VALKYRIE
COMODO

File Name: ThisMayBeMalware11.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: be3e6a4405c5afda221e886bbc56f9326c139121
MD5: ee885e7c0ee7945a6b4275e61a08d177
First Seen Date: 2016-04-20 17:13:44 UTC
Number of Clients Seen: 3
Last Analysis Date: 2016-04-20 17:13:44 UTC
Human Expert Analysis Date: 2016-04-20 18:50:41 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

MALWARE
Valkyrie Final Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2016-04-20 17:13:44 UTC	No Match
Static Analysis Overall Verdict	2016-04-20 17:13:44 UTC	Highly Suspicious
Dynamic Analysis Overall Verdict	2016-04-20 17:13:44 UTC	No Threat Found
Human Expert Analysis Overall Verdict	2016-04-20 18:50:41 UTC	Malware
File Certificate Validation	2016-05-10 20:17:10	Certificate Valid,Vendor name Not Valid

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	Suspicious
TLS callback functions array detected	Clean

Anti-debug calls

FindWindowExA

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS
Reads memory of another process
Writes to address space of another process
Creates a child process
Opens a file in a system directory
Has no visible windows

Behavioral Information

LoadLibrary

SHFOLDER

ole32.dll

comctl32.dll

ADVAPI32.dll

SHELL32.dll

propsys.dll

ntmarta.dll

API-MS-Win-Core-LocalRegistry-L1-1-0.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\CheckRunVirtual.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\FindProcDLL.dll

PSAPI.DLL

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\Banner.dll

UxTheme.dll

C:\Windows\system32\ole32.dll

C:\Windows\syswow64\MSCTF.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\NSISdl.dll

API-MS-Win-Security-SDDL-L1-1-0.dll

WS2_32.dll

OLEAUT32.DLL

C:\Windows\SysWOW64\ieframe.dll

kernel32.dll

api-ms-win-downlevel-shlwapi-l2-1-0.dll

api-ms-win-downlevel-ole32-l1-1-0.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\DialogEx.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\System.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\ShellLink.dll

urlmon.dll

RichEd20

GdiPlus

C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\GdiPlus.DLL

WindowsCodecs.dll

IMM32.dll

C:\Windows\system32\shell32.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\ToolTips.dll

imageres.dll

ReadRegisteryKey

ProgramFilesDir

Disable

DataFilePath

Plane1

Plane2

Plane3

Plane4

Plane5

Plane6

Plane7

Plane8

Plane9

Plane10

Plane11

Plane12

Plane13

Plane14

Plane15

Plane16

ProxyEnable

CreateUriCacheSize

EnablePunycode

CreateRegisteryKey

SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BROWSER_EMULATION

Software\hmrl\huamaorili

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\nszD3A.tmp

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\CheckRunVirtual.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\FindProcDLL.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\Banner.dll

C:\Windows\Fonts\staticcache.dat

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\NSISdl.dll

C:\Users\win7\AppData\Roaming\azbconfig.ini

\\.\Nsi

C:\Users\win7\AppData\Roaming\kp2configuration.ini

C:\Users\win7\AppData\Roaming\.ico

\??\C:\Windows\SysWOW64\ieframe.dll

C:\Users\win7\Desktop\99.lnk

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\DialogEx.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\System.dll

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\ShellLink.dll

C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk

C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk

C:\Windows\desktop.ini

C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\1finish.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\1jieya_button.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\bg.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\bg_02.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\cancel.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\change.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\check-box.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\delete.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\down.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\finish.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\go.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\img_01.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\input_01.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\jieya_button.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\jindutiao.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\up.png

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\ToolTips.dll

OpenRegisteryKey

Software\Microsoft\Windows\CurrentVersion

SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink

SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0

SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback

Tahoma

Software\Microsoft\Windows\CurrentVersion\Internet Settings

Software\Microsoft\Windows\CurrentVersion\Uninstall\360

Software\Policies\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_INTERNET_SHELL_FOLDERS

Software\Microsoft\Windows\CurrentVersion\Uninstall\QQPCMgr

Software\Microsoft\Windows\CurrentVersion\Uninstall\NSIS

Software\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark

CreateMutex

<NULL>

OpenMutex

Local\MSCTF.Asm.MutexDefault1

DefaultTabtip-MainUI

CreateProcess

QueryFilePath

C:\sample

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp\DialogEx.dll

C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\GdiPlus.DLL

C:\Windows\syswow64\MSCTF.dll

C:\Windows\syswow64\USER32.dll

C:\Windows\SysWOW64\ieframe.dll

C:\Windows\system32\propsys.dll

C:\Windows\system32\RichEd20.DLL

DeleteFile

C:\Users\win7\AppData\Local\Temp\nsuD1A.tmp

C:\Users\win7\AppData\Local\Temp\nsoD4A.tmp

C:\Users\win7\AppData\Roaming\azbconfig.ini

C:\Users\win7\AppData\Roaming\kp2configuration.ini

Advance Heuristics

DETECTOR	RESULT

Human Expert Analysis Results

Analysis Start Date: 2016-04-20 17:36:16 UTC

Analysis End Date: 2016-04-20 18:50:41 UTC

File Upload Date: 2016-04-20 17:13:44 UTC

Human Expert Analyst Feedback:

Verdict: Malware

Additional File Information

Vendor Validation - Not Verified ✖

[+] Shanghai kuaiping Network Technology Co., Ltd

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] Shanghai kuaiping Network Technology Co., Ltd

Status	NoError ✔
Start Date	2015-03-04 00:00:00+00:00
End Date	2017-03-03 23:59:59+00:00
Sha256	f0ef3a8768942ded69b716cbd9fb2913c31bf906455feacee3bfb36f61dcaedb
Serial	5C3D0D443E6A7108A14844B5FCFEF28A
Subject Key Identifier	c9 c1 b7 c7 03 e9 89 d1 e6 8b c3 f4 7c 1c 87 9b c3 95 9b e3
Issuer Name	VeriSign Class 3 Code Signing 2010 CA
Issuer Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Crl link	http://sf.symcb.com/sf.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] VeriSign Class 3 Code Signing 2010 CA

Status	NoError ✔
Start Date	2010-02-08 00:00:00+00:00
End Date	2020-02-07 23:59:59+00:00
Sha256	0f5cd6ebab15fa367e35893fad2bc49cd1a95449f58e7eb978d72bb0b100d764
Serial	5200E5AA2556FC1A86ED96C9D44B33C7
Subject Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Crl link	http://crl.verisign.com/pca3-g5.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

[+] VeriSign Class 3 Public Primary Certification Authority - G5

Status	NoError ✔
Start Date	2006-11-08 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] Symantec Time Stamping Services CA - G2

Status	NoError ✔
Start Date	2012-12-21 00:00:00+00:00
End Date	2020-12-30 23:59:59+00:00
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

[+] Thawte Timestamping CA

Status	NoError ✔
Start Date	1997-01-01 00:00:00+00:00
End Date	2020-12-31 23:59:59+00:00
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	undefined
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Number Of Sections	5
Compilation Time Stamp	0x5336956B [Sat Mar 29 09:42:03 2014 UTC]
LegalCopyright	Copyright (C) 2015□□□□
InternalName	${Name}
FileVersion	V1.0
CompanyName	□□□□□□□□□□
LegalTrademarks	□□□□
ProductName	□□□□
ProductVersion	1.0.0.0
FileDescription	□□□□□□□□
Translation	0x0804 0x03a8
Entry Point	0x403dd3 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	4048752
Sha256	d425437f345d570173aa30cbc6d62233612adc139949e3043c90da4dd0967de6
Mime Type	application/x-dosexec

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\Users\salims\Desktop\Malware\ThisMayBeMalware11.exe	6

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY
.text	0x1000	0x714f	0x7200	6.492320
.rdata	0x9000	0x1198	0x1200	5.241732
.data	0xb000	0x1afbc	0x400	4.804006
.ndata	0x26000	0x2b000	0x0	0.000000[SUSPICIOUS]
.rsrc	0x51000	0x6a98	0x6c00	4.006433

PE Imports

- KERNEL32.dll
  - GlobalLock
  - GlobalAlloc
  - CloseHandle
  - SetFileTime
  - CompareFileTime
  - SearchPathA
  - GetShortPathNameA
  - GetFullPathNameA
  - MoveFileA
  - SetCurrentDirectoryA
  - GetFileAttributesA
  - GetLastError
  - CreateDirectoryA
  - SetFileAttributesA

- Sleep
- GetTickCount
- CreateFileA
- GetFileSize
- GetModuleFileNameA
- GetCurrentProcess
- CopyFileA
- GlobalUnlock
- GetWindowsDirectoryA
- GetTempPathA
- GetCommandLineA
- SetErrorMode
- lstrcpyA
- lstrcpynA
- lstrcatA
- LoadLibraryA
- lstrlenA
- WideCharToMultiByte
- VirtualAlloc
- VirtualProtect
- GetDiskFreeSpaceA
- CreateThread
- CreateProcessA
- RemoveDirectoryA
- GetTempFileNameA
- GetSystemDirectoryA
- GetVersion
- lstrcmpiA
- lstrcmpA
- ExpandEnvironmentStringsA
- GlobalFree
- WaitForSingleObject
- GetExitCodeProcess
- GetModuleHandleA
- LoadLibraryExA
- GetProcAddress
- FreeLibrary
- MulDiv
- MultiByteToWideChar
- WritePrivateProfileStringA
- GetPrivateProfileStringA
- WriteFile
- ReadFile
- SetFilePointer
- FindClose
- FindNextFileA
- FindFirstFileA
- DeleteFileA
- GlobalSize
- ExitProcess

USER32.dll

- SetClassLongA
- IsWindowEnabled
- GetSysColor
- GetWindowLongA
- SetCursor
- LoadCursorA
- CheckDlgButton
- GetMessagePos

- LoadBitmapA
- CallWindowProcA
- IsWindowVisible
- CloseClipboard
- SetClipboardData
- EmptyClipboard
- OpenClipboard
- TrackPopupMenu
- GetSystemMenu
- CreatePopupMenu
- GetSystemMetrics
- SetDlgItemTextA
- GetDlgItemTextA
- MessageBoxIndirectA
- CharPrevA
- DispatchMessageA
- PeekMessageA
- RegisterClassA
- DialogBoxParamA
- CharNextA
- ExitWindowsEx
- DestroyWindow
- CreateDialogParamA
- SetTimer
- SetWindowTextA
- EnableMenuItem
- GetWindowRect
- ScreenToClient
- SetWindowPos
- EndDialog
- AppendMenuA
- GetClassInfoA
- PostQuitMessage
- SetForegroundWindow
- ShowWindow
- wsprintfA
- FindWindowExA
- IsWindow
- GetDlgItem
- SetWindowLongA
- GetClientRect
- LoadImageA
- GetDC
- EnableWindow
- InvalidateRect
- SendMessageA
- SendMessageTimeoutA

GDI32.dll

- SetBkMode
- SetBkColor
- CreateBrushIndirect
- DeleteObject
- GetDeviceCaps
- SetTextColor
- CreateFontIndirectA

SHELL32.dll

- SHGetPathFromIDListA
- SHBrowseForFolderA
- SHGetFileInfoA

- ShellExecuteA
- SHFileOperationA
- SHGetSpecialFolderLocation

ADVAPI32.dll
- RegSetValueExA
- RegCreateKeyExA
- RegQueryValueExA
- RegEnumKeyA
- RegOpenKeyExA
- RegDeleteKeyA
- RegDeleteValueA
- RegEnumValueA
- RegCloseKey

COMCTL32.dll
- ImageList_AddMasked
- ImageList_Destroy
- None
- ImageList_Create

ole32.dll
- CLSIDFromString
- OleInitialize
- OleUninitialize
- CoTaskMemFree
- StringFromGUID2
- CoCreateInstance

VERSION.dll
- GetFileVersionInfoA
- VerQueryValueA
- GetFileVersionInfoSizeA

PE Resources

- RT_ICON
- RT_DIALOG
- RT_GROUP_ICON
- RT_VERSION
- RT_MANIFEST