VALKYRIE COMODO

Summary

File Name: 4707625.exe

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

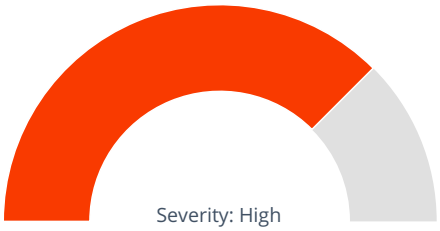
SHA1: 50c3ca4ae5ae505a73e69af2d995840504bf4fbc

MD5: b01a0e13dda4163924c8257cbad655b1

MALWARE

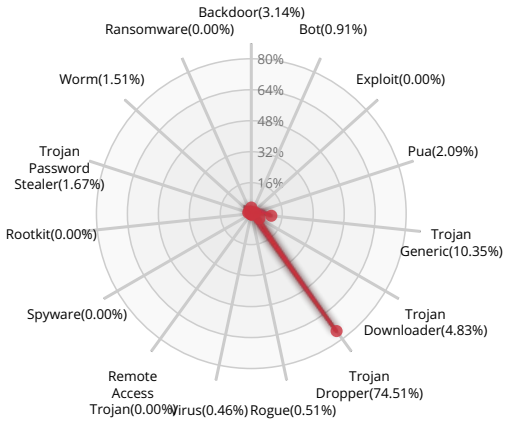
Valkyrie Final Verdict

DETECTION SECTION

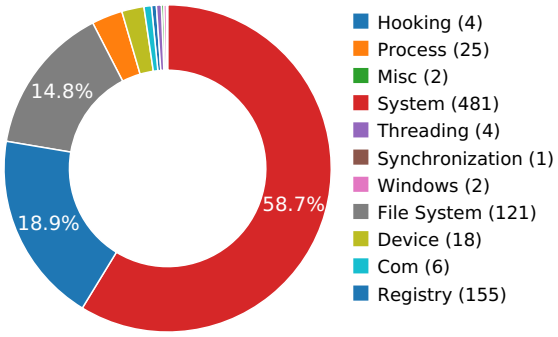


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup — Show sources

Creates a copy of itself — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time — Show sources

A process created a hidden window — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

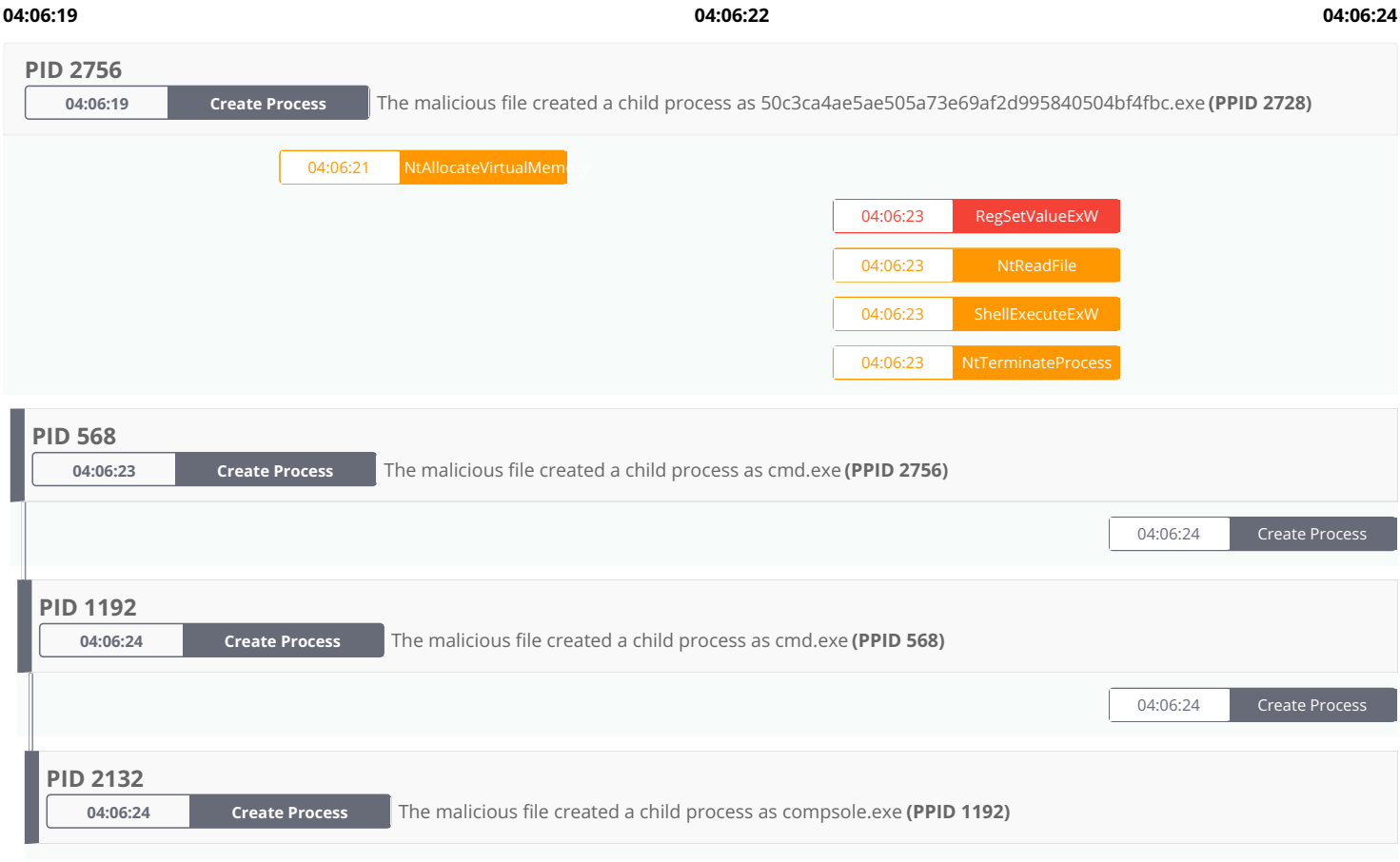
Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\a.Manifest
C:\Users\user\AppData\Local\Temp\50c3ca4ae5ae505a73e69af2d995840504bf4fbc.exe
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\sysnative\C_1252.NLS
C:\Windows\sysnative*.dll
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Comrprop
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Roaming\Microsoft\Comrprop\compsole.exe
C:\Users\user\AppData\Local\Temp\6384
C:\Users\user\AppData\Local\Temp\6384\B1A2.tmp
C:\Users\user\AppData\Local\Temp\6384\B1A2.bat
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\"C:\Users\user\AppData\Local\Temp\6384\B1A2.bat"
C:\Users\user\AppData\Local\Temp\cmd.*
C:\Users\user\AppData\Local\Temp\cmd
C:\ProgramData\Oracle\Java\javapath\cmd.*
C:\ProgramData\Oracle\Java\javapath\cmd
C:\Windows\System32\cmd.*
C:\Windows\System32\cmd.COM
C:\Windows\System32\cmd.exe
C:\Users\user\AppData\Local\Temp\"C:\Users\user\AppData\Roaming\MICROS~1\Comrprop\compsole.exe"

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\api-rans
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US

HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\FCF47A3A-2BCC-8E73-95F0-8FA2992433F6\Client
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\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\PathCompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

MODIFIED FILES

C:\Users\user\AppData\Roaming\Microsoft\Comrprop\compsole.exe
C:\Users\user\AppData\Local\Temp\6384\B1A2.bat

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue

kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.VirtualAlloc
ntdll.dll.ZwOpenProcessToken
ntdll.dll.ZwClose
ntdll.dll.mbstowcs
ntdll.dll.NtQuerySystemInformation
ntdll.dll.RtlNtStatusToDosError
ntdll.dll.memcpy
ntdll.dll.memset
ntdll.dll.ZwQueryInformationProcess
ntdll.dll.NtUnmapViewOfSection
ntdll.dll.NtMapViewOfSection
ntdll.dll.RtlUpcaseUnicodeString
ntdll.dll.NtCreateSection
ntdll.dll.ZwOpenProcess
ntdll.dll.ZwQueryInformationToken
ntdll.dll.RtlFreeUnicodeString
ntdll.dll.RtlUnwind
ntdll.dll.NtQueryVirtualMemory
shlwapi.dll.PathFindExtensionW
shlwapi.dll.StrRChrA
shlwapi.dll.PathFindExtensionA
shlwapi.dll.StrChrA
shlwapi.dll.PathCombineW
shlwapi.dll.PathFindFileNameW
shlwapi.dll.StrChrW
shlwapi.dll.StrTrimW
shlwapi.dll.PathFindFileNameA
kernel32.dll.CloseHandle
kernel32.dll.ResetEvent
kernel32.dll.LoadLibraryA
kernel32.dll.CreateWaitableTimerA
kernel32.dll.GetTickCount

kernel32.dll.SetFileAttributesW
kernel32.dll.CreateProcessA
kernel32.dll.SetEvent
kernel32.dll.CreateEventA
kernel32.dll.GetProcAddress
kernel32.dll.GetLastError
kernel32.dll.lstrcatW
kernel32.dll.Sleep
kernel32.dll.HeapFree
kernel32.dll.lstrcmpiW
kernel32.dll.lstrlenW
kernel32.dll.SetWaitableTimer
kernel32.dll.HeapAlloc
kernel32.dll.GetCommandLineW
kernel32.dll.ExitProcess
kernel32.dll.GetModuleHandleA
kernel32.dll.HeapCreate
kernel32.dll.HeapDestroy
kernel32.dll.WaitForSingleObject
kernel32.dll.DeleteFileW
kernel32.dll.VirtualProtectEx
kernel32.dll.ResumeThread
kernel32.dll.SuspendThread
kernel32.dll.lstrcmpA
kernel32.dll.GetTempFileNameA
kernel32.dll.CreateDirectoryA
kernel32.dll.GetTempPathA
kernel32.dll.GetFileSize
kernel32.dll.lstrcpynA
kernel32.dll.GetFileTime
kernel32.dll.FindNextFileA
kernel32.dll.CompareFileTime
kernel32.dll.GetLongPathNameW
kernel32.dll.OpenProcess

kernel32.dll.GetVersion
kernel32.dll.GetCurrentProcessId
kernel32.dll.CreateFileW
kernel32.dll.GetModuleFileNameA
kernel32.dll.lstrcatA

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\api-rans
HKEY_USERS\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData
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_CURRENT_USER\Software\AppDataLow\Software\Microsoft\FCF47A3A-2BCC-8E73-95F0-8FA2992433F6
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\FCF47A3A-2BCC-8E73-95F0-8FA2992433F6\Client
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\50c3ca4ae5ae505a73e69af2d995840504bf4fbc.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\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\PathCompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
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\System\CurrentControlSet\Control\SafeBoot\Option

EXECUTED COMMANDS

C:\Users\user\AppData\Local\Temp\6384\B1A2.bat "C:\Users\user\AppData\Roaming\MICROS~1\Comrprop\compsole.exe" "C:\Users\user\AppData\Local\Temp\50C3CA~1.EXE"
cmd /C ""C:\Users\user\AppData\Roaming\MICROS~1\Comrprop\compsole.exe" "C:\Users\user\AppData\Local\Temp\50C3CA~1.EXE""
"C:\Users\user\AppData\Roaming\MICROS~1\Comrprop\compsole.exe" "C:\Users\user\AppData\Local\Temp\50C3CA~1.EXE"

READ FILES

C:\Users\user\AppData\Local\Temp\a.Manifest
C:\Windows\sysnative\C_1252.NLS

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

C:\Users\user\AppData\Local\Temp\50c3ca4ae5ae505a73e69af2d995840504bf4fbc.exe

C:\Users\user\AppData\Roaming\Microsoft\Comrprop\compsole.exe

C:\Users\user\AppData\Local\Temp\6384\B1A2.tmp

C:\Users\user\AppData\Local\Temp\6384\B1A2.bat

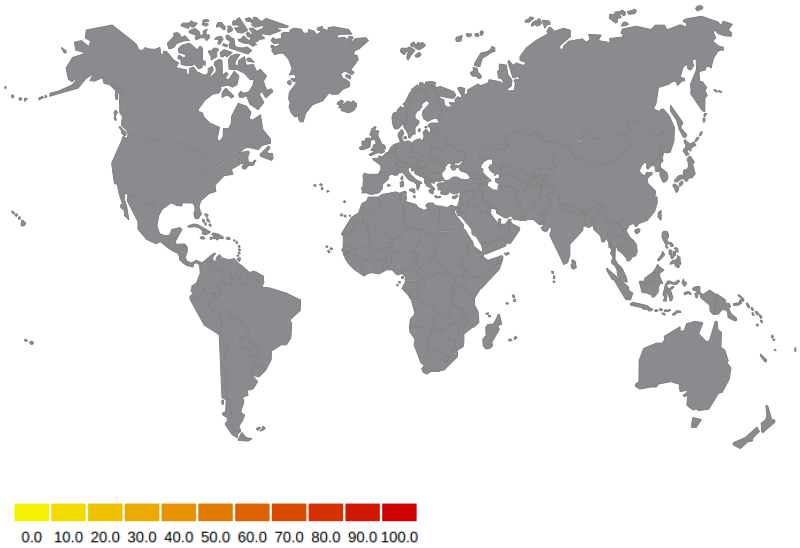
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\api-rans

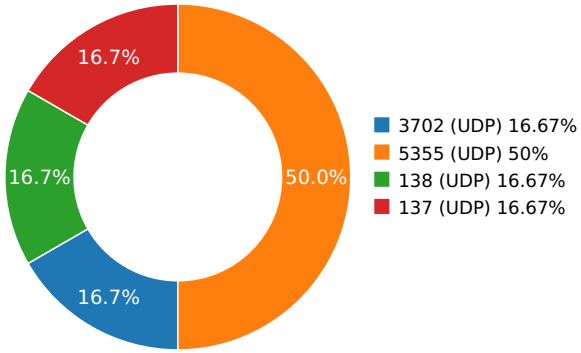
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\FCF47A3A-2BCC-8E73-95F0-8FA2992433F6

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
3.03584194183	Sandbox	224.0.0.252	5355
3.036921978	Sandbox	224.0.0.252	5355
3.04470181465	Sandbox	239.255.255.250	3702
3.07943701744	Sandbox	192.168.56.255	137
5.59502983093	Sandbox	224.0.0.252	5355
9.11040782928	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Microsoft\Comrprop\Compsole.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** b01a0e13dda4163924c8257cbad655b1 **SHA-1 :** 50c3ca4ae5ae505a73e69af2d995840504bf4fbc **SHA-256 :** e89e6447dfee57abfa2307bd3de516ed54008cf3 **SHA-512 :** 8f91b3d74993084958cb922368cf80fd69516dea **Size :** 484.944 Kilobytes.
C:\Users\User\AppData\Local\Temp\6384\B1A2.Bat	**Type :** ASCII text, with CRLF line terminators **MD5 :** 723c41903b3fee34562881f4f016a68a **SHA-1 :** bed4f1c2bfa3f1c7ab706ad3b1ebf33ba1245370 **SHA-256 :** 0bf4691b4af84ad8ed4e09b9ac92b9e8d1b306e7 **SHA-512 :** 947c1ccd30dee1b9039e37f5da378ba031cc5a7e **Size :** 0.11 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	4707625.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	50c3ca4ae5ae505a73e69af2d995840504bf4fbc
MD5:	b01a0e13dda4163924c8257cbad655b1
First Seen Date:	2017-08-18 21:38:24.748760 (2 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-08-18 21:38:24.748760 (2 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
File Type Enum	6
Number Of Sections	4
Compilation Time Stamp	0x5994BE38 [Wed Aug 16 21:50:48 2017 UTC]
Entry Point	0x405e72 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	484944
Sha256	e89e6447dfee57abfa2307bd3de516ed54008cf34f8274f19bb7f1ce07bfa4a6
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xe154	0xf000	6.36016288464	a87499a907509da7ecf9681ec16ebc77
.rdata	0x10000	0x61ac0	0x62000	6.16890265188	8a3b60737180de1430ab4fc8bc12caeb
.data	0x72000	0x26bd8	0x1000	3.7862541864	7e0ff4eba9c05974ba382ae3da6c71c3
.rsrc	0x99000	0x1900	0x2000	2.00574276664	8b2020bcf0b2338c833e57fcde82c11f

CERTIFICATE VALIDATION

- Success ✔

[+] AiTi Shag	
Status	NoError ✔
Start Date	2016-11-09 00:00:00+00:00
End Date	2017-11-09 23:59:59+00:00
Sha256	cbaaf89b44baad0ab9b6b66065f3567c622ca75d385df61fe8e20f44ac7da609
Serial	009B61AC54A45B31FE22EED5D6F90F95BF
Subject Key Identifier	21 a0 47 ad d5 af fc 28 f6 c8 40 60 0a dd 2c 07 c6 db ac 50
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Code Signing CA	
Status	NoError ✔
Start Date	2013-05-09 00:00:00+00:00
End Date	2028-05-08 23:59:59+00:00
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Certification Authority	
Status	NoError ✔
Start Date	2010-01-19 00:00:00+00:00
End Date	2038-01-18 23:59:59+00:00
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

SCREENSHOTS