VALKYRIE COMODO

Summary

File Name: virussign.com_84b52eae25f93c81a8d68ee488540b71.exe

File Type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed

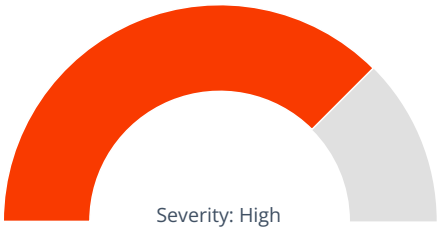
SHA1: e54f2ef6cad12f328d386d823ec63bd352097243

MD5: 84b52eae25f93c81a8d68ee488540b71

MALWARE

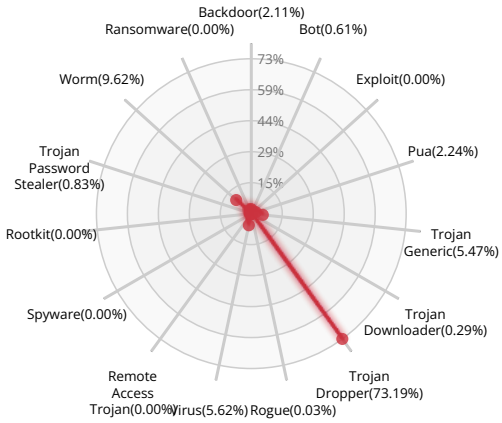
Valkyrie Final Verdict

DETECTION SECTION

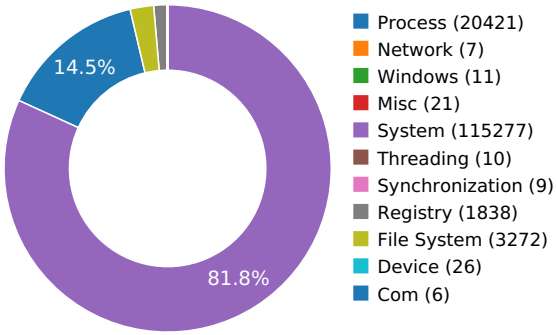


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes	Show sources
Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (1 unique times)	Show sources

PACKER

The executable is compressed using UPX	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Attempts to modify Explorer settings to prevent hidden files from being displayed	Show sources
Creates a hidden or system file	Show sources

VALKYRIE COMODO

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\e54f2ef6cad12f328d386d823ec63bd352097243.exe.cfg
C:\Windows\sysnative\C_932.NLS
C:\Windows\sysnative\C_949.NLS
C:\Windows\System32\tzres.dll
C:\Windows\sysnative\C_950.NLS
C:\Windows\sysnative\C_936.NLS
C:\Program Files\Common Files\System\symsrv.dll
C:\Users\user\AppData\Local\Temp\A1D26E2
C:\Users\user\AppData\Local\Temp\e54f2ef6cad12f328d386d823ec63bd352097243.exe
C:\Users\user\maeni.exe
\??\MountPointManager
\Device\Afd\AsyncSelectHlp
C:\Program Files\Common Files\System\symsrv.dll.dat
C:\Users\user\maeni.exe.cfg
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\KERNELBASE.dll
C:\Windows\System32\msvbvm60.dll
C:\Windows\SysWOW64\user32.dll
C:\Windows\SysWOW64\gdi32.dll
C:\Windows\SysWOW64\lpk.dll
C:\Windows\SysWOW64\usp10.dll
C:\Windows\SysWOW64\msvcrt.dll
C:\Windows\SysWOW64\advapi32.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\SysWOW64\rpcrt4.dll
C:\Windows\SysWOW64\sspicli.dll
C:\Windows\SysWOW64\CRYPTBASE.dll
C:\Windows\SysWOW64\ole32.dll
C:\Windows\SysWOW64\oleaut32.dll
C:\Windows\System32\imm32.dll

C:\Windows\SysWOW64\msctf.dll
C:\Windows\System32\api-ms-win-core-synch-l1-2-0.DLL
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\sxs.dll
C:\Windows\SysWOW64\clbcatq.dll
C:\Windows\System32\dwmapi.dll
C:\Windows\SysWOW64\wintrust.dll
C:\Windows\SysWOW64\crypt32.dll
C:\Windows\SysWOW64\msasn1.dll
C:\Windows\System32\ws2help.dll
C:\Windows\SysWOW64\ws2_32.dll
C:\Windows\SysWOW64\nsi.dll
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\shlwapi.dll
C:\Windows\System32\profapi.dll
C:\Windows\System32\propsys.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\System32\ntmarta.dll
C:\Windows\SysWOW64\Wldap32.dll
C:\Windows\SysWOW64\setupapi.dll
C:\Windows\SysWOW64\cfgmgr32.dll
C:\Windows\SysWOW64\devobj.dll
C:\Windows\System32\apphelp.dll
C:\Windows\System32\shdocvw.dll
C:\Windows\SysWOW64\urlmon.dll
C:\Windows\SysWOW64\wininet.dll
C:\Windows\SysWOW64\iertutil.dll
C:\Windows\System32\nlaapi.dll
C:\Windows\System32\NapiNSP.dll
C:\Windows\System32\pnrpnsp.dll
C:\Windows\System32\mswsock.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\winrnr.dll
C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\Com+Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaxSxSHashCount
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs

MODIFIED FILES

C:\Users\user\maeni.exe
\Device\Afd\AsyncSelectHlp

RESOLVED APIS

cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
kernel32.dll.OpenProcess
kernel32.dll.TerminateProcess
kernel32.dll.WriteProcessMemory
kernel32.dll.VirtualAllocEx
user32.dll.IsProcessDPIAware
oleaut32.dll.OleLoadPictureEx
oleaut32.dll.DispCallFunc

oleaut32.dll.LoadTypeLibEx
oleaut32.dll.UnRegisterTypeLib
oleaut32.dll.CreateTypeLib2
oleaut32.dll.VarDateFromUdate
oleaut32.dll.VarUdateFromDate
oleaut32.dll.GetAltMonthNames
oleaut32.dll.VarNumFromParseNum
oleaut32.dll.VarParseNumFromStr
oleaut32.dll.VarDecFromR4
oleaut32.dll.VarDecFromR8
oleaut32.dll.VarDecFromDate
oleaut32.dll.VarDecFromI4
oleaut32.dll.VarDecFromCy
oleaut32.dll.VarR4FromDec
oleaut32.dll.GetRecordInfoFromTypeInfo
oleaut32.dll.GetRecordInfoFromGuids
oleaut32.dll.SafeArrayGetRecordInfo
oleaut32.dll.SafeArraySetRecordInfo
oleaut32.dll.SafeArrayGetIID
oleaut32.dll.SafeArraySetIID
oleaut32.dll.SafeArrayCopyData
oleaut32.dll.SafeArrayAllocDescriptorEx
oleaut32.dll.SafeArrayCreateEx
oleaut32.dll.VarFormat
oleaut32.dll.VarFormatDateTime
oleaut32.dll.VarFormatNumber
oleaut32.dll.VarFormatPercent
oleaut32.dll.VarFormatCurrency
oleaut32.dll.VarWeekdayName
oleaut32.dll.VarMonthName
oleaut32.dll.VarAdd
oleaut32.dll.VarAnd
oleaut32.dll.VarCat
oleaut32.dll.VarDiv
oleaut32.dll.VarEqv

oleaut32.dll.VarIdiv
oleaut32.dll.VarImp
oleaut32.dll.VarMod
oleaut32.dll.VarMul
oleaut32.dll.VarOr
oleaut32.dll.VarPow
oleaut32.dll.VarSub
oleaut32.dll.VarXor
oleaut32.dll.VarAbs
oleaut32.dll.VarFix
oleaut32.dll.VarInt
oleaut32.dll.VarNeg
oleaut32.dll.VarNot
oleaut32.dll.VarRound
oleaut32.dll.VarCmp
oleaut32.dll.VarDecAdd
oleaut32.dll.VarDecCmp
oleaut32.dll.VarBstrCat
oleaut32.dll.VarCyMull4
oleaut32.dll.VarBstrCmp
ole32.dll.CoCreateInstanceEx
ole32.dll.CLSIDFromProgIDEx
sxs.dll.SxsOleAut32MapIIDOrCLSIDToTypeLibrary
user32.dll.GetSystemMetrics
user32.dll.MonitorFromWindow
user32.dll.MonitorFromRect
user32.dll.MonitorFromPoint
user32.dll.EnumDisplayMonitors
user32.dll.GetMonitorInfoA
advapi32.dll.AdjustTokenPrivileges
user32.dll.MessageBoxTimeoutW
wintrust.dll.WinVerifyTrust

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors
HKEY_CURRENT_USER\Software\Classes
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\Com+Enabled
HKEY_CURRENT_USER\Software\Classes\CLSID\{776CFA8D-A102-456E-8525-078CAFCB99A6}
HKEY_LOCAL_MACHINE\Software\Microsoft\OLE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaxSxSHashCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\e54f2ef6cad12f328d386d823ec63bd352097243.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\windows
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\maeni
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden

READ FILES

\Device\KsecDD
C:\Windows\System32\tzres.dll
C:\Program Files\Common Files\System\symsrv.dll
C:\Users\user\AppData\Local\Temp\e54f2ef6cad12f328d386d823ec63bd352097243.exe
\Device\Afd\AsyncSelectHlp
C:\Users\user\maeni.exe
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\KERNELBASE.dll
C:\Windows\System32\msvbvm60.dll
C:\Windows\SysWOW64\user32.dll
C:\Windows\SysWOW64\gdi32.dll
C:\Windows\SysWOW64\lpk.dll
C:\Windows\SysWOW64\usp10.dll
C:\Windows\SysWOW64\msvcrt.dll
C:\Windows\SysWOW64\advapi32.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\SysWOW64\rpcrt4.dll
C:\Windows\SysWOW64\sspicli.dll
C:\Windows\SysWOW64\CRYPTBASE.dll
C:\Windows\SysWOW64\ole32.dll
C:\Windows\SysWOW64\oleaut32.dll
C:\Windows\System32\imm32.dll
C:\Windows\SysWOW64\msctf.dll
C:\Windows\System32\api-ms-win-core-synch-l1-2-0.DLL
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\sxs.dll
C:\Windows\SysWOW64\clbcatq.dll
C:\Windows\System32\dwmapi.dll
C:\Windows\SysWOW64\wintrust.dll
C:\Windows\SysWOW64\crypt32.dll
C:\Windows\SysWOW64\msasn1.dll

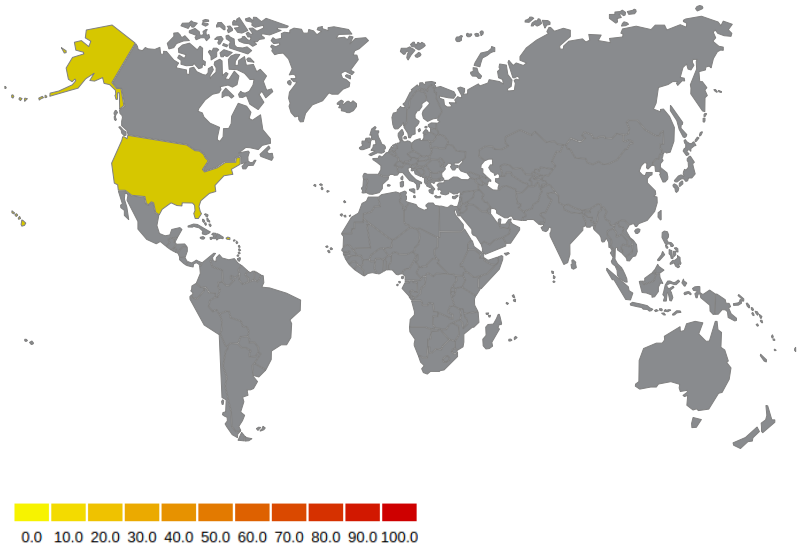
C:\Windows\System32\ws2help.dll
C:\Windows\SysWOW64\ws2_32.dll
C:\Windows\SysWOW64\nsi.dll
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\shlwapi.dll
C:\Windows\System32\profapi.dll
C:\Windows\System32\propsys.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\System32\ntmarta.dll
C:\Windows\SysWOW64\Wldap32.dll
C:\Windows\SysWOW64\setupapi.dll
C:\Windows\SysWOW64\cfgmgr32.dll
C:\Windows\SysWOW64\devobj.dll
C:\Windows\System32\apphelp.dll
C:\Windows\System32\shdocvw.dll
C:\Windows\SysWOW64\urlmon.dll
C:\Windows\SysWOW64\wininet.dll
C:\Windows\SysWOW64\iertutil.dll
C:\Windows\System32\nlaapi.dll
C:\Windows\System32\NapiNSP.dll
C:\Windows\System32\pnrpnsp.dll
C:\Windows\System32\mswsock.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\winrnr.dll
C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll

MODIFIED REGISTRY KEYS

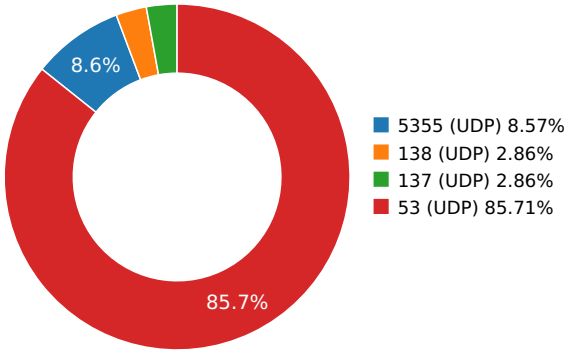
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\maeni
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
www.aieov.com	45.56.79.23	United States	63949	Akamai Technologies, Inc.	Malware Process
					Malware Process
					Malware Process
					Malware Process

DNS QUERIES

Request	Type
5isohu.com	A
ns1.codeconline.biz	A
www.aieov.com	A
ns1.player1523.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.01024389267	Sandbox	224.0.0.252	5355
7.010627985	Sandbox	224.0.0.252	5355
7.07506203651	Sandbox	192.168.56.255	137
9.55958795547	Sandbox	224.0.0.252	5355
10.2320549488	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
11.2306900024	Sandbox	8.8.8.8	53
12.7955629826	Sandbox	8.8.4.4	53
13.0750091076	Sandbox	192.168.56.255	138
13.7933199406	Sandbox	8.8.8.8	53
24.5907409191	Sandbox	8.8.8.8	53
24.7951419353	Sandbox	8.8.8.8	53
25.5901401043	Sandbox	8.8.4.4	53
25.79362607	Sandbox	8.8.4.4	53
38.950097084	Sandbox	8.8.8.8	53
39.9500200748	Sandbox	8.8.4.4	53
57.2008080482	Sandbox	8.8.8.8	53
58.2000210285	Sandbox	8.8.4.4	53
71.5596499443	Sandbox	8.8.8.8	53
72.5589299202	Sandbox	8.8.4.4	53
85.9189040661	Sandbox	8.8.8.8	53
86.918902874	Sandbox	8.8.4.4	53
104.168809891	Sandbox	8.8.8.8	53
105.168941975	Sandbox	8.8.4.4	53
118.528181076	Sandbox	8.8.8.8	53
119.527932882	Sandbox	8.8.4.4	53
132.888271093	Sandbox	8.8.8.8	53
133.887125015	Sandbox	8.8.4.4	53
151.13805294	Sandbox	8.8.8.8	53
152.140145063	Sandbox	8.8.4.4	53
165.497370005	Sandbox	8.8.8.8	53
166.496584892	Sandbox	8.8.4.4	53
179.856295109	Sandbox	8.8.8.8	53
180.85623908	Sandbox	8.8.4.4	53
198.107492924	Sandbox	8.8.8.8	53
199.106201887	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\Maeni.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed **MD5 :** aa737ec5d8e5b2089fdcbc3a737c51c7 **SHA-1 :** 10c8d025668a86ee9604864cec9530363151408a **SHA-256 :** 585847b060d186c1b6a840304f2dd78abcc1763b **SHA-512 :** f395de497a3b00e0506461a89ee60fba61b0b31(**Size :** 209.408 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	virussign.com_84b52eae25f93c81a8d68ee488540b71.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
SHA1:	e54f2ef6cad12f328d386d823ec63bd352097243
MD5:	84b52eae25f93c81a8d68ee488540b71
First Seen Date:	2024-09-03 22:49:25.644122 (5 days ago)
Number Of Clients Seen:	2
Last Analysis Date:	2024-09-03 22:49:25.644122 (5 days 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	4
Trid	[[64.2, u'UPX compressed Win32 Executable'], [15.6, u'Win32 Dynamic Link Library (generic)'], [10.6, u'Win32 Executable (generic)'], [4.7, u'Generic Win/DOS Executable'], [4.7, u'DOS Executable Generic']]
Compilation Time Stamp	0x4C7CC2B0 [Tue Aug 31 08:52:00 2010 UTC]
Translation	0x0409 0x04b0
FileVersion	2.99
ProductVersion	2.99
Entry Point	0x4011d4 (UPX0)
Machine Type	Intel 386 or later - 32Bit
File Size	209408
Ssdeep	768:LlvMa7aJJhzqmsswbjMPkG1VuW/wqvRXMXp677yCzdXZRT2Nq1MaQnepMri14PGV:LRl+JJtqJxlGVs4emEFb3P0lp
Sha256	58b99f278f964f480c46e0df39d69626ee87616f5e76ae774138a98973e11b6f
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/e/5/4/f/e54f2ef6cad12f328d386d823ec63bd352097243', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:09:03 22:49:16+00:00', u'EXE:InitializedDataSize': 4096, u'EXE:rsion': 2.99, u'File:FileModifyDate': u'2024:09:03 22:48:42+00:00', u'EXE:FileVersionNumber': u'1.0.0.0', u'File:FileSize': u'204 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 229376, u'File:FileName': u'e54f2ef6cad12f328d386d823ec63bd352097243', u'EXE:ImageVersion': 1.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2010:08:31 08:52:00+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LinkerVersion': 6.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/e/5/4/f', u'EXE:EntryPoint': u'0x11d4', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 32768, u'File:FileInodeChangeDate': u'2024:09:03 22:49:08+00:00', u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	612bcbdddb651d0c9e65f586426fc6d6

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x38000	0x2ae00	5.21608347473	7ef55dc034a2dcd0fac5b18a4f8f13d8
UPX1	0x39000	0x8000	0x7400	1.79128406688	ad2c1b24aaba7addb62dd4011d57471a
.rsrc	0x41000	0x1000	0xa00	2.90090073538	d278e5ff942a05c3f591bf9dadb35da4
.imports	0x42000	0x1000	0x200	1.98713718186	2810103ec56f703e2c17598dc1615ffa

PE Imports

- MSVBVM60.DLL
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - MethCallEngine
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - EVENT_SINK_AddRef
  - None
  - None
  - None
  - EVENT_SINK_Release
  - EVENT_SINK_QueryInterface
  - __vbaExceptHandler
  - None
  - None
  - None
  - None
  - None
  - ProcCallEngine
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 266572, u'sha256': u'2d3915cdc82e909357d44c4de1b8890bd753605c28df11b10299e3fd09d930b9', u'type': u'data', u'size': 304}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 266880, u'sha256': u'a32e750bc1b0315530097434a7e1d324b843e1f5ffd95238b49d3a8aa8e6fe09', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 267628, u'sha256': u'46dc088910439dad6a0d69da5e64227d04a640845fd1c31e90a7d4340c539fe0', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 267928, u'sha256': u'cbdcb84268fcf2a25b844c1dca787de835c0376e82c1a2e62814a3c940a26cfb', u'type': u'MS Windows icon resource - 3 icons, 32x32, 2 colors', u'size': 48}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 267980, u'sha256': u'e0bb4bf7d16ceec473db0100c7f42dda7cd5fe5ae85dd5921bc690dd0c852d7b', u'type': u'data', u'size': 460}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS