall Verdict	2016-06-12 12:45:17 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2016-06-12 12:45:17 UTC	Highly Suspicious	
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!	Suspicious	
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	
Modifies Windows policies	!
Uses a function clandestinely	!
Modifies Windows Service Keys	!
Downloads data from internet	!
Downloads a file via network	!
Opens a file in a system directory	!
Has no visible windows	!

Behavioral Information

QueryFilePath

C:\sample

CreateRegisteryKey

Software\Microsoft\DownloadManager
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
Software\Microsoft\Windows\CurrentVersion\Internet Settings
System\CurrentControlSet\Services\Tcpip\Parameters
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
{69DC4768-446B-4F82-A6B0-63966A243064}
52-54-00-12-35-02
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History

LoadLibrary

API-MS-Win-Core-LocalRegistry-L1-1-0.dll
SHFOLDER
ole32.dll
comctl32.dll
ADVAPI32.dll
SHELL32.dll
propsys.dll
ntmarta.dll
C:\Users\win7\AppData\Local\Temp\nsjD9ED.tmp\System.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
Secur32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
WS2_32.dll
winhttp.dll
IPHLPAPI.DLL
OLEAUT32.dll
DNSAPI.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
CRYPTBASE.dll
dhcpcsvc.DLL
urlmon.dll
Comctl32.dll
C:\Windows\system32\ws2_32
bcrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.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
IsTextPlainHonored
WpadDecisionReason
WpadDhcp
WpadDns
WpadDetectedUrl
PrivacyAdvanced
SecurityIdlUriCacheSize
CLSID

InternetDownload

cc000c
t"http://pv.sohu.com/cityjson"
t"http://w.x.baidu.com/go/full/201/1202000538"

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:\sample
C:\Users\win7\AppData\Local\Temp\nsuD9DD.tmp
C:\Users\win7\AppData\Local\Temp\nsjD9ED.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsjD9ED.tmp\1.ico
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
\\.\Nsi
C:\Windows\system32\rsaenh.dll
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0G27RVV\cityjson[1].txt
1.zip
C:\Users\win7\AppData\Local\Temp\nsjD9ED.tmp\nsvDD88.tmp
C:\Users\win7\AppData\Local\Temp\nsjD9ED.tmp\1.zip
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Cookies\TSXYEQJ7.txt
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\RGC5OOPl\Ccmaxgal_TN_channel1_2016-05-29_14-42-09_80_3.3.2.1028_1202000538[1].exe
56a190le_1202000538.exe

OpenRegisteryKey

SOFTWARE\Microsoft\OLEAUT
Software\Microsoft\Windows\CurrentVersion\Setup
Software\Microsoft\Windows\CurrentVersion
system\CurrentControlSet\control\NetworkProvider\HwOrder
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\sample
CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
{babe9b11-0f98-11e5-b301-806e6f6e6963}\
Drive\shellex\FolderExtensions
Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Software\Policies\Microsoft\Windows\Explorer
Software\Microsoft\Windows\CurrentVersion\Explorer
<NULL>
Advanced
Software\Microsoft\Windows\Shell\RegisteredApplications\UrlAssociations\Directory\OpenWithProgids
Software\Microsoft\Windows\Shell\Associations\UrlAssociations\Directory
Directory
CurVer
ShellEx\IconHandler
Folder
AllFilesystemObjects

DocObject
BrowseInPlace
Clsid
Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}
PropertyBag
SessionInfo\1
KnownFolders
Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
Software\Microsoft\COM3
CLSID\{1F486A52-3CB1-48FD-8F50-B8DC300D9F9D}
InprocServer32
Software\Microsoft\OLE
TreatAs
System\CurrentControlSet\Services\LDAP
{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
Software\Microsoft\Rpc
Software\Policies\Microsoft\Windows NT\Rpc
{5E6C858F-0E22-4760-9AFE-EA3317B67173}
Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3979321414-2393373014-2172761192-1000
{babe9b14-0f98-11e5-b301-806e6f6e6963}\
{babe9b10-0f98-11e5-b301-806e6f6e6963}\
t s
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*\
Software\Microsoft\Ole
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
{352481E8-33BE-4251-BA85-6007CAEDCF9D}
.DEFAULT
Software\Microsoft\Windows NT\CurrentVersion\ProfileList
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
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
System\CurrentControlSet\Services\WinSock2\Parameters
AppId_Catalog
0FF82528
Protocol_Catalog9

00000005
Catalog_Entries
000000000001
000000000002
000000000003
000000000004
000000000005
000000000006
000000000007
000000000008
000000000009
000000000010
NameSpace_Catalog5
00000028
System\CurrentControlSet\Services\Winsock2\Parameters
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
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\
ZoneMap\Ranges\
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
Microsoft\Internet Explorer\Security
System\Setup
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
FEATURE_LOCALMACHINE_LOCKDOWN
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4
Software\Microsoft\windows\CurrentVersion\Internet Settings
Domains\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\
ProtocolDefaults\
SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\users\S-1-5-21-3979321414-2393373014-2172761192-1000
Content
{F1B32785-6FBA-4FCF-9D55-7B8E7F157091}
Cookies
{2B0F765D-C0E9-4171-908E-08A611B84FF6}
History
{D9DC8A3B-B784-432E-A781-5A1130A75963}
SYSTEM\CurrentControlSet\Services\Winsock\Parameters
System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock
SYSTEM\CurrentControlSet\Services\Winsock\Setup Migration\Providers
Tcpip6
CLSID\{DCB00C01-570F-4A9B-8D69-199FDBA5723B}
CLSID\{A47979D2-C419-11D9-A5B4-001185AD2B89}
System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
Tcpip
System\CurrentControlSet\Services\DnsCache\Parameters
Software\Policies\Microsoft\Windows NT\DnsClient

Software\Policies\Microsoft\System\DNSClient
AppID\sample
Software\Microsoft\OLE\AppCompat
SOFTWARE\Microsoft\OLE
SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider
Software\Policies\Microsoft\Cryptography
Software\Microsoft\Cryptography
Software\Microsoft\Cryptography\Offload
Interface\{00000134-0000-0000-C000-000000000046}
ProxyStubClsid32
SYSTEM\CurrentControlSet\Services\BFE
Interface\{D0074FFD-570F-4A9B-8D69-199FDBA5723B}
CLSID\{1299CF18-C4F5-4B6A-BB0F-2299F0398E27}
Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}
Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}
Interface\{55272A00-42CB-11CE-8135-00AA004BB851}
CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}
Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}
Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}
SYSTEM\CurrentControlSet\Services\NetBT\Linkage
{69DC4768-446B-4F82-A6B0-63966A243064}
System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
{cfe68b1e-656a-488b-8077-738ca67ba3a5}
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{CFE68B1E-656A-488B-8077-738CA67BA3A5}
{3d3783a2-703a-11de-8c7a-806e6f6e6963}
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{3D3783A2-703A-11DE-8C7A-806E6F6E6963}
SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{3D3783A2-703A-11DE-8C7A-806E6F6E6963}
{1409cd30-b4f5-4078-86aa-9b8c995c7d0c}
SYSTEM\CurrentControlSet\Services\Tcpip\Linkage
MIME\Database\Content Type\text/json; charset=gbk
MIME\Database\Content Type\text/json
FEATURE_SHOW_CERT_WARNINGS_ON_POST_FROM_ISTREAM_KB2894776
SOFTWARE\Classes\PROTOCOLS\Filter\text/json; charset=gbk
FEATURE_MIME_SNIFFING
CLSID\{C39EE728-D419-4BD4-A3EF-EDA059DBD935}
Interface\{B06B0CE5-689B-4AFD-B326-0A08A1A647AF}
CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}
baidu.com
FEATURE_ZONE_ELEVATION
FEATURE_DISABLE_INTERNAL_SECURITY_MANAGER
MIME\Database\Content Type\application/octet-stream
SOFTWARE\Classes\PROTOCOLS\Filter\application/octet-stream
FEATURE_PROTOCOL_LOCKDOWN
FEATURE_FEEDS
FEATURE_ENABLE_COMPAT_LOGGING

CreateMutex

<NULL>
t "BoltInstall"
B
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

DeleteFile

C:\Users\win7\AppData\Local\Temp\nsuD9DC.tmp
C:\Users\win7\AppData\Local\Temp\nsjD9ED.tmp
C:\Users\win7\AppData\Local\Temp\nsjD9ED.tmp\1.zip

QueryProcessAddress

URLDownloadToFile
URLDownloadToFileW

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	0x52AFF32D [Tue Dec 17 06:46:05 2013 UTC]
Entry Point	0x403a37 (.text)
File Size	133623
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	c35b3ee5eb9e8a88cadc1a00e3a37cb9d04ef59ba5763d55abe65e019acec93c

File Paths

FILE PATH ON CLIENT	SEEN COUNT
00000000-0000-0000-0000-000000000000	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x7dc6	0x7e00	6.560512	-
.rdata	0x9000	0x30a0	0x3200	4.542302	-
.data	0xd000	0x72b9c	0x200	2.020663	-
.ndata	0x80000	0x1a1000	0x0	0.000000[SUSPICIOUS]	-
.rsrc	0x221000	0x3ee0	0x4000	2.235343	-