VALKYRIE COMODO

Summary

File Name: fn1o2ifn1f21n2of1no12oj2b4o3h3jhwdvssdfosdfk.exe

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

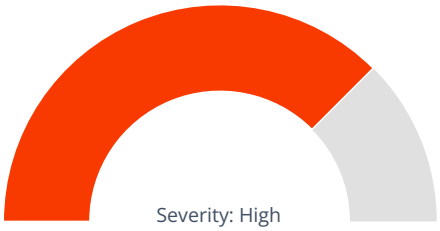
SHA1: acbbb49f6ed2e281f81cc82240a0c954f178d6a1

MD5: 0066f7a96a58509de0dc17c82403b7e4

MALWARE

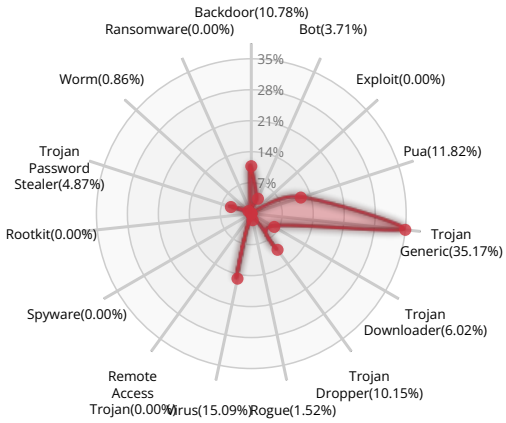
Valkyrie Final Verdict

DETECTION SECTION

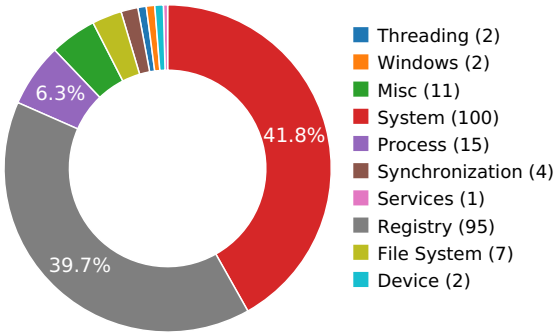


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

The executable is likely packed with VMProtect Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\acbbb49f6ed2e281f81cc82240a0c954f178d6a1.exe
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

RESOLVED APIS

gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
dwmapi.dll.DwmIsCompositionEnabled
gdi32.dll.GdiIsMetaPrintDC
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
cryptbase.dll.SystemFunction036
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
oleaut32.dll.#500

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\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
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_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
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\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\acbbb49f6ed2e281f81cc82240a0c954f178d6a1.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

READ FILES

C:\Users\user\AppData\Local\Temp\acbbb49f6ed2e281f81cc82240a0c954f178d6a1.exe

C:\Windows\Fonts\staticcache.dat

\Device\KsecDD

C:\Windows\Globalization\Sorting\sortdefault.nls

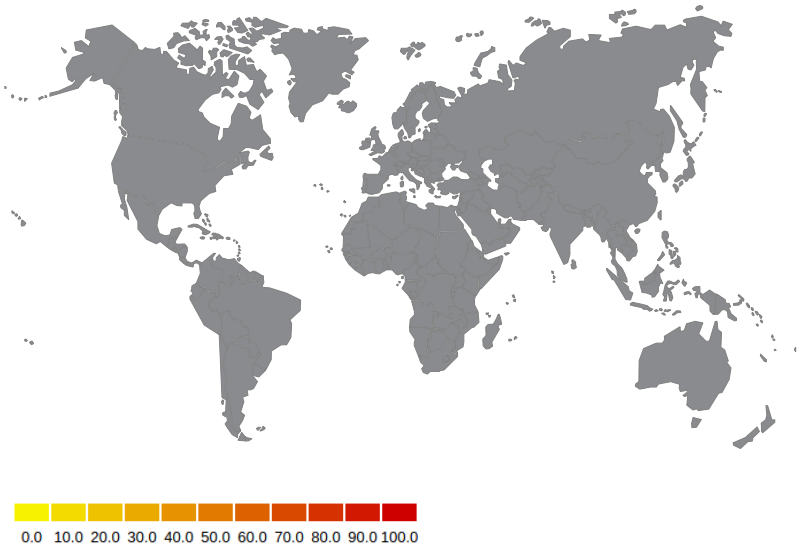
MUTEXES

CicLoadWinStaWinSta0

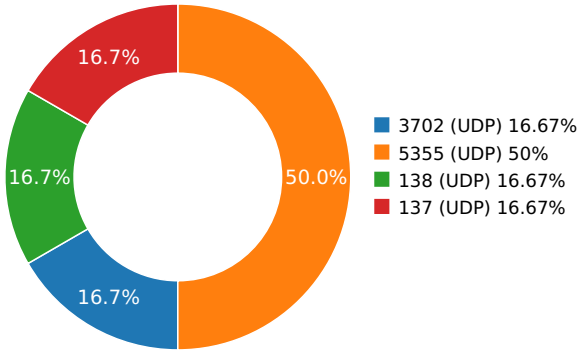
Local\MSCTF.CtfMonitorInstMutexDefault1

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
3.15797376633	Sandbox	192.168.56.255	137
3.20056986809	Sandbox	224.0.0.252	5355
3.24838399887	Sandbox	224.0.0.252	5355
3.45443987846	Sandbox	239.255.255.250	3702
5.81248497963	Sandbox	224.0.0.252	5355
9.27876377106	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	fn1o2ifn1f21n2of1no12oj2b4o3h3jhwdvssdfosdfk.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
SHA1:	acbbb49f6ed2e281f81cc82240a0c954f178d6a1
MD5:	0066f7a96a58509de0dc17c82403b7e4
First Seen Date:	2018-06-02 10:15:46.763576 (6 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2018-06-02 10:15:46.763576 (6 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	1
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	9
Trid	[]
Compilation Time Stamp	0x5B115E2D [Fri Jun 1 14:54:37 2018 UTC]
Entry Point	0x82a200 (.vmp1)
Machine Type	Intel 386 or later - 32Bit
File Size	3438592
Ssdeep	
Sha256	360d9204675c0317c6712c5d0ffd1f30651684a4fe59d0b64fa3ea225e4e928b
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x73be6	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x75000	0x1d4a2	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.data	0x93000	0x6234	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.gfids	0x9a000	0xcd4	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.tls	0x9b000	0x9	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.vmp0	0x9c000	0x2f9cb5	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.vmp1	0x396000	0x346de0	0x346e00	7.99428570594	2b317e5f396318768784ed8e2a887492
.reloc	0x6dd000	0x124	0x200	2.79850334772	95eadef518727849e8649fc39887f340
.rsrc	0x6de000	0x1d5	0x200	4.70732650868	70adc6d04f7c6f56e671d012613e68b1

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 7200856, u'sha256': u'4bb79dcea0a901f7d9eac5aa05728ae92acb42e0cb22e5dd14134f4421a3d8df', u'type': u'XML 1.0 document text', u'size': 381}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS