VALKYRIE COMODO

Summary

File Name: None

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

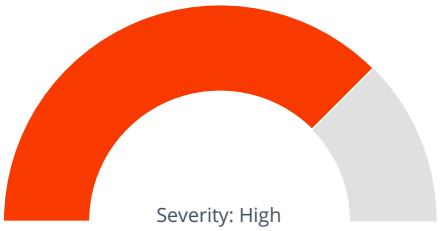
SHA1: 03fb39f1041f15d83cbf89a4b8cf9a32de5fa46b

MD5:

MALWARE

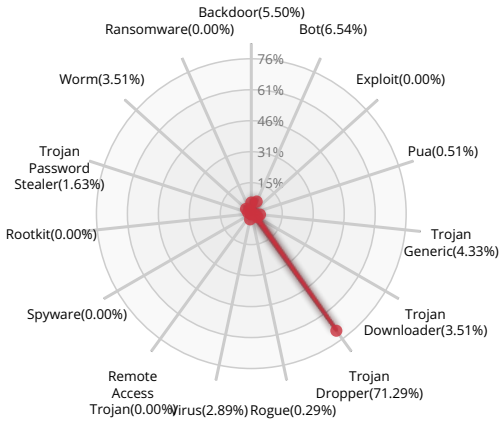
Valkyrie Final Verdict

DETECTION SECTION

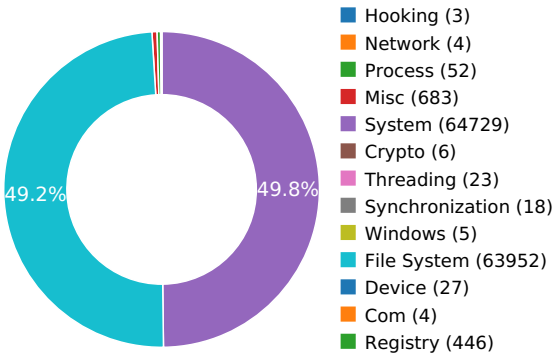


Verdict: Malware

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

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

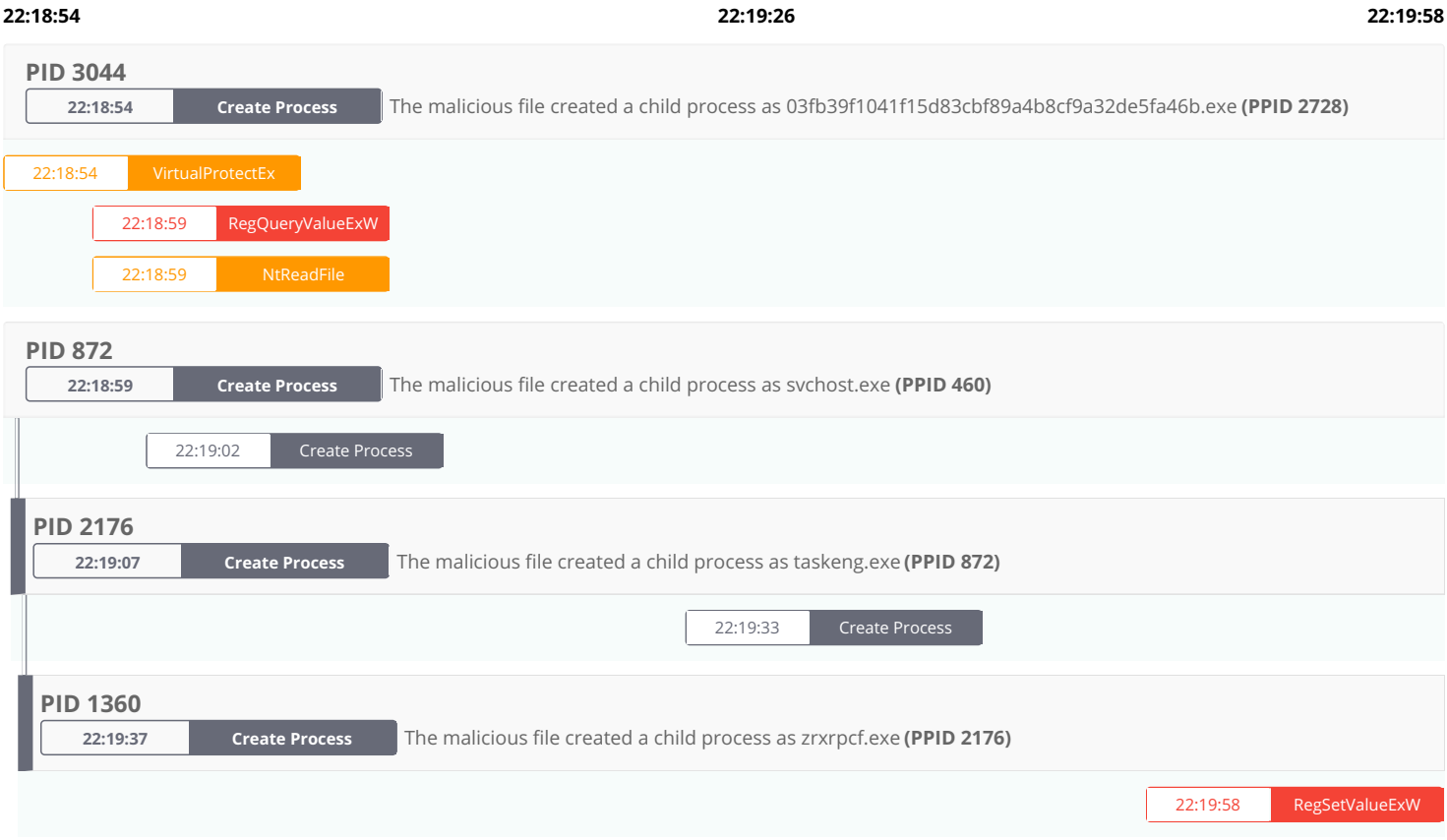
Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Roaming
C:\Windows\Fonts\staticcache.dat
C:\ProgramData\Mozilla\
C:\ProgramData
C:\Users\user\AppData\Local\Temp\03fb39f1041f15d83cbf89a4b8cf9a32de5fa46b.exe
C:\ProgramData\Mozilla\zrxrpcf.exe
\Device\KsecDD
C:\Windows\sysnative\Tasks
C:\Windows\sysnative\Tasks*
C:\Windows\sysnative\Tasks\GoogleUpdateTaskMachineCore
C:\Windows\Tasks\ofeqzyf.job
C:\Windows\sysnative\Tasks\ofeqzyf
C:\Windows\sysnative\Tasks\
\??\PIPE\srvsvc
C:\DosDevices\pipe\
\??\MountPointManager
C:\ProgramData\Mozilla
\Device\LanmanDatagramReceiver
C:\Windows\System32\config\systemprofile\AppData\Roaming
C:\ProgramData\Mozilla\iseokfl.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Shell Folders\Common AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\GoogleUpdateTaskMachineCore\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\SchedulingEngineKnob
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Control Panel\International\LocaleName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ofeqzyf\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\Triggers
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{BCF8DB88-253B-412B-A98E-C632FC2EDF02}\data
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\SecurityService\DefaultAuthLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\IpHlpSvc\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\IpHlpSvc\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\IpHlpSvc\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\IpHlpSvc\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\IpHlpSvc\MaxFileSize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\IpHlpSvc\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration\DataVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration\EnableBackCompat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration\MissedTasksStartupDelay
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration\TasksInMemoryQueue
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration\TasksPerHighestPrivEngine
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration\TasksPerLeastPrivEngine
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration\TracingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration\WindowSeconds
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\6BA0E3C1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\Com+Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaxSxSHashCount
HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName
HKEY_USERS\.DEFAULT\Control Panel\International\sCountry
HKEY_USERS\.DEFAULT\Control Panel\International\sList
HKEY_USERS\.DEFAULT\Control Panel\International\sDecimal
HKEY_USERS\.DEFAULT\Control Panel\International\sThousand
HKEY_USERS\.DEFAULT\Control Panel\International\sGrouping
HKEY_USERS\.DEFAULT\Control Panel\International\sNativeDigits
HKEY_USERS\.DEFAULT\Control Panel\International\sCurrency
HKEY_USERS\.DEFAULT\Control Panel\International\sMonDecimalSep
HKEY_USERS\.DEFAULT\Control Panel\International\sMonThousandSep
HKEY_USERS\.DEFAULT\Control Panel\International\sMonGrouping
HKEY_USERS\.DEFAULT\Control Panel\International\sPositiveSign
HKEY_USERS\.DEFAULT\Control Panel\International\sNegativeSign
HKEY_USERS\.DEFAULT\Control Panel\International\sTimeFormat

MODIFIED FILES

C:\ProgramData\Mozilla\zrxrpcf.exe
C:\Windows\sysnative\Tasks\ofeqzyf

\??\PIPE\srvsvc
\Device\LanmanDatagramReceiver
C:\ProgramData\Mozilla\iseokfl.dll

RESOLVED APIS

kernel32.dll.LoadLibraryA
kernel32.dll.GetProcAddress
kernel32.dll.VirtualAlloc
kernel32.dll.IsBadReadPtr
kernel32.dll.VirtualProtect
kernel32.dll.Sleep
kernel32.dll.UnmapViewOfFile
kernel32.dll.VirtualFree
kernel32.dll.GetModuleHandleA
kernel32.dll.ExitProcess
kernel32.dll.ReadFile
kernel32.dll.GetTickCount
kernel32.dll.MoveFileExW
kernel32.dll.HeapFree
kernel32.dll.GetVersion
kernel32.dll.GetTempPathW
kernel32.dll.DeleteFileW
kernel32.dll.GetProcessHeap
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetCurrentThreadId
kernel32.dll.CreateDirectoryW
kernel32.dll.GetShortPathNameW
kernel32.dll.GetCommandLineW
kernel32.dll.MultiByteToWideChar
kernel32.dll.HeapAlloc
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.HeapReAlloc
kernel32.dll.HeapSize
kernel32.dll.WideCharToMultiByte

kernel32.dll.RtlUnwind
kernel32.dll.IsValidCodePage
kernel32.dll.GetOEMCP
kernel32.dll.GetACP
kernel32.dll.GetCPInfo
kernel32.dll.LoadLibraryW
kernel32.dll.EnterCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.QueryPerformanceCounter
kernel32.dll.GetFileSize
kernel32.dll.GetModuleFileNameW
kernel32.dll.CloseHandle
kernel32.dll.WriteFile
kernel32.dll.LCMapStringW
kernel32.dll.CreateFileW
kernel32.dll.HeapCreate
kernel32.dll.InterlockedDecrement
kernel32.dll.GetLastError
kernel32.dll.SetLastError
kernel32.dll.GetStringTypeW
kernel32.dll.InterlockedIncrement
kernel32.dll.TlsFree
kernel32.dll.HeapSetInformation
kernel32.dll.GetStartupInfoW
kernel32.dll.TerminateProcess
kernel32.dll.GetCurrentProcess
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.SetUnhandledExceptionFilter
kernel32.dll.IsDebuggerPresent
kernel32.dll.GetModuleHandleW
kernel32.dll.GetStdHandle
kernel32.dll.FreeEnvironmentStringsW
kernel32.dll.GetEnvironmentStringsW
kernel32.dll.SetHandleCount
kernel32.dll.InitializeCriticalSectionAndSpinCount

kernel32.dll.GetFileType
kernel32.dll.DeleteCriticalSection
kernel32.dll.TlsAlloc
kernel32.dll.TlsGetValue
kernel32.dll.TlsSetValue
user32.dll.TranslateAcceleratorW
user32.dll.GetMessageW
user32.dll.LoadAcceleratorsW
user32.dll.LoadStringW
user32.dll.EndDialog
user32.dll.PostQuitMessage

DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\ofeqzyf.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\ofeqzyf.job.fp

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\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\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Shell Folders\Common AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\AppID\03fb39f1041f15d83cbf89a4b8cf9a32de5fa46b.exe
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SQMClient\Windows
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\GoogleUpdateTaskMachineCore
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\GoogleUpdateTaskMachineCore\Id
HKEY_LOCAL_MACHINE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\SchedulingEngineKnob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\ofeqzyf.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\ofeqzyf.job.fp
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Control Panel\International
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Control Panel\International\LocaleName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ofeqzyf
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\Path

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ofeqzyf\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ofeqzyf\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{BCF8DB88-253B-412B-A98E-C632FC2EDF02}
HKEY_LOCAL_MACHINE\system\Setup
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\RepositoryRestoreInProgress
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{BCF8DB88-253B-412B-A98E-C632FC2EDF02}\data
HKEY_LOCAL_MACHINE\Software\Classes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{92BDB7E4-F28B-46A0-B551-45A52BDD5125}\InprocServer32\InprocServer32

EXECUTED COMMANDS

taskeng.exe {BCF8DB88-253B-412B-A98E-C632FC2EDF02} S-1-5-18:NT AUTHORITY\System:Service:
C:\PROGRA~3\Mozilla\zrxrpcf.exe -jahdlji

READ FILES

C:\Users\user\AppData\Roaming
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\03fb39f1041f15d83cbf89a4b8cf9a32de5fa46b.exe
\Device\KsecDD
C:\Windows\sysnative\Tasks\ofeqzyf
\??\PIPE\srvsvc

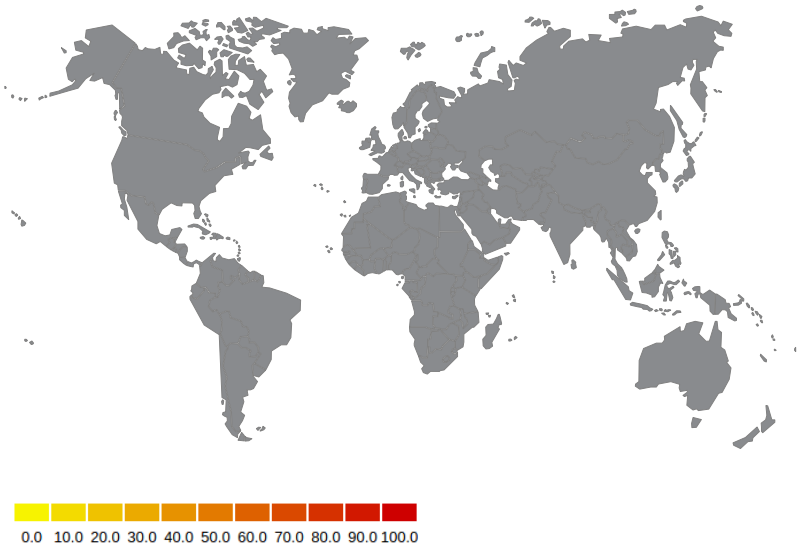
\Device\LanmanDatagramReceiver
C:\Windows\System32\config\systemprofile\AppData\Roaming

MODIFIED REGISTRY KEYS

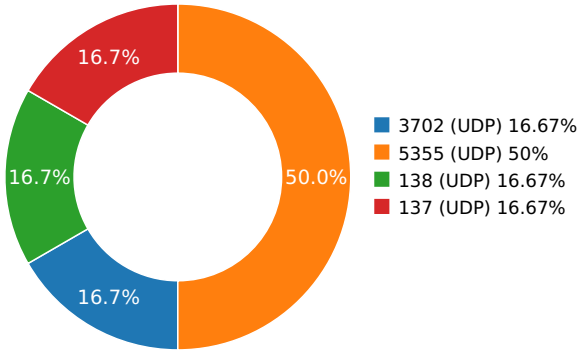
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ofeqzyf\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ofeqzyf\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{E86EC476-5926-4DA1-A47C-F8AA5158062A}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{BCF8DB88-253B-412B-A98E-C632FC2EDF02}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{BCF8DB88-253B-412B-A98E-C632FC2EDF02}\data
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs

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
6.98269200325	Sandbox	192.168.56.255	137
6.98376607895	Sandbox	224.0.0.252	5355
6.9880399704	Sandbox	224.0.0.252	5355
7.18265914917	Sandbox	239.255.255.250	3702
9.5493490696	Sandbox	224.0.0.252	5355
12.9699981213	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Windows\Sysnative\Tasks\Ofeqzyf	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** 89a486c854edcc858db9b4fe769889ec **SHA-1 :** 4a8f4e6c26c7974b46b6cf67aff1af85961072b8 **SHA-256 :** 9fc52ddd8d9659d2c7d3a9521cc974bcebd3aff0 **SHA-512 :** a0cd0d4fda050dcce3cd2a8940ab087f6a8791d9 **Size :** 2.9 Kilobytes.
C:\ProgramData\Mozilla\Iseokfl.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** bde67d29cc01c8e94049f4000d1fa291 **SHA-1 :** cd910a48d98b8f5f8f9d3b18250264089ee85247 **SHA-256 :** 8167e3e4a7508dfbcd597b899b8380fba32ec7bf **SHA-512 :** 98ffafe255c543fd2107a3fd1fd27d811ddbdd4e9 **Size :** 18.944 Kilobytes.
C:\ProgramData\Mozilla\Zrxrpcf.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** d4c08ec1171bdf0aef9d8903bd5e2be5 **SHA-1 :** bf819f43efdc2c4f47ddd1d964abf541dfa879aa **SHA-256 :** 85143e0c8600ee4a797543d978fbb164a712562 **SHA-512 :** 7ef08bdcba33d4f4769ad0b32eef8ad1f6d1dea7 **Size :** 145.688 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	None
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
SHA1:	03fb39f1041f15d83cbf89a4b8cf9a32de5fa46b
MD5:	
First Seen Date:	2018-09-02 18:58:05.634458 (6 months ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-09-02 18:58:05.634458 (6 months 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	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	7
Trid	[]
Compilation Time Stamp	0x51A91C3E [Fri May 31 21:55:10 2013 UTC]
Entry Point	0x401647 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	145680
Ssdeep	
Sha256	0b09de41b77ef668c0138c227acb7294ebd300b3bddd8665fd95b7b4425dfc60
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1160	0x1200	6.08471963758	5df29ef4014cd13406d892b205c03ce0
.data	0x3000	0x5b0d8	0x1d400	6.53067396528	a6070b68d2a270ea702fcffd94447c7a
.idata	0x5f000	0x488	0x600	3.78475195811	6e915acf27f6d03b88abd43a924f2c2b
.rsrc	0x60000	0x1240	0x1400	3.34660052156	e265afdc68c91bc154edea3a82ad7ed7
.reloc	0x62000	0x64	0x200	1.45728450764	c1e6949724aef8094f9532d053fb976f
.xdata	0x63000	0x12d	0x200	3.76452516876	430f35b3468d6743915788c3f73ded2a
.ydata	0x64000	0x8c	0x200	1.92697129093	6998051e696fc805169ccde40a437d07

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS