VALKYRIE COMODO

## Summary

**File Name:** XGr4Y

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

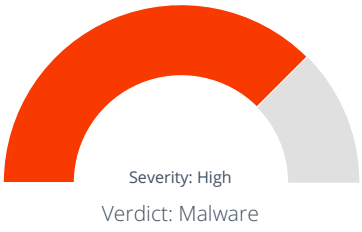
**SHA1:** 36f117cf983dce2c79268e121ab7435adc02dd9c

**MD5:** 61ea6b81f0de691abfb2f29625537dfb

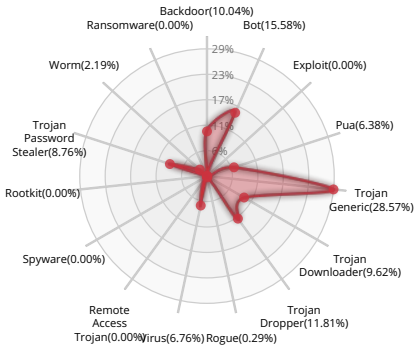
MALWARE

Valkyrie Final Verdict

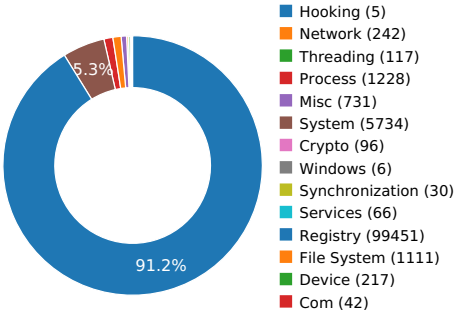
### DETECTION SECTION




### CLASSIFICATION




### HIGH LEVEL BEHAVIOR DISTRIBUTION




### ACTIVITY OVERVIEW

VALKYRIE COMODO

## Activity Details

### INFORMATION DISCOVERY

- Repeatedly searches for a not-found process, may want to run with startbrowser=1 option
- Attempts to remove evidence of file being downloaded from the Internet — Show sources

### NETWORKING

- HTTP traffic contains suspicious features which may be indicative of malware related traffic — Show sources
- Performs some HTTP requests — Show sources

### LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

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

### PACKER

- The binary likely contains encrypted or compressed data. — Show sources

### HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

- Creates RWX memory — Show sources

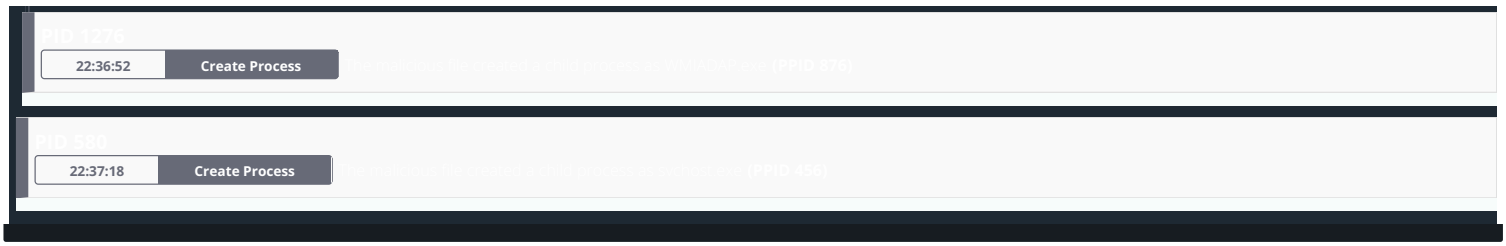
### PERSISTENCE AND INSTALLATION BEHAVIOR

- Deletes its original binary from disk — Show sources
- Installs itself for autorun at Windows startup — Show sources

### MALWARE ANALYSIS SYSTEM EVASION

- Possible date expiration check, exits too soon after checking local time — Show sources
- Mimics the system's user agent string for its own requests — Show sources
- Attempts to repeatedly call a single API many times in order to delay analysis time — Show sources

## Behavior Graph


PID 1276
22:36:52
Create Process
PID 580
22:37:18
Create Process

VALKYRIE COMODO

## Behavior Summary

### ACCESSED FILES

| |
|---|
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| C:\ |
| C:\Users\user\AppData\Local\Temp\36f117cf983dce2c79268e121ab7435adc02dd9c.exe |
| C:\Windows\ |
| C:\Windows\SysWOW64\ |
| \Device\KsecDD |
| C:\Windows\SysWOW64\shell32.dll |
| C:\Windows\SysWOW64\wordpaddev.exe |
| C:\Users |
| 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\desktop.ini |
| C:\Users\user |
| C:\Users\user\AppData |
| C:\Users\user\AppData\Local |
| C:\Users\user\AppData\Local\Temp |
| C:\Windows |
| C:\Windows\SysWOW64 |
| C:\Windows\SysWOW64\propsys.dll |
| C:\Windows\sysnative\propsys.dll |
| \??\MountPointManager |
| C:\Users\user\AppData\Local\ |
| C:\Windows\SysWOW64\wordpaddev.exe:Zone.Identifier |
| C:\Windows\Temp |
| C:\Windows\LastGood.Tmp |
| C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp |
| C:\Windows\ServiceProfiles |
| C:\Windows\ServiceProfiles\NetworkService |
| C:\Windows\sysnative\Tasks\Microsoft\Windows\WDI\ResolutionHost |
| C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk |
| C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk |
| C:\Windows\System32\ras*.pbk |
| C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk |
| C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk |
| 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 |
| C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.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\Framework\v4.0.30319 |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Windows\System32\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Windows\System32\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenservicetestlock.dat |
| C:\Windows\Microsoft.NET\ngenserviceclientlock.dat |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenofflinequeuelock.dat |
| C:\Windows\Microsoft.NET\ngenservice_pri0_lock.dat |
| C:\Windows\Microsoft.NET\ngenservice_pri1_lock.dat |
| C:\Windows\Microsoft.NET\ngenservice_pri2_lock.dat |

## READ REGISTRY KEYS

| |
|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{AA5B6A80-B834-11D0-932F-00A0C90DCAA9}\(Default) |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest |

| |
|---|
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\NoFileFolderConnection |
| 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_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_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension |
| 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\.exe\(Default) |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\DocObject |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\DocObject |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\BrowseInPlace |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\BrowseInPlace |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.exe\Content Type |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\IsShortcut |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\IsShortcut |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\AlwaysShowExt |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\AlwaysShowExt |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\NeverShowExt |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\NeverShowExt |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\PropertySystem\PropertyHandlers\.exe\(Default) |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{66742402-F9B9-11D1-A202-0000F81FEDEE}\DisableProcessIsolation |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{66742402-F9B9-11D1-A202-0000F81FEDEE}\NoOplock |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{66742402-F9B9-11D1-A202-0000F81FEDEE}\UseInProcHandlerCache |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{66742402-F9B9-11D1-A202-0000F81FEDEE}\UseOutOfProcHandlerCache |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\DocObject |
| HKEY_CURRENT_USER\Software\Classes\Folder\DocObject |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\DocObject |

## MODIFIED FILES

| |
|---|
| C:\Windows\SysWOW64\wordpaddev.exe |
| 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\ngenservice_pri3_lock.dat |
| C:\Windows\Microsoft.NET\ngennicupdatelock.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 |

| |
|---|
| C:\Windows\SoftwareDistribution\ReportingEvents.log |
| \Device\LanmanDatagramReceiver |

## RESOLVED APIS

| |
|---|
| advapi32.dll.RegQueryValueExA |
| kernel32.dll.LoadLibraryExA |
| kernel32.dll.GetProcAddress |
| kernel32.dll.VirtualAlloc |
| kernel32.dll.SetFilePointer |
| kernel32.dll.lstrlenA |
| kernel32.dll.lstrcatA |
| kernel32.dll.VirtualProtect |
| kernel32.dll.UnmapViewOfFile |
| kernel32.dll.GetModuleHandleA |
| kernel32.dll.WriteFile |
| kernel32.dll.CloseHandle |
| kernel32.dll.VirtualFree |
| kernel32.dll.GetTempPathA |
| kernel32.dll.CreateFileA |
| kernel32.dll.HeapAlloc |
| kernel32.dll.HeapFree |
| kernel32.dll.GetProcessHeap |
| kernel32.dll.GetModuleHandleW |
| kernel32.dll.GetLastError |
| ntdll.dll.RtlComputeCrc32 |
| ntdll.dll.NtUnmapViewOfSection |
| ntdll.dll._vsnprintf |
| ntdll.dll._snwprintf |
| ntdll.dll.RtlGetVersion |
| ntdll.dll._snprintf |
| ntdll.dll.memset |
| ntdll.dll._vsnwprintf |
| ntdll.dll.memcpy |
| kernel32.dll.ProcessIdToSessionId |
| kernel32.dll.LocalFree |
| kernel32.dll.LockFileEx |
| kernel32.dll.UnlockFileEx |
| kernel32.dll.FreeLibrary |
| kernel32.dll.VirtualQueryEx |
| kernel32.dll.GetTickCount |
| kernel32.dll.VirtualAllocEx |
| kernel32.dll.HeapReAlloc |

| |
|---|
| kernel32.dll.GetFileAttributesW |
| kernel32.dll.WTSGetActiveConsoleSessionId |
| kernel32.dll.CreateFileW |
| kernel32.dll.lstrcatW |
| kernel32.dll.ResumeThread |
| kernel32.dll.CreateProcessW |
| kernel32.dll.GetCurrentProcessId |
| kernel32.dll.MoveFileExW |
| kernel32.dll.LoadLibraryA |
| kernel32.dll.SetThreadContext |
| kernel32.dll.CreateToolhelp32Snapshot |
| kernel32.dll.SetLastError |
| kernel32.dll.WaitForSingleObject |
| kernel32.dll.GetCommandLineW |
| kernel32.dll.Process32FirstW |
| kernel32.dll.WideCharToMultiByte |
| kernel32.dll.GetLocalTime |
| kernel32.dll.GetTempFileNameW |
| kernel32.dll.GetModuleFileNameW |
| kernel32.dll.Process32NextW |
| kernel32.dll.CreateThread |
| kernel32.dll.lstrcmpiW |
| kernel32.dll.Wow64DisableWow64FsRedirection |
| kernel32.dll.IsWow64Process |
| kernel32.dll.DeleteFileW |
| kernel32.dll.SetFileAttributesW |
| kernel32.dll.Sleep |
| kernel32.dll.GetVolumeInformationW |
| kernel32.dll.GetNativeSystemInfo |
| kernel32.dll.VirtualProtectEx |
| kernel32.dll.lstrcpyW |
| kernel32.dll.GetComputerNameW |
| kernel32.dll.TerminateProcess |
| kernel32.dll.GetTempPathW |
| kernel32.dll.MapViewOfFile |
| kernel32.dll.CreateDirectoryW |
| kernel32.dll.SetEvent |
| kernel32.dll.SetErrorMode |

## DELETED FILES

| |
|---|
| C:\Users\user\AppData\Local\Temp\36f117cf983dce2c79268e121ab7435adc02dd9c.exe |
| C:\Windows\SysWOW64\wordpaddev.exe:Zone.Identifier |
| C:\Windows\LastGood.Tmp |

| |
|---|
| C:\Windows\Microsoft.NET\ngenserviceclientlock.dat |
| C:\Windows\Microsoft.NET\ngenservice_pri0_lock.dat |
| C:\Windows\Microsoft.NET\ngenservice_pri1_lock.dat |
| C:\Windows\Microsoft.NET\ngenservice_pri2_lock.dat |

## REGISTRY KEYS

| |
|---|
| HKEY_CLASSES_ROOT\interface\{aa5b6a80-b834-11d0-932f-00a0c90dcaa9} |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{AA5B6A80-B834-11D0-932F-00A0C90DCAA9}\(Default) |
| 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\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles |
| 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\Explorer |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\NoFileFolderConnection |
| 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\36f117cf983dce2c79268e121ab7435adc02dd9c.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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume |
| 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_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Explorer |
| HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension |
| 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\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 |

## EXECUTED COMMANDS

| |
|---|
| C:\Users\user\AppData\Local\Temp\36f117cf983dce2c79268e121ab7435adc02dd9c.exe --6b17f7b |

| |
|---|
| "C:\Windows\SysWOW64\wordpaddev.exe" |
| 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\SysWOW64\wordpaddev.exe --93330b7e |
| \\?\C:\Windows\system32\wbem\WMIADAP.EXE wmiadap.exe /F /T /R |

**READ FILES**

| |
|---|
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| C:\Users\user\AppData\Local\Temp\36f117cf983dce2c79268e121ab7435adc02dd9c.exe |
| \Device\KsecDD |
| C:\Windows\SysWOW64\shell32.dll |
| C:\ |
| 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\desktop.ini |
| C:\Users |
| C:\Users\user |
| C:\Users\user\AppData |
| C:\Users\user\AppData\Local |
| C:\Windows |
| C:\Users\user\AppData\Local\Temp |
| C:\Windows\LastGood.Tmp |
| C:\Windows\SysWOW64\wordpaddev.exe |
| 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\Framework\v4.0.30319\clr.dll |
| C:\Windows\assembly\GAC_MSIL\Accessibility\2.0.0.0__b03f5f7f11d50a3a\Accessibility.dll.config |
| C:\Windows\assembly\GAC_MSIL\Accessibility\2.0.0.0__b03f5f7f11d50a3a\Accessibility.dll |
| C:\Windows\Microsoft.Net\assembly\GAC_MSIL\AspNetMMCExt\v4.0_4.0.0.0__b03f5f7f11d50a3a\AspNetMMCExt.dll.config |
| C:\Windows\Microsoft.Net\assembly\GAC_MSIL\AspNetMMCExt\v4.0_4.0.0.0__b03f5f7f11d50a3a\AspNetMMCExt.dll |
| C:\Windows\assembly\GAC_32\AuditPolicyGPManagedStubs.Interop\6.1.0.0__31bf3856ad364e35\AuditPolicyGPManagedStubs.Interop.dll.config |
| C:\Windows\assembly\GAC_32\AuditPolicyGPManagedStubs.Interop\6.1.0.0__31bf3856ad364e35\AuditPolicyGPManagedStubs.Interop.dll |
| C:\Windows\assembly\GAC_32\BDATunePIA\6.1.0.0__31bf3856ad364e35\BDATunePIA.dll.config |
| C:\Windows\assembly\GAC_32\BDATunePIA\6.1.0.0__31bf3856ad364e35\BDATunePIA.dll |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\aspnet_intern.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\aspnet_intern.exe |

| |
|---|
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\aspnet_merge.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\AxImp.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\AxImp.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\lc.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\ResGen.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\ResGen.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\SecAnnotate.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\SecAnnotate.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\sgen.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\sgen.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\SqlMetal.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\SqlMetal.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\SvcUtil.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\SvcUtil.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\TlbExp.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\TlbExp.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\TlbImp.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\TlbImp.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\WinMDExp.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\WinMDExp.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\wsdl.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\xsd.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\xsd.exe |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\xsltc.exe.config |
| C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\xsltc.exe |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\ComSvcConfig.exe.config |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\ComSvcConfig.exe |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\dfsvc.exe.config |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe.config |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe.config |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\WsatConfig.exe.config |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\WsatConfig.exe |
| C:\Windows\assembly\GAC_MSIL\ComSvcConfig\3.0.0.0__b03f5f7f11d50a3a\ComSvcConfig.exe.config |
| C:\Windows\assembly\GAC_MSIL\ComSvcConfig\3.0.0.0__b03f5f7f11d50a3a\ComSvcConfig.exe |
| C:\Windows\assembly\GAC_32\CustomMarshalers\2.0.0.0__b03f5f7f11d50a3a\CustomMarshalers.dll.config |
| C:\Windows\assembly\GAC_32\CustomMarshalers\2.0.0.0__b03f5f7f11d50a3a\CustomMarshalers.dll |
| C:\Windows\assembly\GAC_MSIL\dfsvc\2.0.0.0__b03f5f7f11d50a3a\dfsvc.exe.config |
| C:\Windows\assembly\GAC_MSIL\dfsvc\2.0.0.0__b03f5f7f11d50a3a\dfsvc.exe |
| C:\Windows\assembly\GAC_32\ehexthost32\6.1.0.0__31bf3856ad364e35\ehexthost32.exe.config |
| C:\Windows\assembly\GAC_MSIL\ehiExtens\6.1.0.0__31bf3856ad364e35\ehiExtens.dll.config |
| C:\Windows\assembly\GAC_MSIL\ehiExtens\6.1.0.0__31bf3856ad364e35\ehiExtens.dll |

C:\Windows\assembly\GAC_MSIL\EventViewer\6.1.0.0__31bf3856ad364e35\EventViewer.dll.config

## MUTEXES

Global\I20503A4E

Global\M20503A4E

IESQMMUTEX_0_208

Global\ADAP_WMI_ENTRY

## STARTED SERVICES

wordpaddev

WerSvc

## MODIFIED REGISTRY KEYS

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\Winmgmt\Type

HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Accessibility, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\AspNetMMCExt, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\AuditPolicyGPManagedStubs.Interop, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\BDATunePIA, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/aspnet_intern.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/aspnet_merge.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/AxImp.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/lc.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/ResGen.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SecAnnotate.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/sgen.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SqlMetal.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SvcUtil.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/TlbExp.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/TlbImp.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/WinMDExp.exe\0\RuntimeVersion

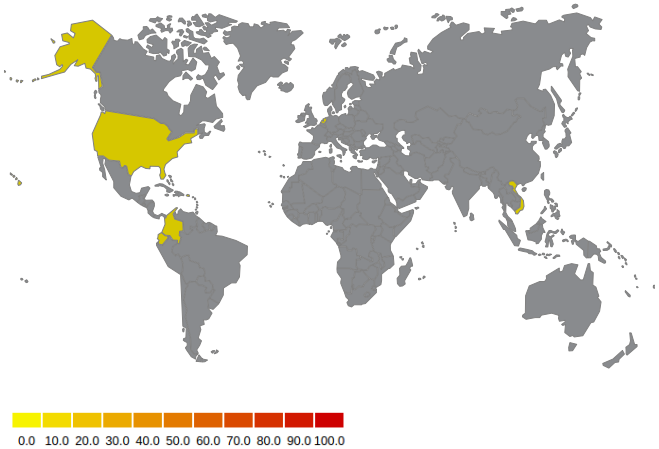
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/wsdl.exe\0\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1

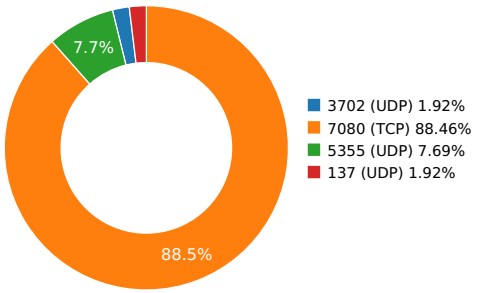
| |
|---|
| Tools/xsd.exe\0\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/xsltc.exe\0\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/ComSvcConfig.exe\0\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/dfsvc.exe\0\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/MSBuild.exe\0\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/SMSvcHost.exe\0\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/WsatConfig.exe\0\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ComSvcConfig, Version=3.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\CustomMarshalers, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=x86\1\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\dfsvc, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ehexthost32, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ehiExtens, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\EventViewer, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\ServiceSessionId |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Reporting\RebootWatch |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\NextSqmReportTime |

## Network Behavior

CONTACTED IPS




NETWORK PORT DISTRIBUTION




| Name | IP | Country | ASN | ASN Name | Trigger Process Type |
|---|---|---|---|---|---|
| | 204.138.46.166 | United States | 32710 | International Reliable Access Network | Malware Process |
| | 190.121.143.147 | Colombia | 27951 | JUVINET SAS | Malware Process |
| | 186.5.100.92 | Ecuador | 27947 | Clientes Guayaquil | Malware Process |
| | 115.75.36.220 | Vietnam | 7552 | Viettel Group No 1, Tran Huu Duc street, My... | Malware Process |

### HTTP PACKETS

| Host | Port | Method | Version | User Agent | Count | Call Time During Execution(Sec) |
|---|---|---|---|---|---|---|
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 139.082484961 |
| **Path:** /glitch/<br>**URI:** http://204.138.46.166:7080/glitch/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 149.579353809 |
| **Path:** /window/results/codec/<br>**URI:** http://204.138.46.166:7080/window/results/codec/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 159.95103097 |
| **Path:** /sess/between/health/<br>**URI:** http://204.138.46.166:7080/sess/between/health/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 170.428140879 |
| **Path:** /chunk/<br>**URI:** http://204.138.46.166:7080/chunk/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 180.84088397 |
| **Path:** /vermont/health/balloon/<br>**URI:** http://204.138.46.166:7080/vermont/health/balloon/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 198.594848871 |
| **Path:** /raster/schema/cab/<br>**URI:** http://204.138.46.166:7080/raster/schema/cab/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 208.998437881 |
| **Path:** /cab/nsip/<br>**URI:** http://204.138.46.166:7080/cab/nsip/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 219.378863811 |
| **Path:** /tpt/xian/<br>**URI:** http://204.138.46.166:7080/tpt/xian/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 229.791169882 |

| Host | Port | Method | Version | User Agent | Count | Call Time During Execution(Sec) |
|---|---|---|---|---|---|---|
| **Path:** /codec/<br>**URI:** http://204.138.46.166:7080/codec/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 240.217738867 |
| **Path:** /walk/window/cookies/<br>**URI:** http://204.138.46.166:7080/walk/window/cookies/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 250.579574823 |
| **Path:** /report/bml/iplk/merge/<br>**URI:** http://204.138.46.166:7080/report/bml/iplk/merge/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 260.980348825 |
| **Path:** /acquire/raster/<br>**URI:** http://204.138.46.166:7080/acquire/raster/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 271.358766794 |
| **Path:** /attrib/merge/<br>**URI:** http://204.138.46.166:7080/attrib/merge/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 281.759620905 |
| **Path:** /stubs/<br>**URI:** http://204.138.46.166:7080/stubs/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 292.190995932 |
| **Path:** /report/sym/mult/<br>**URI:** http://204.138.46.166:7080/report/sym/mult/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 302.645983934 |
| **Path:** /chunk/health/<br>**URI:** http://204.138.46.166:7080/chunk/health/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 313.008513927 |
| **Path:** /pdf/devices/<br>**URI:** http://204.138.46.166:7080/pdf/devices/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 323.418316841 |
| **Path:** /jit/<br>**URI:** http://204.138.46.166:7080/jit/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 333.806045771 |
| **Path:** /devices/schema/schema/merge/<br>**URI:** http://204.138.46.166:7080/devices/schema/schema/merge/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 344.21901083 |
| **Path:** /pnp/mult/<br>**URI:** http://204.138.46.166:7080/pnp/mult/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 354.587119818 |
| **Path:** /xian/<br>**URI:** http://204.138.46.166:7080/xian/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 364.98700285 |
| **Path:** /enable/stubs/publish/merge/<br>**URI:** http://204.138.46.166:7080/enable/stubs/publish/merge/ | | | | | | |
| 204.138.46.166:7080 | 7080 | POST | 1.1 | Mozilla/4.0 (compatible; MSIE 7.0; W... | 1 | 375.443287849 |
| **Path:** /mult/loadan/prep/merge/<br>**URI:** http://204.138.46.166:7080/mult/loadan/prep/merge/ | | | | | | |

## TCP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 139.082484961 | Sandbox | 204.138.46.166 | 7080 |
| 149.579353809 | Sandbox | 204.138.46.166 | 7080 |
| 159.95103097 | Sandbox | 204.138.46.166 | 7080 |
| 170.428140879 | Sandbox | 204.138.46.166 | 7080 |
| 180.84088397 | Sandbox | 204.138.46.166 | 7080 |
| 198.594848871 | Sandbox | 204.138.46.166 | 7080 |
| 208.998437881 | Sandbox | 204.138.46.166 | 7080 |
| 219.378863811 | Sandbox | 204.138.46.166 | 7080 |
| 229.791169882 | Sandbox | 204.138.46.166 | 7080 |
| 240.217738867 | Sandbox | 204.138.46.166 | 7080 |
| 250.579574823 | Sandbox | 204.138.46.166 | 7080 |
| 260.980348825 | Sandbox | 204.138.46.166 | 7080 |
| 271.358766794 | Sandbox | 204.138.46.166 | 7080 |
| 281.759620905 | Sandbox | 204.138.46.166 | 7080 |
| 292.190995932 | Sandbox | 204.138.46.166 | 7080 |
| 302.645983934 | Sandbox | 204.138.46.166 | 7080 |
| 313.008513927 | Sandbox | 204.138.46.166 | 7080 |
| 323.418316841 | Sandbox | 204.138.46.166 | 7080 |
| 333.806045771 | Sandbox | 204.138.46.166 | 7080 |
| 344.21901083 | Sandbox | 204.138.46.166 | 7080 |
| 354.587119818 | Sandbox | 204.138.46.166 | 7080 |
| 364.98700285 | Sandbox | 204.138.46.166 | 7080 |
| 375.443287849 | Sandbox | 204.138.46.166 | 7080 |

## UDP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 3.03527379036 | Sandbox | 224.0.0.252 | 5355 |
| 3.03587388992 | Sandbox | 224.0.0.252 | 5355 |
| 3.03628182411 | Sandbox | 239.255.255.250 | 3702 |
| 3.07932782173 | Sandbox | 192.168.56.255 | 137 |
| 5.62689685822 | Sandbox | 224.0.0.252 | 5355 |
| 52.417388916 | Sandbox | 224.0.0.252 | 5355 |

VALKYRIE COMODO

DETAILED FILE INFO

## CREATED / DROPPED FILES

| FILE PATH | TYPE AND HASHES |
|---|---|
| **C:\Windows\Microsoft.NET\Framework\V4.0.30319\Ngen_service.Log** | **Type :** UTF-8 Unicode (with BOM) text, with CRLF line terminators<br>**MD5 :** f9c359f7382563a11245d8afecab1f1a<br>**SHA-1 :** 2a9264021d920403cd8697c510b3516b5963053a<br>**SHA-256 :** 91429e026627f89978716dae847344ba6f47169be3faf722a40cc<br>**SHA-512 :** 1a410d0b935306002d4b53ec7ad6be8a4422c2df0b0006e5e14(<br>**Size :** 6.302 Kilobytes. |
| **C:\Windows\Microsoft.NET\Framework64\V4.0.30319\Ngen_service.Log** | **Type :** UTF-8 Unicode (with BOM) text, with CRLF line terminators<br>**MD5 :** ab6020699db5d8835d907b016e66c177<br>**SHA-1 :** cd47836592d58fca9e79825982fa88861deb34c7<br>**SHA-256 :** 402a72d71628ea4d7e52788721025aa73aa1b62feaa0f5c06db9<br>**SHA-512 :** 9e6ec112c2c9d8cba7bddd7fcf9e3cf062e51ffd62cccd7f440651b<br>**Size :** 6.329 Kilobytes. |

## MATCH YARA RULES

| MATCH RULES |
|---|

## STATIC FILE INFO

| | |
|---|---|
| **File Name:** | XGr4Y |
| **File Type:** | PE32 executable (GUI) Intel 80386, for MS Windows |
| **SHA1:** | 36f117cf983dce2c79268e121ab7435adc02dd9c |
| **MD5:** | 61ea6b81f0de691abfb2f29625537dfb |
| **First Seen Date:** | 2019-03-26 09:29:18.321438 ( 7 days ago ) |
| **Number Of Clients Seen:** | 2 |
| **Last Analysis Date:** | 2019-03-27 07:12:54.963213 ( 6 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 | [[67.4, u'Win32 Executable MS Visual C++ (generic)'], [14.2, u'Win32 Dynamic Link Library (generic)'], [9.7, u'Win32 Executable (generic)'], [4.3, u'Generic Win/DOS Executable'], [4.3, u'DOS Executable Generic']] |
| Compilation Time Stamp | 0x5C99ED84 [Tue Mar 26 09:14:44 2019 UTC] |
| LegalCopyright | Copyright (C) 2005-2014. All rights reserved. |
| InternalName | SupportWizard.exe |
| FileVersion | 4.5.4.1 |
| CompanyName | |
| ProductName | |
| ProductVersion | 4.5.4.1 |
| FileDescription | SupportWizard.exe |
| OriginalFilename | SupportWizard.exe |
| Translation | 0x0000 0x04b0 |
| Entry Point | 0x401960 (.text) |
| Machine Type | Intel 386 or later - 32Bit |
| File Size | 248072 |
| Ssdeep | 6144:GAgLyfzX9PRYP4WRCnYstdP2tmmm8myoXPYoPrgdI8U:DgGz9PugWYfu0mm8myoXTP8U |
| Sha256 | 04214377b1b5f7b7b1df58676f92f4abb302840516170ba35159de746e0e7015 |
| Exifinfo | [{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/6/f/1/36f117cf983dce2c79268e121ab7435adc02dd9c', u'EXE:OriginalFileName': u'SupportWizard.exe', u'EXE:ProductName': u' ', u'EXE:InternalName': u'SupportWizard.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2019:03:26 09:28:37+00:00', u'EXE:InitializedDataSize': 236032, u'File:FileModifyDate': u'2019:03:26 09:28:37+00:00', u'EXE:FileVersionNumber': u'4.5.4.1', u'EXE:FileVersion': u'4.5.4.1', u'File:FileSize': u'242 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': u'4.5.4.1', u'EXE:ObjectFileType': u'Dynamic link library', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u' ', u'File:FileName': u'36f117cf983dce2c79268e121ab7435adc02dd9c', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2019:03:26 09:14:44+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright (C) 2005-2014. All rights reserved.', u'EXE:LinkerVersion': 9.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/6/f/1', u'EXE:FileDescription': u'SupportWizard.exe', u'EXE:EntryPoint': u'0x1960', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 7680, u'File:FileInodeChangeDate': u'2019:03:26 09:28:37+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'4.5.4.1'}] |
| Mime Type | application/x-dosexec |
| Imphash | 7bc4d4aa0311efdac1b87157013f1df1 |

### PE Sections

| NAME | VIRTUAL ADDRESS | VIRTUAL SIZE | RAW SIZE | ENTROPY | MD5 |
|---|---|---|---|---|---|
| .text | 0x1000 | 0x1cc0 | 0x1e00 | 5.2592886866 | 9e7b8ee1673251a09f1e090057e4f17c |
| .rdata | 0x3000 | 0x1e070 | 0x1e200 | 7.72697991186 | d07f1487339fbd41cde3875cdff97769 |
| .data | 0x22000 | 0x154 | 0x200 | 1.44901819313 | 47fba1ec778c43e9b8f3d34a7ec350d0 |
| .rsrc | 0x23000 | 0x1b4c8 | 0x1b600 | 6.51267586977 | 10126cc6e90bc42886f6dd874ffd5f90 |

### PE Imports

- KERNEL32.dll

- GetCommandLineW
- GetConsoleCP
- GetConsoleMode
- GetConsoleOutputCP
- GetCurrentDirectoryA
- GetCurrentDirectoryW
- GetCurrentProcess
- GetCurrentProcessId
- GetCurrentThread
- GetCurrentThreadId
- GetDateFormatA
- GetDateFormatW
- GetDiskFreeSpaceA
- GetDiskFreeSpaceW
- GetDriveTypeA
- GetDriveTypeW
- GetEnvironmentStrings
- GetEnvironmentStringsW
- GetEnvironmentVariableA
- GetEnvironmentVariableW
- GetExitCodeThread
- GetFileAttributesA
- GetFileAttributesExA
- GetFileAttributesExW
- GetFileAttributesW
- GetFileSize
- GetFileSizeEx
- GetFileTime
- GetFileType
- GetFullPathNameA
- GetFullPathNameW
- GetHandleInformation
- GetLastError
- GetLocalTime
- GetLocaleInfoA
- GetLocaleInfoW
- GetLogicalDriveStringsW
- GetLongPathNameW
- GetModuleFileNameA
- GetModuleFileNameW
- GetModuleHandleA
- GetOEMCP
- GetPrivateProfileIntA
- GetPrivateProfileStringA
- GetPrivateProfileStringW
- GetProcessHeap
- GetProfileIntA
- GetShortPathNameA
- GetShortPathNameW
- GetStartupInfoA
- GetStartupInfoW
- GetStdHandle
- GetStringTypeA
- GetStringTypeExA
- GetStringTypeW
- GetSystemDefaultLangID
- GetSystemDefaultUILanguage
- GetSystemDirectoryW
- GetSystemInfo
- GetSystemTime
- GetSystemTimeAsFileTime
- GetSystemWindowsDirectoryW
- GetTempFileNameA
- GetTempFileNameW
- GetTempPathA
- GetTempPathW
- GetThreadLocale
- GetThreadPriority
- GetTickCount
- GetTimeFormatA
- GetTimeZoneInformation
- GetUserDefaultLCID
- GetUserDefaultLangID
- GetUserDefaultUILanguage
- GetVersion
- GetVersionExA
- GetVersionExW
- GetVolumeInformationA
- GetVolumeInformationW
- GetWindowsDirectoryW
- GlobalAddAtomA
- GlobalAddAtomW
- GlobalAlloc
- GlobalDeleteAtom
- GlobalFindAtomA
- GlobalFindAtomW
- GlobalFlags
- GlobalFree
- GlobalGetAtomNameA
- GlobalHandle
- GlobalLock

- GlobalMemoryStatus
- GlobalReAlloc
- GlobalSize
- GlobalUnlock
- HeapAlloc
- HeapCreate
- HeapDestroy
- HeapFree
- HeapReAlloc
- HeapSetInformation
- HeapSize
- HeapValidate
- InitializeCriticalSection
- GetCommandLineA
- InterlockedCompareExchange
- InterlockedDecrement
- InterlockedExchange
- InterlockedExchangeAdd
- InterlockedIncrement
- IsBadReadPtr
- IsBadWritePtr
- IsDebuggerPresent
- IsValidCodePage
- IsValidLocale
- LCMapStringA
- LCMapStringW
- LeaveCriticalSection
- LoadLibraryExA
- LoadLibraryExW
- LoadLibraryW
- LoadResource
- LocalAlloc
- LocalFileTimeToFileTime
- LocalFree
- LocalReAlloc
- LocalShrink
- LockFile
- LockResource
- MapViewOfFile
- Module32NextW
- MoveFileA
- MoveFileExW
- MulDiv
- MultiByteToWideChar
- OpenEventA
- OpenEventW
- OpenFileMappingA
- OutputDebugStringA
- OutputDebugStringW
- QueryPerformanceCounter
- RaiseException
- ReadFile
- ReadProcessMemory
- RemoveDirectoryW
- ResetEvent
- ResumeThread
- RtlUnwind
- SearchPathW
- SetConsoleCtrlHandler
- SetCurrentDirectoryW
- SetEndOfFile
- SetEnvironmentVariableA
- SetEnvironmentVariableW
- SetErrorMode
- SetEvent
- SetFileAttributesA
- SetFileAttributesW
- SetFilePointer
- SetFileTime
- SetHandleCount
- SetLastError
- SetPriorityClass
- SetStdHandle
- SetThreadLocale
- SetThreadPriority
- SetUnhandledExceptionFilter
- SizeofResource
- Sleep
- SleepEx
- SuspendThread
- SwitchToThread
- SystemTimeToFileTime
- SystemTimeToTzSpecificLocalTime
- TerminateProcess
- TerminateThread
- TlsAlloc
- TlsFree
- TlsGetValue
- TlsSetValue
- TryEnterCriticalSection
- UnhandledExceptionFilter

    - UnlockFile
    - UnmapViewOfFile
    - VirtualFree
    - VirtualProtect
    - VirtualQuery
    - VirtualQueryEx
    - WaitForMultipleObjectsEx
    - WaitForSingleObject
    - WideCharToMultiByte
    - WinExec
    - WriteConsoleA
    - WriteConsoleW
    - WriteFile
    - WritePrivateProfileStringA
    - WritePrivateProfileStringW
    - WriteProcessMemory
    - lstrcatW
    - lstrcmpA
    - lstrcmpW
    - lstrcmpiA
    - lstrcmpiW
    - lstrcpyA
    - lstrcpyW
    - lstrcpyn
    - lstrcpynW
    - lstrlenA
    - lstrlenW
    - GetCalendarInfoW
    - GetCPInfoExW
    - GetCPInfo
    - GetAtomNameA
    - GetACP
    - FreeResource
    - FreeLibrary
    - FreeEnvironmentStringsW
    - FreeEnvironmentStringsA
    - FormatMessageW
    - FormatMessageA
    - FlushInstructionCache
    - FlushFileBuffers
    - FindResourceW
    - FindResourceExA
    - FindResourceA
    - FindNextFileW
    - FindFirstFileW
    - FindFirstFileA
    - FindClose
    - FileTimeToSystemTime
    - FileTimeToLocalFileTime
    - FileTimeToDosDateTime
    - FatalExit
    - FatalAppExitA
    - ExpandEnvironmentStringsW
    - ExitThread
    - ExitProcess
    - EnumSystemLocalesW
    - EnumSystemLocalesA
    - EnumResourceLanguagesA
    - EnumCalendarInfoW
    - EnterCriticalSection
    - DuplicateHandle
    - DeviceIoControl
    - DeleteFileW
    - DeleteFileA
    - DeleteCriticalSection
    - DebugBreak
    - CreateThread
    - CreateProcessW
    - CreateMutexW
    - CreateFileW
    - CreateFileMappingA
    - CreateFileA
    - CreateEventW
    - CreateEventA
    - CreateDirectoryW
    - CreateDirectoryA
    - CopyFileW
    - CopyFileA
    - ConvertDefaultLocale
    - CompareStringW
    - CompareStringA
    - CompareFileTime
    - CloseHandle
    - AssignProcessToJobObject
    - GetModuleHandleW
    - LoadLibraryA
    - GetProcAddress
    - InitializeCriticalSectionAndSpinCount
    - VirtualAlloc
- USER32.dll
    - GetWindowDC

- GetWindowLongW
- GetWindowPlacement
- GetWindowRect
- GetWindowTextW
- GetWindowThreadProcessId
- GrayStringW
- IntersectRect
- IsChild
- IsDialogMessageW
- IsIconic
- IsWindow
- IsWindowEnabled
- IsWindowVisible
- KillTimer
- LoadBitmapW
- LoadCursorW
- LoadIconW
- LoadStringW
- MapDialogRect
- MapWindowPoints
- MessageBeep
- MessageBoxW
- ModifyMenuW
- MoveWindow
- OffsetRect
- PeekMessageW
- PostMessageW
- PostQuitMessage
- PostThreadMessageW
- PtInRect
- RedrawWindow
- RegisterClassW
- RegisterClipboardFormatW
- RegisterWindowMessageW
- ReleaseCapture
- ReleaseDC
- RemovePropW
- SendDlgItemMessageA
- SendDlgItemMessageW
- SendMessageW
- SetActiveWindow
- SetCapture
- SetCursor
- SetFocus
- SetForegroundWindow
- SetMenuItemBitmaps
- SetPropW
- SetRect
- SetTimer
- SetWindowContextHelpId
- SetWindowLongW
- SetWindowPos
- SetWindowRgn
- SetWindowTextW
- SetWindowsHookExW
- ShowWindow
- SwitchToThisWindow
- SystemParametersInfoA
- SystemParametersInfoW
- TabbedTextOutW
- TranslateMessage
- UnhookWindowsHookEx
- UnregisterClassA
- UnregisterClassW
- UpdateWindow
- ValidateRect
- WinHelpW
- GetSystemMetrics
- GetSysColorBrush
- GetSysColor
- GetSubMenu
- GetPropW
- GetParent
- GetNextDlgTabItem
- GetNextDlgGroupItem
- GetMessageW
- GetMessageTime
- GetMessagePos
- GetMenuState
- GetMenuItemID
- GetMenuItemCount
- GetMenuCheckMarkDimensions
- GetMenu
- GetLastInputInfo
- GetLastActivePopup
- GetKeyState
- GetForegroundWindow
- GetFocus
- GetDlgItem
- GetDlgCtrlID
- GetDesktopWindow

- GetDC
- GetCursorPos
- GetClientRect
- GetClassNameW
- GetClassLongW
- GetClassInfoW
- GetClassInfoExW
- GetCapture
- GetActiveWindow
- FlashWindowEx
- FindWindowW
- EqualRect
- EndPaint
- EndDialog
- EnableWindow
- EnableMenuItem
- DrawTextW
- DrawTextExW
- DrawIcon
- DispatchMessageW
- DestroyWindow
- DestroyMenu
- DefWindowProcW
- CreateWindowExW
- CreateDialogIndirectParamW
- CopyRect
- ClientToScreen
- CheckMenuItem
- CharUpperW
- CharNextW
- CallWindowProcW
- CallNextHookEx
- BringWindowToTop
- BeginPaint
- AttachThreadInput
- AdjustWindowRectEx
- GetTopWindow
- GetWindow

- GDI32.dll
  - CreateFontIndirectW
  - CreateFontW
  - CreateHalftonePalette
  - CreatePalette
  - CreatePen
  - CreateRectRgn
  - CreateSolidBrush
  - DeleteDC
  - DeleteObject
  - Ellipse
  - EndPath
  - EnumFontFamiliesExW
  - ExcludeClipRect
  - ExtCreateRegion
  - ExtTextOutW
  - FillPath
  - FillRgn
  - FrameRgn
  - GdiFlush
  - GetDeviceCaps
  - GetNearestPaletteIndex
  - GetObjectW
  - GetPaletteEntries
  - GetRegionData
  - CreateDIBSection
  - GetStockObject
  - GetSystemPaletteEntries
  - GetTextAlign
  - GetTextColor
  - GetTextExtentPoint32W
  - GetTextExtentPointW
  - GetTextMetricsW
  - LineTo
  - MoveToEx
  - RealizePalette
  - RoundRect
  - SelectObject
  - SelectPalette
  - SetBkColor
  - SetBkMode
  - SetMapMode
  - SetPolyFillMode
  - SetRectRgn
  - SetStretchBltMode
  - SetTextAlign
  - SetTextColor
  - StretchDIBits
  - TextOutW
  - TranslateCharsetInfo
  - CreateCompatibleDC
  - CreateCompatibleBitmap
  - CombineRgn

- BitBlt
- GetRgnBox
- BeginPath

- ADVAPI32.dll
  - RegOpenKeyA
- COMCTL32.dll
  - ImageList_Create
  - InitCommonControlsEx
  - _TrackMouseEvent

### PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 200480, u'sha256': u'4d4998264c5fee9510985e226403d72f02a712d2e195cf0e85baefaaf0962df2', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 200816, u'sha256': u'8f1e1a840f461c1011b3e6e90ff086a2622a8765009ab0c4e87275c52f16c2ad', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 201152, u'sha256': u'f88b5d6d4a4ce0b11147f5c3d832db973bc06d3f6046d7c4cb7331e97867aa8f', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 201488, u'sha256': u'b31a8733696b65d9223657ba0a40298f102914ec742b2473962b4ac8a75f7ee6', u'type': u'AmigaOS bitmap font', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 201800, u'sha256': u'b1a30849981139 57e42273ce24371f383e2dd589beb9e4d52644ae38891eefc9', u'type': u'data', u'size': 180}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 202024, u'sha256': u'9a9b0a708d41db5c08ba7c84d2e52a93ba2dfae6e9bbf58d3a8f62655f24899e', u'type': u'AmigaOS bitmap font', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 202336, u'sha256': u'9cf18aac5d9ff9ef843647d310ba163e978454236edc71bee34732367e1618de', u'type': u'data', u'size': 180}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 202560, u'sha256': u'1019c029ff17960eecbaadc647b3020ffd2af0a07377f1c8ac1414d8e11fd87a', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 202896, u'sha256': u'c01b10d2e3109905be48d7cab7ff26c3fcddd75671359711fa320d7329f0d012', u'type': u'Hitachi SH big-endian COFF object, not stripped', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 145136, u'sha256': u'f4634d37875c877183356d4acfec7cec365358026ecc36707ca20a71fff2e6d9', u'type': u'dBase IV DBT of p.DBF, block length 50176, next free block index 40, next free block 0, next used block 0', u'size': 50216}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 203232, u'sha256': u'718672f1deeab7cbd23a12ed1f00a588453833db46a97db22792d20f1888c6a4', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 32637}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 235872, u'sha256': u'860337bd6a1301aad125ac1d8f2e1c293ea773f5622c613abc901b31abd6d1e6', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 245512, u'sha256': u'90db7be698130be075d1cfcff643e3b954d9f68568cdaccbaf646f1136952aeb', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 249776, u'sha256': u'cccfb7e3a3d433c702f6e53ea7e4885324d4544a67d836ce8e8421e2e49dbc01', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 252216, u'sha256': u'7422c69b2e05bdadb13415009fa2f667978319ee973791ce8650f349a6e46cff', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 195352, u'sha256': u'bce7070b73bac70f147eb6ab5041759fd6e7eb13539db9a96c47de918a1f0571', u'type': u'data', u'size': 1204}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 196560, u'sha256': u'88650f1ce60f9ccf68e78cda18cd280a998e2ca51748011bb2af89b75cc0ee0e', u'type': u'data', u'size': 1156}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 197720, u'sha256': u'f8ba24aa80903e61f2b476b6d8bfa4672b37d5d790ae6c82c1e691086fa7f3a6', u'type': u'data', u'size': 444}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 198168, u'sha256': u'5cc3f2f4da4f6d4483a43f574d41e670aa55e35ac0531062b23144a68e5011cb', u'type': u'data', u'size': 998}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 199168, u'sha256': u'f329c9af5a50ebf4b85d7ead46767b6fe0407ed21f3404ef8423dd45ca8eb9cc', u'type': u'data', u'size': 1032}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 200200, u'sha256': u'4bac1b94186b8be6eb1828808830d3efc849f2acb94bed7f7ca380abd8125ebe', u'type': u'data', u'size': 280}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 254968, u'sha256': u'34b7d0d30fdf0b5399bc51b069ddcc3b54579546883e400904379c4ddae44b45', u'type': u'data', u'size': 208}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_RCDATA', u'offset': 254168, u'sha256': u'e56b4abc7f5ed56d0d980c4a6121aef45d178bbf32c53c392446890862d0c1ca', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators', u'size': 796}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 200792, u'sha256': u'c53efa8085835ba129c1909beaff8a67b45f50837707f22dfff0f24d8cd26710', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 201128, u'sha256': u'b07e022f8ef0a8e5fd3f56986b2e5bf06df07054e9ea9177996b0a6c27d74d7c', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 201464, u'sha256': u'43f40dd5140804309a4c901ec3c85b54481316e67a6fe18beb9d5c0ce3a42c3a', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 201984, u'sha256': u'f9cb2c13ebaaa826fc9e85033fffe3259f22f28d9cff2d53f9086d2f3bfafaed', u'type': u'MS Windows cursor resource - 2 icons, 32x256, hotspot @1x1', u'size': 34}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 202520, u'sha256': u'01b1735b2f7a0eade419baef8c3558aa38fc873d13ee872816a6bc65af24f542', u'type': u'MS Windows cursor resource - 2 icons, 32x256, hotspot @1x1', u'size': 34}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 202872, u'sha256': u'ec26c438d10e3e84ec855c47f07a176e6c11bbfae1557d526490711b80f087fe', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 203208, u'sha256': u'9c17b4621412d6ded24a76aed74d4425ae61f86b6d4092ca1e28ca66b7c71399', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 253344, u'sha256': u'427476f1323343d3d567002ad5b2c2044c8dd0c51b88d24d396c9f8983ff6fcb', u'type': u'MS Windows icon resource - 5 icons, 255x255', u'size': 76}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 253424, u'sha256': u'74cea2e3966e043f920e03bda7d6ca3bd5587fd87e6ab1dd3fe8f078dfc6a349', u'type': u'data', u'size': 740}

## CERTIFICATE VALIDATION

- UntrustedRoot ✖

| [+] ZLDAYKIB | |
|---|---|
| Status | UntrustedRoot ✖ |
| Start Date | 2019-03-25 19:34:22 |
| End Date | 2040-01-01 01:59:59 |
| Sha256 | a77c6d1f5136abbce2c26f726f727e39405f9fdd397469a69e413cf254bf8e04 |
| Serial | 0B85522BC4725BAB47CE26CC885A8B5E |
| Subject Key Identifier | null |
| Issuer Name | ZLDAYKIB |
| Issuer Key Identifier | 3a d8 3c 8a 8d fe 4e 7c 5b a6 df 18 a4 1a b7 41 |
| Crl link | null |
| Key Usage | null |
| Extended Usage | {"Code Signing (1.3.6.1.5.5.7.3.3)"} |

## SCREENSHOTS