Summary

File Name: None

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

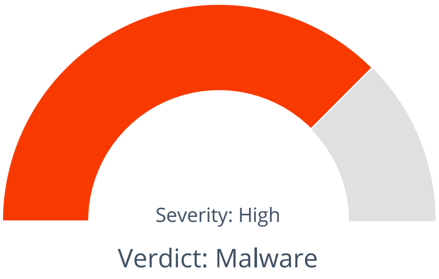
SHA1: 273bb9afae4db2d8847b5a22c455c6fd858e6af7

MD5:

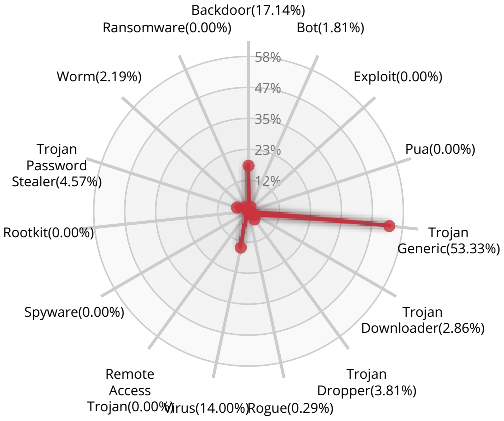
MALWARE

Valkyrie Final Verdict

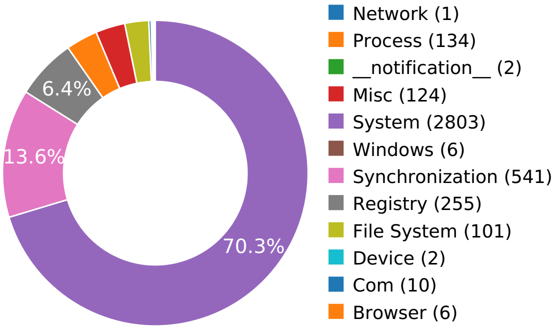
DETECTION SECTION



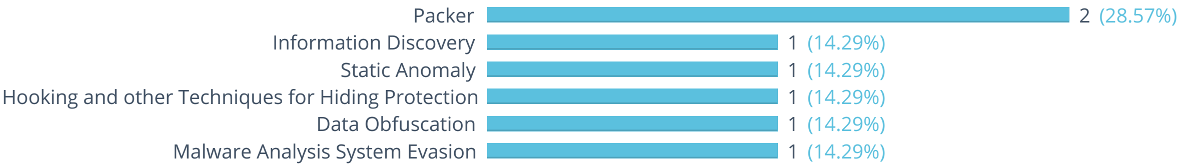
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

PACKER

The binary likely contains encrypted or compressed data. — Show sources

The executable is compressed using UPX — Show sources

STATIC ANOMALY

Anomalous binary characteristics — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

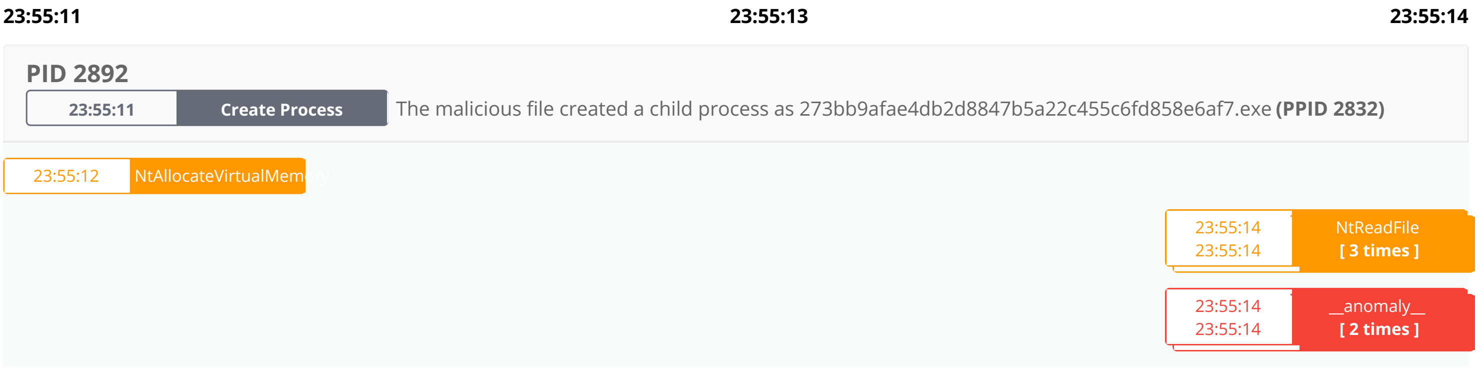
DATA OBFUSCATION

Unconventionial binary language: Chinese (Simplified)

MALWARE ANALYSIS SYSTEM EVASION

Tries to unhook or modify Windows functions monitored by Cuckoo — Show sources

Behavior Graph



23:55:11 23:55:13 23:55:14

PID 2892

23:55:11 Create Process The malicious file created a child process as 273bb9afae4db2d8847b5a22c455c6fd858e6af7.exe **(PPID 2832)**

23:55:12 NtAllocateVirtualMemory

23:55:14
23:55:14 NtReadFile **[3 times]**

23:55:14
23:55:14 __anomaly__ **[2 times]**

Behavior Summary

ACCESSED FILES

C:\Windows\SysWOW64\ntdll.dll

C:\Windows\SysWOW64\KernelBase.dll

C:\Windows\SysWOW64\kernel32.dll

C:\Windows\SysWOW64\user32.dll

C:\Windows\SysWOW64\advapi32.dll

C:\Windows\SysWOW64\IPHLPAPI.DLL

\Device\KsecDD

C:\Users\user\AppData\Local\Temp\273bb9afae4db2d8847b5a22c455c6fd858e6af7.exe

C:\Windows\SysWOW64\msscript.ocx

C:\Users\user\AppData\Local\Temp\gzip.dll

C:\Users\user\AppData\Local\Temp\AppLink\gzip.dll

C:\Users\user\AppData\Local\Temp\AppLink\zlib.dll

C:\Windows\win.ini

C:\Windows\System32\uxtheme.dll.Config

C:\Windows\System32\uxtheme.dll

C:\Users\user\AppData\Local\Temp\273bb9afae4db2d8847b5a22c455c6fd858e6af7.exe.Local\

C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

C:\Windows\WindowsShell.Manifest

C:\Windows\Fonts\staticcache.dat

C:\Users\user\AppData\Local\Temp\\xc2\xa0\xc3\xba\x18

C:\Users\user\AppData\Local\Temp\

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Name

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\DX6TextureEnumInclusionList\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\DX6TextureEnumInclusionList\Name

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Direct3D HAL\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Direct3D HAL\Name

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Ramp Emulation\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Ramp Emulation\Name

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\RGB Emulation\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\RGB Emulation\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0\0\win32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\COM+Enabled
HKEY_CURRENT_USER\Software\Microsoft\Windows Script\Settings\JITDebug
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\zlib.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\gzip.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInset
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragMinDist
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInterval
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext

RESOLVED APIS

ntdll.dll.RtlUnicodeStringToAnsiString
ntdll.dll.RtlAnsiStringToUnicodeString
ntdll.dll._vsnwprintf
ntdll.dll.memset
ntdll.dll.RtlFreeAnsiString
ntdll.dll.RtlFreeHeap
ntdll.dll.RtlDeleteCriticalSection
ntdll.dll.RtlInitializeCriticalSection
ntdll.dll.RtlAllocateHeap
ntdll.dll.CsrVerifyRegion
ntdll.dll.RtlGetNativeSystemInformation
ntdll.dll.NtQuerySystemInformation
ntdll.dll.RtlCreateTagHeap
ntdll.dll.NtQueryInformationProcess
ntdll.dll.NtSetInformationProcess
ntdll.dll.NtClose
ntdll.dll.NtSetInformationFile
ntdll.dll.NtCreateIoCompletion
ntdll.dll.NtSetIoCompletion
ntdll.dll.RtlSetLastWin32Error
ntdll.dll.SbSelectProcedure
ntdll.dll.NtRemoveIoCompletion
ntdll.dll.RtlDeactivateActivationContextUnsafeFast
ntdll.dll.NtRemoveIoCompletionEx
ntdll.dll.RtlActivateActivationContextUnsafeFast
ntdll.dll.NtCreateNamedPipeFile
ntdll.dll.NtOpenFile
ntdll.dll.NtWaitForSingleObject
ntdll.dll.NtFsControlFile

ntdll.dll.NtCreateEvent
ntdll.dll.NtQueryInformationFile
ntdll.dll._allmul
ntdll.dll.RtlSetDaclSecurityDescriptor
ntdll.dll.RtlCreateSecurityDescriptor
ntdll.dll.RtlDefaultNpAcl
ntdll.dll.RtlDosPathNameToNtPathName_U
ntdll.dll.RtlAppendUnicodeStringToString
ntdll.dll._wcsnicmp
ntdll.dll.RtlPrefixString
ntdll.dll.RtlInitUnicodeString
ntdll.dll.RtlFreeUnicodeString
ntdll.dll.RtlDetermineDosPathNameType_U
ntdll.dll.RtlCreateUnicodeString
ntdll.dll.memcpy
ntdll.dll.NtDeviceIoControlFile
ntdll.dll.NtCreateFile
ntdll.dll.RtlTimeToTimeFields
ntdll.dll.RtlTimeFieldsToTime
ntdll.dll.RtlAcquirePrivilege
ntdll.dll.RtlInitializeSRWLock
ntdll.dll.RtlReleaseSRWLockExclusive
ntdll.dll.RtlAcquireSRWLockExclusive
ntdll.dll.RtlCutoverTimeToSystemTime
ntdll.dll.RtlReleaseSRWLockShared
ntdll.dll.RtlAcquireSRWLockShared
ntdll.dll.RtlReleasePrivilege
ntdll.dll.NtSetSystemTime
ntdll.dll.RtlUnicodeStringToInteger
ntdll.dll.wcschr
ntdll.dll.wcscpy_s
ntdll.dll.RtlpCheckDynamicTimeZoneInformation
ntdll.dll._stricmp
ntdll.dll._wcsicmp

ntdll.dll.RtlDeregisterWaitEx

ntdll.dll.RtlCreateTimerQueue

ntdll.dll.NtDelayExecution

ntdll.dll.RtlCreateTimer

ntdll.dll.RtlUpdateTimer

ntdll.dll.RtlDeleteTimer

ntdll.dll.RtlDeleteTimerQueueEx

ntdll.dll.RtlRegisterWait

ntdll.dll.wcsrchr

ntdll.dll.NtQueryValueKey

ntdll.dll.NtOpenKey

ntdll.dll.RtlxAnsiStringToUnicodeSize

ntdll.dll.NlsMbCodePageTag

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Direct3D

HKEY_LOCAL_MACHINE\Software\Microsoft\Direct3D\Drivers

HKEY_CURRENT_USER\Software\Microsoft\Direct3D

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\Scheduler

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Name

HKEY_LOCAL_MACHINE\Software\Microsoft\Direct3D\DX6TextureEnumInclusionList

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\DX6TextureEnumInclusionList\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\DX6TextureEnumInclusionList\Name

HKEY_CURRENT_USER\Software\Microsoft\Direct3D\Drivers

HKEY_LOCAL_MACHINE\Software\Microsoft\Direct3D\Drivers\Direct3D HAL

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Direct3D HAL\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Direct3D HAL\Name

HKEY_LOCAL_MACHINE\Software\Microsoft\Direct3D\Drivers\Ramp Emulation

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Ramp Emulation\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\Ramp Emulation\Name

HKEY_LOCAL_MACHINE\Software\Microsoft\Direct3D\Drivers\RGB Emulation

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\RGB Emulation\Size

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Direct3D\Drivers\RGB Emulation\Name

HKEY_CURRENT_USER\System\CurrentControlSet\Control\GraphicsDrivers\Scheduler

HKEY_CURRENT_USER\Software\Microsoft\Direct3D\MostRecentApplication
HKEY_CURRENT_USER\Software\Microsoft\Direct3D\MostRecentApplication\Name
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SQMClient\Windows
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\TypeLib
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0\0
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0\0\win32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0\0\win32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID
HKEY_CURRENT_USER\Software\Classes\Wow6432Node\CLSID\{F414C260-6AC0-11CF-B6D1-00AA00BBBB58}\Implemented Categories\{7DD95802-9882-11CF-9FA9-00AA006C42C4}
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\COM+Enabled
HKEY_CURRENT_USER\Software\Microsoft\Windows Script\Settings
HKEY_CURRENT_USER\Software\Microsoft\Windows Script\Settings\JITDebug
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\zlib.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\gzip.dll
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\273bb9afae4db2d8847b5a22c455c6fd858e6af7.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInset
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragDelay

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragMinDist
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInterval
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8

READ FILES

C:\Windows\SysWOW64\ntdll.dll
C:\Windows\SysWOW64\KernelBase.dll
C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\user32.dll
C:\Windows\SysWOW64\advapi32.dll
C:\Windows\SysWOW64\IPHLPAPI.DLL
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\273bb9afae4db2d8847b5a22c455c6fd858e6af7.exe
C:\Windows\SysWOW64\msscript.ocx
C:\Users\user\AppData\Local\Temp\gzip.dll
C:\Users\user\AppData\Local\Temp\AppLink\gzip.dll

C:\Users\user\AppData\Local\Temp\AppLink\zlib.dll

C:\Windows\win.ini

C:\Windows\System32\uxtheme.dll.Config

C:\Windows\System32\uxtheme.dll

C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

C:\Windows\WindowsShell.Manifest

C:\Windows\Fonts\staticcache.dat

C:\Users\user\AppData\Local\Temp\\xc2\xa0\xc3\xba\x18

MUTEXES

CicLoadWinStaWinSta0

Local\MSCTF.CtfMonitorInstMutexDefault1

MODIFIED REGISTRY KEYS

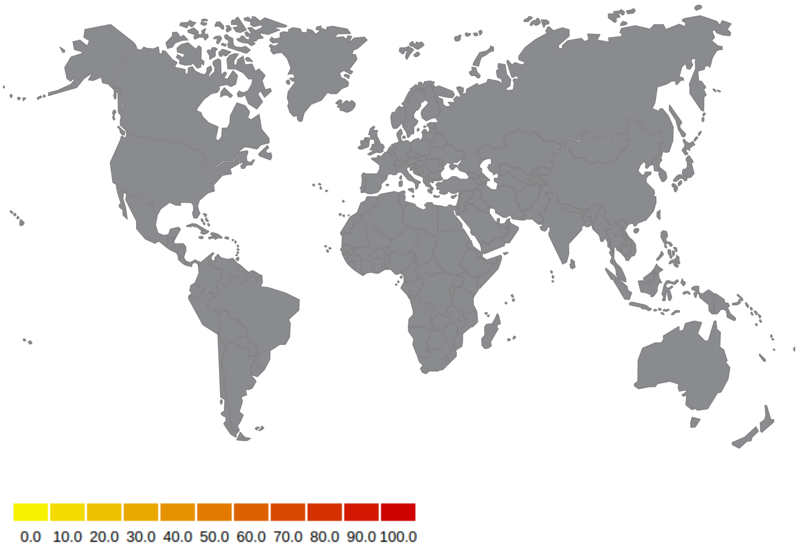
HKEY_CURRENT_USER\Software\Microsoft\Direct3D\MostRecentApplication\Name

HKEY_CURRENT_USER\Software\Microsoft\Multimedia\DrawDib

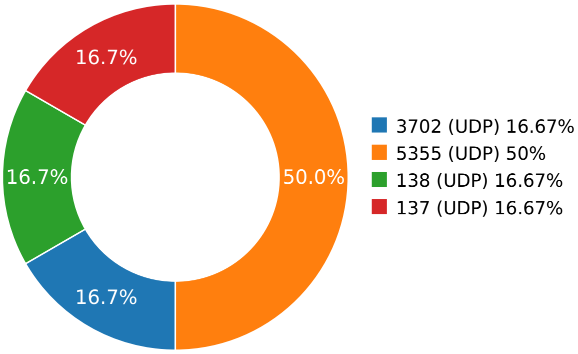
HKEY_CURRENT_USER\Software\Microsoft\Multimedia\DrawDib\ 800x600x32(BGR 0)

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.06677412987	Sandbox	224.0.0.252	5355
3.06729102135	Sandbox	224.0.0.252	5355
3.07387113571	Sandbox	239.255.255.250	3702
3.1248960495	Sandbox	192.168.56.255	137
5.65587902069	Sandbox	224.0.0.252	5355
9.13804411888	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES
DebuggerCheck__RemoteAPI
DebuggerHiding__Thread
ThreadControl__Context
anti_dbg
screenshot
keylogger
win_registry
win_private_profile
win_files_operation
win_hook
Str_Win32_Winsock2_Library

STATIC FILE INFO

File Name:	None
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	273bb9afae4db2d8847b5a22c455c6fd858e6af7
MD5:	
First Seen Date:	2018-11-06 22:07:22.461616 (4 months ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-11-06 22:07:22.461616 (4 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[78.5, u'Win32 Executable MS Visual C++ (generic)'], [11.3, u'Win32 Executable (generic)'], [5.0, u'Generic Win/DOS Executab
Compilation Time Stamp	0x5B9CF46B [Sat Sep 15 12:00:43 2018 UTC]
LegalCopyright	\u672c\u7a0b\u5e8f\u6765\u81ea\u5dc5\u5cf0\u9601\u793e\u533a[www.52dfg.com]\uff0c\u7a0b\u5e8f\u6c38\u4e45\u5
FileVersion	1.0.0.0
CompanyName	\u5dc5\u5cf0\u9601\u793e\u533a
Comments	\u5dc5\u5cf0\u9601\u539f\u521b\u4f5c\u54c1
ProductName	\u5dc5\u5cf0\u6279\u91cf\u5361iphone
ProductVersion	1.0.0.0
FileDescription	\u6279\u91cf\u5b8c\u6210\u5361iphone\u64cd\u4f5c
Translation	0x0804 0x04b0
Entry Point	0x86d0f6 (UPX)
Machine Type	Intel 386 or later - 32Bit
File Size	2961488
Ssdeep	49152:y+NI1j72mC/n/kOgawoTFbQW9lyELCcN1rQOPUC1UUFVPb0jBzWz8kwYISKy:y+NIV+n+at5n9lYcvrQOPCwVD0jB6Ykb
Sha256	f90362bb00bf3deacb742fa9f261a65863aa93f888902d15fe19606d889b46a2
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/7/3/ u'\u5dc5\u5cf0\u6279\u91cf\u5361iphone', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:11: u'2018:11:06 22:07:04+00:00', u'EXE:FileVersionNumber': u'1.0.0.0', u'EXE:FileVersion': u'1.0.0.0', u'File:FileSize': u'2.8 MB', u' compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1.0.0.0', u'EXE:ObjectFileType': u'Executable application', u'Fil u'\u5dc5\u5cf0\u9601\u793e\u533a', u'File:FileName': u'273bb9afae4db2d8847b5a22c455c6fd858e6af7', u'EXE:ImageVersi u'PE32', u'EXE:TimeStamp': u'2018:09:15 12:00:43+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LegalCopyright': u'\u672c\u7a0b\u5e8f\u6765\u81ea\u5dc5\u5cf0\u9601\u793e\u533a[www.52dfg.com]\uff0c\u7a0b\u5e8f\u6c38\u4e45\u u'EXE:LinkerVersion': 6.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_s u'\u6279\u91cf\u5b8c\u6210\u5361iphone\u64cd\u4f5c', u'EXE:EntryPoint': u'0x46d0f6', u'EXE:SubsystemVersion': 5.0, u'EX u'\u5dc5\u5cf0\u9601\u539f\u521b\u4f5c\u54c1', u'File:FileInodeChangeDate': u'2018:11:06 22:07:04+00:00', u'EXE:Uninitia u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	dc8354a22555d46e6efe868f812ec764

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x304000	0x15f000	7.99873770736	07ff277d78ecef5fc9ceb6d1e732b6ae
UPX	0x305000	0x16a000	0x16a000	7.00979676009	ebc83a66d5226b8b53b94cea6edca07b
.idata	0x46f000	0x1000	0x1000	1.5844152957	fbbbd974709a78b33f609d2b3515a6d4
.rsrc	0x470000	0x5000	0x5000	3.57477057156	bb25ca0dcacfaba2cef54063085c2b9d
UPX	0x475000	0x1000	0x1000	7.98422288413	d33df41f05f9e3936ef89686105dc74e

PE Imports

- MSVFW32.dll
    - DrawDibDraw
- AVIFIL32.dll
    - AVIStreamInfoA
- WINMM.dll
    - midiOutPrepareHeader
- WS2_32.dll
    - inet_addr
- KERNEL32.dll
    - InterlockedIncrement
- USER32.dll
    - PostThreadMessageA
- GDI32.dll
    - GetPixel
- WINSPOOL.DRV
    - OpenPrinterA
- comdlg32.dll
    - GetOpenFileNameA
- ADVAPI32.dll
    - RegOpenKeyA
- SHELL32.dll
    - DragFinish
- ole32.dll
    - OleIsCurrentClipboard
- OLEAUT32.dll
    - SafeArrayPutElement
- COMCTL32.dll
    - ImageList_Read
- oledlg.dll
    - None
- MSVCRT.dll
    - strncpy
- IPHLPAPI.DLL
    - GetInterfaceInfo
- PSAPI.DLL
    - GetMappedFileNameW

PE Resources

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 4653648, u'sha256': u'c70bbabb35024b71265ad0cbc6b6553146b8417e6469c7031b292f87ac7f027c', u'type': u'data', u'size': 744}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 4654392, u'sha256': u'bfd6b9443d835d48f4872879c901fd73a9cb1dcd85ceb44ab769410cf282b756', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 4654688, u'sha256': u'e8a96a1eeda5446b8c10f9f22d704c533ec975791eb6297eff643ad66353e422', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 4664328, u'sha256': u'5ad1f83a667f35cb623df37c22a3bb03cbb8a54251dcfa378e45d842ac97e8d8', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 4668592, u'sha256': u'8a3b6598830451b00c3e42c58a5bb6771b67f70c7beda6f78302a0a09ab13d92', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 4669748, u'sha256': u'08b0d4676557520858c02da939000fba6d9291b000ab5f7b120c7f49008a5016', u'type': u'MS Windows icon resource - 3 icons, 48x48', u'size': 48}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_ICON', u'offset': 4669796, u'sha256': u'a0c9d012e2bf6b2fe05c2d97cb5594d97cf2f539e97935c12abd7a3562f4d9bf', u'type': u'MS Windows icon resource - 1 icon, 32x32, 16 colors', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_ICON', u'offset': 4669816, u'sha256': u'6bcce1250099cc08d574211b3debabb0244cd2641f6d960538e7ddc97d319164', u'type': u'MS Windows icon resource - 1 icon, 16x16, 16 colors', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_VERSION', u'offset': 4669836, u'sha256':

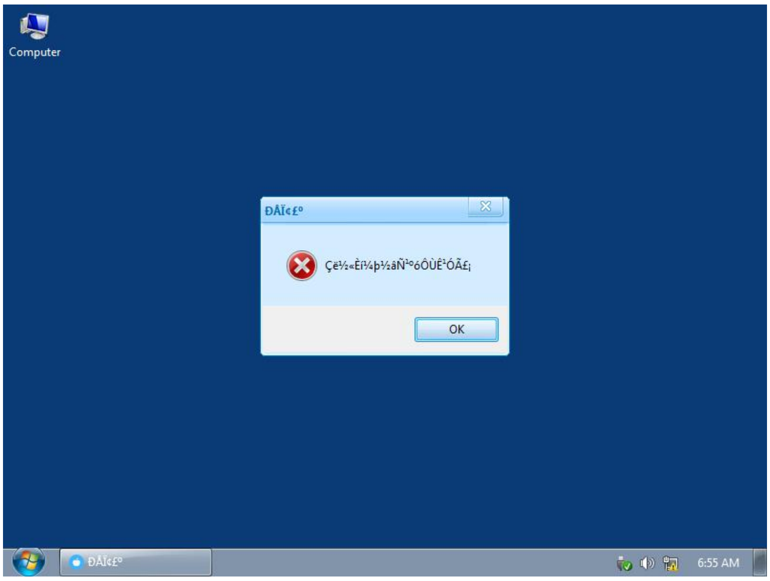
u'c714acc06e55f8ffb4d5dac4808b4609a087a572c68b39f0debe176d3fba8ae5', u'type': u'DOS executable (COM)', u'size': 652}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 4670488, u'sha256': u'b595c22caf4a7dc4766ed7d679ab5a800204dc25ddf07c106b21b430dde38aad', u'type': u'XML 1.0 document, ASCII text, with very long lines, with no line terminators', u'size': 466}

CERTIFICATE VALIDATION

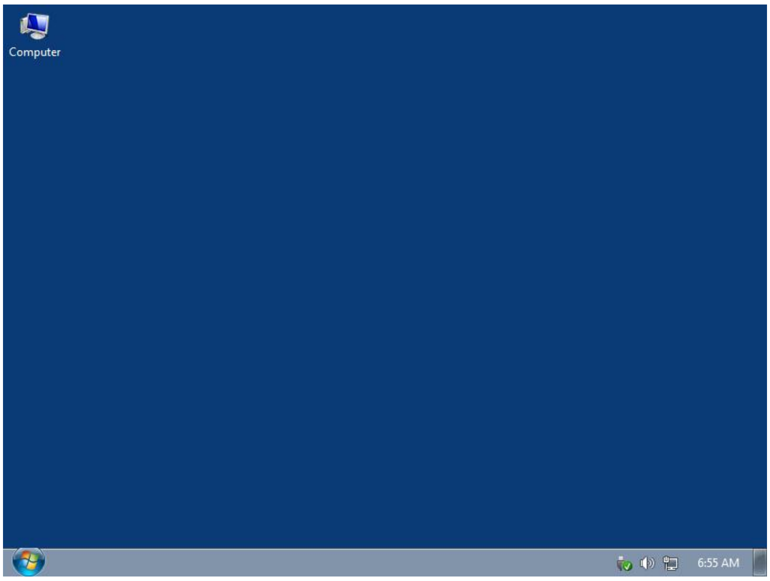
- Certificate Validation is not Applicable ?

SCREENSHOTS



ÐÅÏ¢£º

Çë½«Èí¼þ½âÑ¹ºóÔÙÊ¹ÓÃ£¡


Computer
6:55 AM