VALKYRIE COMODO

Summary

File Name: SystemDestroyer.bat

File Type: DOS batch file, ASCII text, with CRLF line terminators

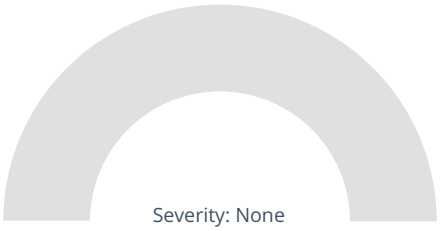
SHA1: 275a1a4cdae156036639a3a4113b128fb5279d13

MD5: 64262e14320cd5d5b1a24b0784faba74

CLEAN

Valkyrie Final Verdict

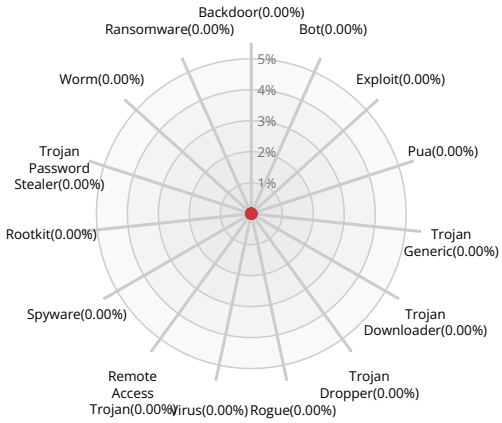
DETECTION SECTION



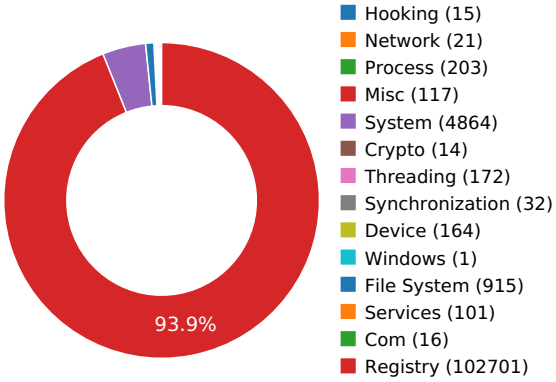
Severity: None

Verdict: Clean

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Loads a driver — Show sources

Attempts to repeatedly call a single API many times in order to delay analysis time — Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES
C:\Users\user\AppData\Local\Temp\275a1a4cdae156036639a3a4113b128fb5279d13
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\275a1a4cdae156036639a3a4113b128fb5279d13.*
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004b.db
C:\Users\user\Desktop\desktop.ini
C:\Windows\SysWOW64\propsys.dll
C:\Windows\sysnative\propsys.dll
C:\
C:\Users
C:\Users\desktop.ini
C:\Users\user
C:\Users\user\Searches
C:\Users\user\Searches\desktop.ini
C:\Users\user\Videos
C:\Users\user\Videos\desktop.ini
C:\Users\user\Pictures
C:\Users\user\Pictures\desktop.ini
C:\Users\user\Desktop
C:\Users\user\Contacts
C:\Users\user\Contacts\desktop.ini
C:\Users\user\Favorites
C:\Users\user\Favorites\desktop.ini
C:\Users\user\Music
C:\Users\user\Music\desktop.ini
C:\Users\user\Downloads
C:\Users\user\Downloads\desktop.ini
C:\Users\user\Documents
C:\Users\user\Documents\desktop.ini
C:\Users\user\Links
C:\Users\user\Links\desktop.ini

C:\Users\user\Saved Games
C:\Users\user\Saved Games\desktop.ini
C:\Windows\System32\shdocvw.dll
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\System32\
C:\Windows\SysWOW64\shdocvw.dll
C:\Windows
C:\Windows\System32
C:\Windows\System32*.*
\??\MountPointManager
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\275a1a4cdae156036639a3a4113b128fb5279d13:Zone.Identifier
C:\Windows\System32\rundll32.exe
C:\Windows\System32\shell32.dll
C:\Windows\SysWOW64\cmd.exe
C:\Windows\Temp
C:\Windows\sysnative\Tasks\Microsoft\Windows\WDI\ResolutionHost
C:\Windows\sysnative\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp
C:\Windows\ServiceProfiles
C:\Windows\ServiceProfiles\NetworkService
\??\PIPE\srvsvc
C:\Windows\sysnative\LogFiles\Scm\044a6734-e90e-4f8f-b357-b2dc8ab3b5ec
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp
C:\Windows\ServiceProfiles\LocalService
C:\Windows\sysnative\Tasks\Microsoft\Windows\Time Synchronization\SynchronizeTime
C:\Windows\sysnative\LogFiles\Scm\a7c73732-9f11-4281-8d19-764d4ec9d94d
C:\Windows\sysnative\LogFiles\Scm\be669c13-8165-4536-96d0-6d6c39292aae
C:\Windows\sysnative\LogFiles\Scm\ca4b8ff2-a4d2-4d88-a52e-3a5bdaf7f56e
C:\Windows\sysnative\LogFiles\Scm\fb3c354d-297a-4eb2-9b58-090f6361906b
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ndpsetup.bat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenservicelock.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenrootstorelock.dat

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvc.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen_service.log
C:\Windows\System32\mscoree.dll.local
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework*
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\NeverShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\ParentFolder

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\InitFolderHandler
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Desktop
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension

MODIFIED FILES

C:\Windows\sysnative\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
\??\PIPE\srvsvc
C:\Windows\sysnative\LogFiles\Scm\044a6734-e90e-4f8f-b357-b2dc8ab3b5ec
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenservicelock.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenrootstorelock.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen_service.log

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenofflinequeuelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenservicelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenrootstorelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenofflinequeuelock.dat
\??\SPDevice
\??\PIPE\wkssvc
C:\DfsServer
\Device\LanmanRedirector
\Device\SrvAdmin
\Device\LanmanServer
\Device\Srv2
\??\PIPE\lsarpc

RESOLVED APIS

shell32.dll.ShellExecuteExW
ole32.dll.OleInitialize
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
ole32.dll.CreateBindCtx
ole32.dll.CoTaskMemAlloc
propsys.dll.PSCreateMemoryPropertyStore
propsys.dll.PSPropertyBag_WriteDWORD
ole32.dll.CoGetApartmentType
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoTaskMemFree
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoGetMalloc
propsys.dll.PSPropertyBag_ReadDWORD
comctl32.dll.#320
ole32.dll.StringFromGUID2
comctl32.dll.#324
comctl32.dll.#323

advapi32.dll.RegEnumKeyW
oleaut32.dll.#2
propsys.dll.PSPropertyBag_ReadBSTR
propsys.dll.PSPropertyBag_ReadStrAlloc
shell32.dll.#102
advapi32.dll.OpenThreadToken
ole32.dll.CoInitializeEx
ole32.dll.CoCreateInstance
advapi32.dll.InitializeSecurityDescriptor
advapi32.dll.SetEntriesInAclW
ntmarta.dll.GetMartaExtensionInterface
advapi32.dll.SetSecurityDescriptorDacl
advapi32.dll.IsTextUnicode
comctl32.dll.#328
comctl32.dll.#334
comctl32.dll.#332
comctl32.dll.#338
ole32.dll.CoUninitialize
sechost.dll.ConvertSidToStringSidW
profapi.dll.#104
propsys.dll.#417
ole32.dll.PropVariantClear
oleaut32.dll.#9
comctl32.dll.#339
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386
advapi32.dll.RegQueryValueW
apphelp.dll.ApphelpCheckShellObject
propsys.dll.#430
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegGetValueW
advapi32.dll.RegCloseKey
ole32.dll.CoTaskMemRealloc
ole32.dll.CoAllowSetForegroundWindow

advapi32.dll.InstallApplication
oleaut32.dll.#500
kernel32.dll.InitializeSRWLock
kernel32.dll.AcquireSRWLockExclusive
kernel32.dll.AcquireSRWLockShared
kernel32.dll.ReleaseSRWLockExclusive
kernel32.dll.ReleaseSRWLockShared
shell32.dll.SHGetFolderPathW
advapi32.dll.SaferGetPolicyInformation
ntdll.dll.RtlDllShutdownInProgress
comctl32.dll.#329
ole32.dll.OleUninitialize
ole32.dll.CoRevokeInitializeSpy
comctl32.dll.#388
kernelbase.dll.SetThreadStackGuarantee
ole32.dll.CoInitializeSecurity
sechost.dll.LookupAccountNameLocalW
advapi32.dll.LookupAccountSidW
sechost.dll.LookupAccountSidLocalW
kernel32.dll.FlsAlloc
kernel32.dll.FlsFree

DELETED FILES

C:\Windows\Microsoft.NET\ngenserviceclientlock.dat
C:\Windows\Microsoft.NET\ngenservice_pri0_lock.dat
C:\Windows\Microsoft.NET\ngenservice_pri1_lock.dat

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanServer\Parameters\Guid

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\cmd.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay
HKEY_CLASSES_ROOT\.
HKEY_CLASSES_ROOT\.\OpenWithProgids
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.\OpenWithProgids
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.\UserChoice
HKEY_CLASSES_ROOT\Unknown

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\CurVer
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\ShellEx\IconHandler
HKEY_CLASSES_ROOT\SystemFileAssociations\.
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\BrowseInPlace

EXECUTED COMMANDS

"C:\Windows\system32\rundll32.exe" C:\Windows\system32\shell32.dll,OpenAs_RunDLL C:\Users\user\AppData\Local\Temp\275a1a4cdae156036639a3a4113b128fb5279d13
C:\Windows\system32\svchost.exe -k netsvcs
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
C:\Windows\system32\sppsvc.exe
C:\Windows\System32\svchost.exe -k WerSvcGroup
C:\Windows\system32\sc.exe start w32time task_started
C:\Windows\system32\svchost.exe -k LocalService

READ FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004b.db
C:\Users\user\Desktop\desktop.ini
C:\
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\Searches\desktop.ini
C:\Users\user\Videos\desktop.ini
C:\Users\user\Pictures\desktop.ini
C:\Users\user\Contacts\desktop.ini
C:\Users\user\Favorites\desktop.ini
C:\Users\user\Music\desktop.ini
C:\Users\user\Downloads\desktop.ini
C:\Users\user\Documents\desktop.ini
C:\Users\user\Links\desktop.ini

C:\Users\user\Saved Games\desktop.ini
C:\Windows\System32\shdocvw.dll
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\System32\
C:\Windows\System32\rundll32.exe
C:\Windows\SysWOW64\cmd.exe
\??\PIPE\srvsvc
C:\Windows\sysnative\LogFiles\Scm\044a6734-e90e-4f8f-b357-b2dc8ab3b5ec
C:\Windows\sysnative\LogFiles\Scm\a7c73732-9f11-4281-8d19-764d4ec9d94d
C:\Windows\sysnative\LogFiles\Scm\be669c13-8165-4536-96d0-6d6c39292aae
C:\Windows\sysnative\LogFiles\Scm\ca4b8ff2-a4d2-4d88-a52e-3a5bdaf7f56e
C:\Windows\sysnative\LogFiles\Scm\fb3c354d-297a-4eb2-9b58-090f6361906b
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvc.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvc.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\fusion.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe.config
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
C:\Windows\sysnative
C:\Windows\sysnative\spp\plugin-manifests-signed\sppwinob-spp-plugin-manifest-signed.xrm-ms
C:\Windows\sysnative\sppwinob.dll
C:\Windows\sysnative\spp\plugin-manifests-signed\sppobjs-spp-plugin-manifest-signed.xrm-ms
C:\Windows\sysnative\sppobjs.dll
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\SoftwareProtectionPlatform\Cache\cache.dat
\??\PIPE\wkssvc
C:\Windows\sysnative\sppsvc.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\LanmanRedirector
\Device\SrvAdmin

\Device\LanmanServer
\Device\Srv2
\??\PIPE\lsarpc
D:\
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui

MUTEXES

Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

STARTED SERVICES

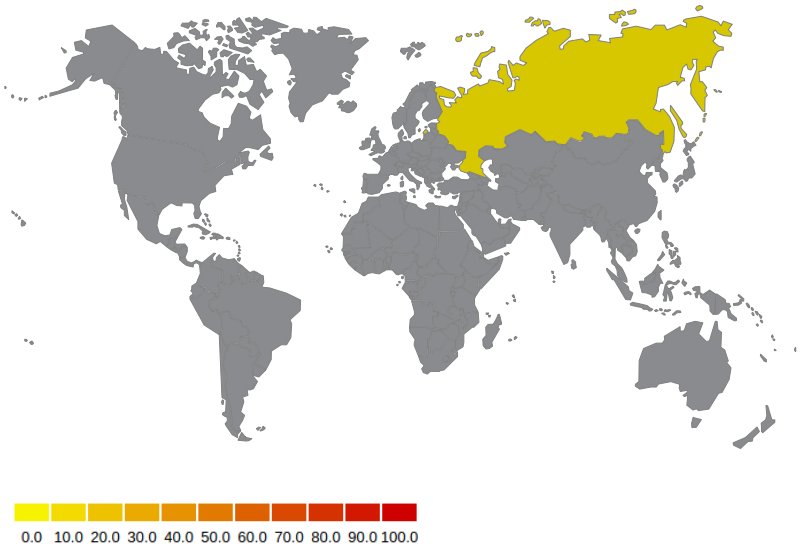
AppMgmt
WerSvc
Browser
IKEEXT
W32Time

MODIFIED REGISTRY KEYS

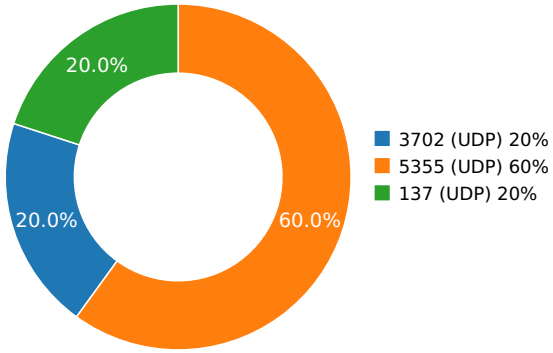
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_64\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WerSvc\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Browser\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\IKEEXT\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\W32Time\Type
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\ServiceSessionId
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanServer\Parameters\Guid
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\W32Time\TimeProviders\NtpClient\SpecialPollTimeRemaining

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	5.42.92.67	Russian Federation	203727	Sweden, Stockholm	Malware Process

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.03827691078	Sandbox	224.0.0.252	5355
3.03952503204	Sandbox	224.0.0.252	5355
3.04835987091	Sandbox	239.255.255.250	3702
3.08150601387	Sandbox	192.168.56.255	137
5.59894490242	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	SystemDestroyer.bat
File Type:	DOS batch file, ASCII text, with CRLF line terminators
SHA1:	275a1a4cdae156036639a3a4113b128fb5279d13
MD5:	64262e14320cd5d5b1a24b0784faba74
First Seen Date:	2023-07-29 13:59:19.698215 (2 years ago)
Number Of Clients Seen:	3
Last Analysis Date:	2023-07-31 17:44:45.707176 (2 years ago)
Human Expert Analysis Date:	2023-07-30 11:44:37.190474 (2 years ago)
Human Expert Analysis Result:	Clean

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	16
File Type Enum	1
File Size	650
Sha256	3f6c16f45b77b17f9cd70abafe5e25db7caa21b44065b0ecdbe12b90c825903a
Mime Type	text/x-msdos-batch

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS