VALKYRIE COMODO

# Summary

**File Name:** aHT0uuO9iQ.exe

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

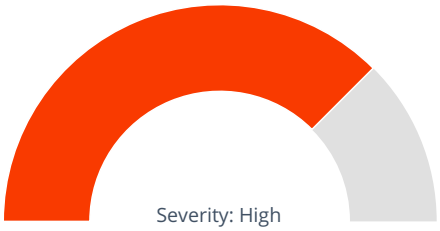
**SHA1:** 9f75d272645b1dbcb6fb63f60ab7873982f13c08

**MD5:** a286f6e999f60d56ce6e7e798d0a5c6d

MALWARE

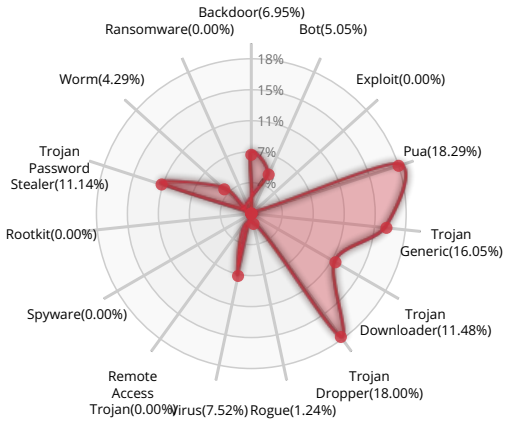
Valkyrie Final Verdict

## DETECTION SECTION

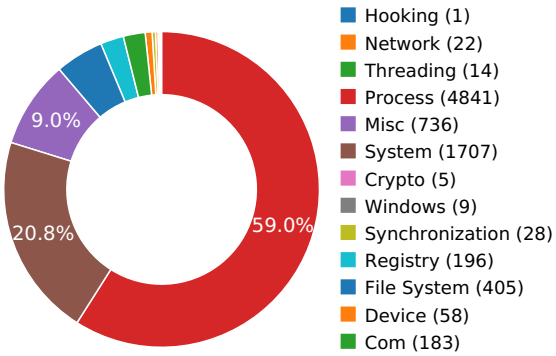



Verdict: Malware

## 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

- Attempts to connect to a dead IP:Port (1 unique times) — Show sources
- HTTP traffic contains suspicious features which may be indicative of malware related traffic — Show sources
- Performs some HTTP requests — 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

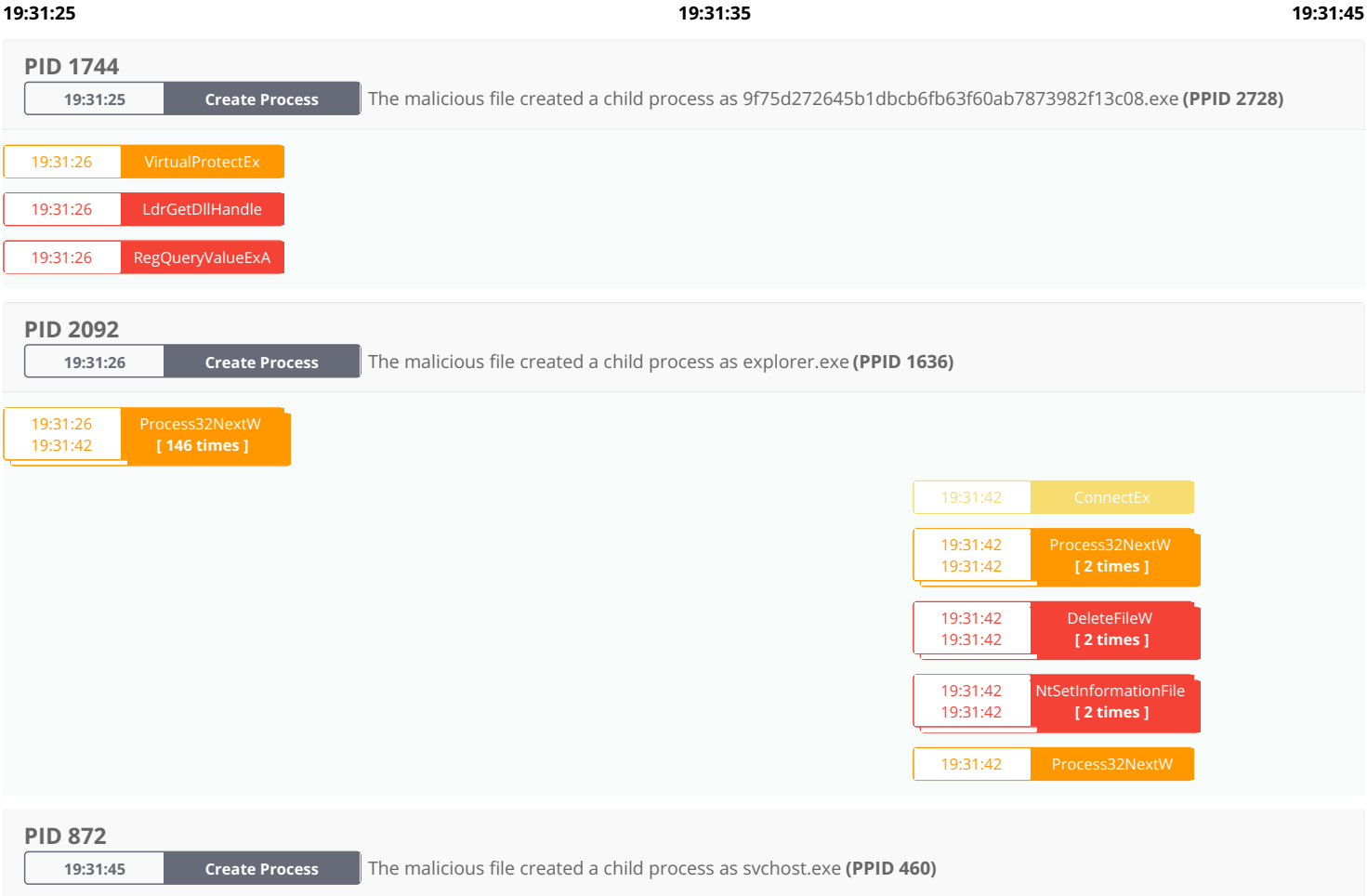
- Deletes its original binary from disk — Show sources
- Installs itself for autorun at Windows startup — Show sources
- Creates a copy of itself — Show sources

## MALWARE ANALYSIS SYSTEM EVASION

- Detects Sandboxie through the presence of a library — Show sources
- Checks the presence of disk drives in the registry, possibly for anti-virtualization — Show sources
- Creates a hidden or system file — Show sources

VALKYRIE COMODO

## Behavior Graph



VALKYRIE COMODO

## Behavior Summary

### ACCESSED FILES

| |
|---|
| C:\Users\user\AppData\Local\Temp\msvcr100.dll |
| C:\Windows\System32\msvcr100.dll |
| C:\Windows\system\msvcr100.dll |
| C:\Windows\msvcr100.dll |
| C:\ProgramData\Oracle\Java\javapath\msvcr100.dll |
| C:\Windows\System32\wbem\msvcr100.dll |
| C:\Windows\System32\WindowsPowerShell\v1.0\msvcr100.dll |
| C:\Program Files\Microsoft Network Monitor 3\msvcr100.dll |
| C:\Program Files (x86)\Universal Extractor\msvcr100.dll |
| C:\Program Files (x86)\Universal Extractor\bin\msvcr100.dll |
| C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\msvcr100.dll |
| C:\Python27\msvcr100.dll |
| C:\Python27\Scripts\msvcr100.dll |
| C:\tools\sysinternals\msvcr100.dll |
| C:\tools\msvcr100.dll |
| C:\tools\IDA_Pro_v6\python\msvcr100.dll |
| C:\ |
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| C:\Windows\winhttp.DLL |
| C:\Windows\sysnative\winhttp.dll |
| C:\Windows\webio.dll |
| C:\Windows\sysnative\webio.dll |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv\cafadrev.exe |
| C:\Users\user\AppData\Local\Temp\9f75d272645b1dbcb6fb63f60ab7873982f13c08.exe |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv\cafadrev.exe:Zone.Identifier |
| C:\Windows\sysnative\advapi32.dll |
| C:\Windows |
| C:\Windows\sysnative |
| C:\Windows\sysnative\cmd.exe |
| C:\Windows\sysnative\ |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\iddbdbdv.lnk |

| |
|---|
| C:\Windows\sysnative\Tasks |
| C:\Windows\sysnative\Tasks* |
| C:\Windows\sysnative\Tasks\GoogleUpdateTaskMachineCore |
| C:\Windows\sysnative\Tasks\Opera scheduled Autoupdate 772857709 |
| C:\Windows\Tasks\Opera scheduled Autoupdate 772857709.job |
| C:\Windows\sysnative\Tasks\ |
| \??\PIPE\srvsvc |
| C:\DosDevices\pipe\ |
| \Device\LanmanDatagramReceiver |

## READ REGISTRY KEYS

| |
|---|
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\0 |
| 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\CurrentVersion\Group Policy\History\NetworkName |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32\(Default) |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32\LoadWithoutCOM |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}\SortOrderIndex |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\SortOrderIndex |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\svcVersion |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\GoogleUpdateTaskMachineCore\Id |
| HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Control Panel\International\LocaleName |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\SchedulingEngineKnob |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\Hash |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\DynamicInfo |
| HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\SecurityService\DefaultAuthLevel |

## MODIFIED FILES

| |
|---|
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv\cafadrev.exe |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\iddbdbdv.lnk |
| C:\Windows\sysnative\Tasks\Opera scheduled Autoupdate 772857709 |
| \??\PIPE\srvsvc |
| \Device\LanmanDatagramReceiver |

## RESOLVED APIS

| |
|---|
| kernel32.dll.FlsAlloc |
| kernel32.dll.FlsGetValue |
| kernel32.dll.FlsSetValue |
| kernel32.dll.FlsFree |
| kernel32.dll.IsProcessorFeaturePresent |
| uxtheme.dll.ThemeInitApiHook |
| user32.dll.IsProcessDPIAware |
| kernel32.dll.LoadLibraryA |
| kernel32.dll.VirtualAlloc |
| kernel32.dll.VirtualProtect |
| kernel32.dll.VirtualFree |
| kernel32.dll.GetVersionExA |
| kernel32.dll.TerminateProcess |
| kernel32.dll.SortGetHandle |
| kernel32.dll.SortCloseHandle |
| kernel32.dll.CloseHandle |
| user32.dll.SetPropA |
| ntdll.dll.RtlExitUserThread |
| ole32.dll.CoInitializeEx |
| advapi32.dll.RegDeleteTreeA |
| advapi32.dll.RegDeleteTreeW |
| ole32.dll.CoTaskMemAlloc |
| ole32.dll.StringFromIID |
| nsi.dll.NsiAllocateAndGetTable |
| cfgmgr32.dll.CM_Open_Class_Key_ExW |
| iphlpapi.dll.ConvertInterfaceGuidToLuid |
| iphlpapi.dll.GetIfEntry2 |

| |
|---|
| iphlpapi.dll.GetIpForwardTable2 |
| iphlpapi.dll.GetIpNetEntry2 |
| iphlpapi.dll.FreeMibTable |
| ole32.dll.CoTaskMemFree |
| nsi.dll.NsiFreeTable |
| ole32.dll.CoUninitialize |
| shlwapi.dll.StrCmpNW |
| ws2_32.dll.GetAddrInfoW |
| ws2_32.dll.WSASocketW |
| ws2_32.dll.#2 |
| ws2_32.dll.#21 |
| ws2_32.dll.#9 |
| ws2_32.dll.WSAIoctl |
| ws2_32.dll.FreeAddrInfoW |
| ws2_32.dll.#6 |
| ws2_32.dll.#5 |
| ws2_32.dll.WSARecv |
| ws2_32.dll.WSASend |
| cryptsp.dll.CryptHashData |
| cryptsp.dll.CryptGetHashParam |
| cryptsp.dll.CryptDestroyHash |
| cryptsp.dll.CryptReleaseContext |
| linkinfo.dll.CreateLinkInfoW |
| user32.dll.IsCharAlphaW |
| user32.dll.CharPrevW |
| ntshrui.dll.GetNetResourceFromLocalPathW |
| shlwapi.dll.PathRemoveFileSpecW |
| linkinfo.dll.DestroyLinkInfo |
| oleaut32.dll.#9 |

## DELETED FILES

| |
|---|
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv\cafadrev.exe |
| C:\Users\user\AppData\Local\Temp\9f75d272645b1dbcb6fb63f60ab7873982f13c08.exe |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv\cafadrev.exe:Zone.Identifier |
| C:\Windows\Tasks\Opera scheduled Autoupdate 772857709.job |

C:\Windows\sysnative\Tasks\Opera scheduled Autoupdate 772857709

## DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\Opera scheduled Autoupdate 772857709.job

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\Opera scheduled Autoupdate 772857709.job.fp

## REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\Enum

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\0

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\CurrentVersion\Group Policy\History

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History\NetworkName

HKEY_CLASSES_ROOT\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32\LoadWithoutCOM

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{7007ACC7-3202-11D1-AAD2-00805FC1270E}

HKEY_CLASSES_ROOT\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}\SortOrderIndex

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{21EC2020-3AEA-1069-A2DD-08002B30309D}

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{21EC2020-3AEA-1069-A2DD-08002B30309D}

HKEY_CLASSES_ROOT\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\SortOrderIndex

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace\{7007ACC7-3202-11D1-AAD2-00805FC1270E}

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace\{7007ACC7-3202-11D1-AAD2-00805FC1270E}

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\svcVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}

HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision

| |
|---|
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays |
| 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\WBEM\CIMOM\RepositoryRestoreInProgress |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\GoogleUpdateTaskMachineCore |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\GoogleUpdateTaskMachineCore\Id |
| HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000 |
| HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Control Panel\International |
| HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Control Panel\International\LocaleName |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Opera scheduled Autoupdate 772857709 |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\Opera scheduled Autoupdate 772857709.job |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\Opera scheduled Autoupdate 772857709.job.fp |
| HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SQMClient\Windows |
| HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\Dynamic DST |
| HKEY_LOCAL_MACHINE |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\SchedulingEngineKnob |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\Path |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\Hash |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Opera scheduled Autoupdate 772857709\Id |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Opera scheduled Autoupdate 772857709\Index |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\Triggers |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32} |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\DynamicInfo |
| HKEY_LOCAL_MACHINE\system\Setup |
| HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\SecurityService |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\SecurityService\DefaultAuthLevel |

## READ FILES

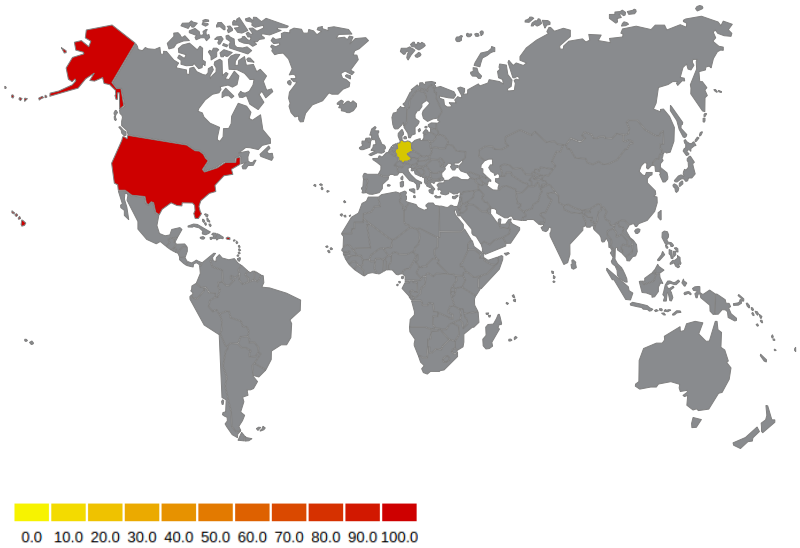
| |
|---|
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| C:\Windows\sysnative\winhttp.dll |
| C:\Windows\sysnative\webio.dll |
| C:\Users\user\AppData\Local\Temp\9f75d272645b1dbcb6fb63f60ab7873982f13c08.exe |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv\cafadrev.exe |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\iddbdbdv |
| C:\ |
| C:\Windows |
| C:\Windows\sysnative |
| C:\Windows\sysnative\cmd.exe |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\iddbdbdv.lnk |
| C:\Windows\sysnative\Tasks\Opera scheduled Autoupdate 772857709 |
| \??\PIPE\srvsvc |
| \Device\LanmanDatagramReceiver |

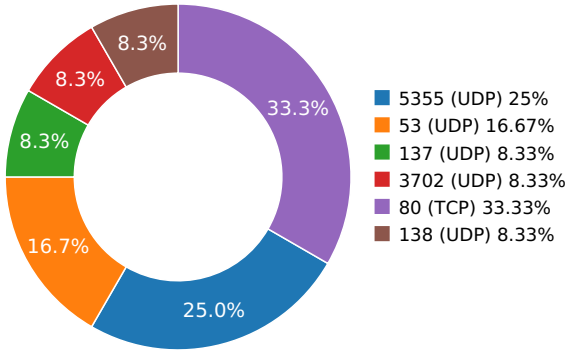
## MODIFIED REGISTRY KEYS

| |
|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\Path |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\Hash |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Opera scheduled Autoupdate 772857709\Id |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Opera scheduled Autoupdate 772857709\Index |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\Triggers |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{060EC885-1638-48E2-9D94-DB306C0FAA32}\DynamicInfo |

## Network Behavior

| CONTACTED IPS | NETWORK PORT DISTRIBUTION |
|---|---|




| Name | IP | Country | ASN | ASN Name | Trigger Process Type |
|---|---|---|---|---|---|
| | 139.59.208.246 | Germany | 14061 | DigitalOcean, LLC | Malware Process |
| | 8.8.4.4 | United States | 15169 | Level 3 Parent, LLC | Malware Process |
| | 23.67.250.184 | United States | 20940 | Akamai Technologies, Inc. | Malware Process |
| | 47.74.235.198 | Singapore | 45102 | Alibaba.com LLC | Malware Process |
| | 23.67.250.154 | | 20940 | Akamai Technologies, Inc. | Malware Process |

### HTTP PACKETS

| Host | Port | Method | Version | User Agent | Count | Call Time During Execution(Sec) |
|---|---|---|---|---|---|---|
| www.msftncsi.com | 80 | GET | 1.1 | Mozilla/4.0 (compatible; MSI... | 1 | 26.0195441246 |
| **Path:** /ncsi.txt<br>**URI:** http://www.msftncsi.com/ncsi.txt | | | | | | |
| connectionfailed.bit | 80 | POST | 1.1 | Mozilla/4.0 (compatible; MSI... | 1 | 33.1671309471 |
| **Path:** /<br>**URI:** http://connectionfailed.bit/ | | | | | | |

## DNS QUERIES

| Request | Type |
|---|---|
| www.msftncsi.com | A |
| **Answers**<br>- 23.67.250.184 (A)<br>- 23.67.250.154 (A)<br>- www.msftncsi.com.edgesuite.net (CNAME)<br>- a1961.g2.akamai.net (CNAME) | |
| connectionfailed.bit | A |
| **Answers**<br>- 47.74.235.198 (A) | |

## TCP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 26.0195441246 | Sandbox | 23.67.250.184 | 80 |
| 33.1671309471 | Sandbox | 47.74.235.198 | 80 |

## UDP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 6.96763205528 | Sandbox | 224.0.0.252 | 5355 |
| 6.97456097603 | Sandbox | 192.168.56.255 | 137 |
| 7.17297911644 | Sandbox | 224.0.0.252 | 5355 |
| 7.17685008049 | Sandbox | 239.255.255.250 | 3702 |
| 9.72813200951 | Sandbox | 224.0.0.252 | 5355 |
| 12.975908041 | Sandbox | 192.168.56.255 | 138 |
| 25.8954460621 | Sandbox | 8.8.4.4 | 53 |
| 32.7731409073 | Sandbox | 139.59.208.246 | 53 |

VALKYRIE COMODO

DETAILED FILE INFO

## CREATED / DROPPED FILES

| FILE PATH | TYPE AND HASHES |
|---|---|
| **C:\Windows\Sysnative\Tasks\Opera Scheduled Autoupdate 772857709** | **Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators<br>**MD5 :** b1e389541256a7510ba57dd4a32c61e8<br>**SHA-1 :** f6c2a3fc6109a5446e2e6d47702a915551c15cef<br>**SHA-256 :** 7e23e23086c6da773dfd3aca5c3aaca56d5a07de<br>**SHA-512 :** 8fd6058d79faa3fffc5c68756dddd041ad31e983d<br>**Size :** 3.578 Kilobytes. |
| **C:\Users\User\AppData\Roaming\Microsoft\Windows\Iddbdbdv\Cafadrev.Exe** | **Type :** PE32 executable (GUI) Intel 80386, for MS Windows<br>**MD5 :** a286f6e999f60d56ce6e7e798d0a5c6d<br>**SHA-1 :** 9f75d272645b1dbcb6fb63f60ab7873982f13c08<br>**SHA-256 :** e19f82571c387673b103368b2b57bfa6a7d83a4a<br>**SHA-512 :** 05c4a9cb39712943b9ca41ba27f4d8ee4688644<br>**Size :** 254.976 Kilobytes. |
| **C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Iddbdbdv.Lnk** | **Type :** MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has command line arguments, Archive, ctime=Sun Nov 21 00:23:55 2010, mtime=Sun Nov 21 00:23:55 2010, atime=Sun Nov 21 00:23:55 2010, length=345088, window=hide<br>**MD5 :** 83bc8b8c09dcaf6bf7c249561ad75f5c<br>**SHA-1 :** 5e7ae4b8bd441b7a2571878c416c3bb14bf09846<br>**SHA-256 :** eab1c20cf7ba2c86de72dc083075ea257d9879c3<br>**SHA-512 :** 1ad1e5bbbbba1e956b42057ff4cdefe8ad6c9472<br>**Size :** 1.014 Kilobytes. |

## MATCH YARA RULES

| MATCH RULES |
|---|

## STATIC FILE INFO

| | |
|---|---|
| **File Name:** | aHT0uuO9iQ.exe |
| **File Type:** | PE32 executable (GUI) Intel 80386, for MS Windows |
| **SHA1:** | 9f75d272645b1dbcb6fb63f60ab7873982f13c08 |
| **MD5:** | a286f6e999f60d56ce6e7e798d0a5c6d |
| **First Seen Date:** | 2018-05-18 15:49:33.066936 ( 10 months ago ) |
| **Number Of Clients Seen:** | 8 |
| **Last Analysis Date:** | 2018-05-21 08:01:14.504904 ( 10 months ago ) |
| **Human Expert Analysis Result:** | No human expert analysis verdict given to this sample yet. |

VALKYRIE COMODO

DETAILED FILE INFO

## ADDITIONAL FILE INFORMATION

### PE Headers

| PROPERTY | VALUE |
|---|---|
| Magic Literal Enum | 3 |
| File Type Enum | 6 |
| Debug Artifacts | [] |
| Number Of Sections | 5 |
| Trid | [] |
| Compilation Time Stamp | 0x5AFD4D4E [Thu May 17 09:37:18 2018 UTC] |
| Entry Point | 0x40513e (.text) |
| Machine Type | Intel 386 or later - 32Bit |
| File Size | 254976 |
| Ssdeep | |
| Sha256 | e19f82571c387673b103368b2b57bfa6a7d83a4afa25c924b5d0938ccad86c29 |
| Exifinfo | [] |
| Mime Type | application/x-dosexec |
| Imphash | |

### PE Sections

| NAME | VIRTUAL ADDRESS | VIRTUAL SIZE | RAW SIZE | ENTROPY | MD5 |
|---|---|---|---|---|---|
| .text | 0x1000 | 0x14ee0 | 0x15000 | 6.67246588923 | c9debe359308c765213bb828d5107128 |
| .rdata | 0x16000 | 0x4262 | 0x4400 | 5.20621861098 | 20b906664235dd553aee7712d83377c4 |
| .data | 0x1b000 | 0x765ddc | 0x1e00 | 3.24698457662 | fb317736475842f2efb9b3401834a44a |
| .rsrc | 0x781000 | 0x1c52a | 0x1c600 | 7.19460331807 | 1693713ca79f46f73d77c5d1e550c1bc |
| .reloc | 0x79e000 | 0x66f6 | 0x6800 | 1.73561483299 | 233f61e93ea62ae30155cfb36c8def73 |

### PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'KVG', u'offset': 7870672, u'sha256': u'f779806ac8e7b68f92b9f79667a90a67c298b925c213e472ea0ffb73e837dd5a', u'type': u'data', u'size': 34094}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 7904768, u'sha256': u'126cb3a102e1dcb93500d9132ced9c64fdc808c504c0c7da62ee5eb42575a12f', u'type': u'data', u'size': 28228}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 7932996, u'sha256': u'2db0fd864c7c01e292da234522a6151c128d997e07816a1ab0dc2669544628c6', u'type': u'data', u'size': 24928}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 7957924, u'sha256': u'81d97f93d42ec4feef032ca047e6e84ba3f91a358a7fd17d09d3283b8b6fd483', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 7961676, u'sha256': u'2e723aed9db946f6588f6b7a21c7a98bd4cb8ef6b554d5812f97d81716977859', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 7963412, u'sha256': u'ab345056f86bcbbc589a21c50c3c677484ba0c3e3e76461778551a608073d4f3', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 7964796, u'sha256': u'07d282f98236dcbd5a7ba6c54c4ed599b8398ac8328f132573c9a168a8da1b9f', u'type': u'dBase III DBT, version number 0, next free block index

40', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 7974436, u'sha256': u'56dc01af0181482e684a33203c1b7a3288ad51eeee6b73cadae20b546048e39f', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 7976876, u'sha256': u'ba636988da4592ca7ee87f25a9a66516220d2cd18e567d821b32e773132c13da', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7978004, u'sha256': u'e1f9ed40d571ab2e9105adb27330f62580946aa56824778ee1130d6b03dc51dd', u'type': u'data', u'size': 104}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7978108, u'sha256': u'bb9028f29fc41bbeafcf5c5280794c8bccc753bb89586c0ea4bca9ed409973e4', u'type': u'data', u'size': 92}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7978200, u'sha256': u'd399a274137c9ef078b6675659d379976ed9c02e705e8c55173ee41599e69f93', u'type': u'data', u'size': 346}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7978548, u'sha256': u'34faed0a1a8911c42465d300605435c1583a7f0cd1ad1064d3716145ea22666d', u'type': u'data', u'size': 672}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7979220, u'sha256': u'b2beade9f565107c87ecb0bff04d6ed59bc24cb49f1bb91954951dc6eb60af17', u'type': u'data', u'size': 192}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7979412, u'sha256': u'da5b48fb48c10edadbf37771433b1b4969f0510249e47d9b2d1c943d90eba155', u'type': u'data', u'size': 182}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7979596, u'sha256': u'348998425d60ef5d090fb6f425096a15a8b94994d64cc8e64ed6f5fbf86a7f5f', u'type': u'data', u'size': 90}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7979688, u'sha256': u'b4d8fb530bc4efba02b3c905f42ee32370c83a3a8416cf6b17ff6d622e81e8ae', u'type': u'data', u'size': 202}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7979892, u'sha256': u'34aad75784b7648fc95cf9e0ffe91d4c74d31ddb41e4c29f7666429075cf9c27', u'type': u'data', u'size': 44}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7979936, u'sha256': u'f97bc740e4d07e7398559a0bac709cfe5fc0a36db8aca9910209d4081cc23a2e', u'type': u'data', u'size': 214}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7980152, u'sha256': u'278840ab1daf10c6041d1e739381fcedf1602c44ec0010d95365fcf1d880aef6', u'type': u'data', u'size': 92}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7980244, u'sha256': u'7b5491b2136567efab32902b1c8efd47aab7c5400f57a2e8a512187b0dcdfb11', u'type': u'data', u'size': 262}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7980508, u'sha256': u'37a178492b4794a9316a68a9d2fa362105524e5a00a91c8199026efd574c346c', u'type': u'data', u'size': 266}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7980776, u'sha256': u'36163c2b9f6f7fd8e9d600d446455463c7658f697e935097a0356e7e4bf50100', u'type': u'data', u'size': 152}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7980928, u'sha256': u'c531592bae31fd38510c03219f4a1e966c23c7f6f71d1ebe291d84934fc5c11a', u'type': u'data', u'size': 298}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7981228, u'sha256': u'f612edc24a9c79ce6264be370a5cc1d74729ebdae1b3b766279329134dad37bd', u'type': u'data', u'size': 208}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7981436, u'sha256': u'edcf698af34ab4dda8a2a4b3149c2900b9494936de9e728c4406c0b0aaad9221', u'type': u'data', u'size': 66}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7981504, u'sha256': u'c3308e5db3dc92d3c9bfb0cf4dded8dc1b46ec5cea1a271eead9ba567d8a63ed', u'type': u'data', u'size': 338}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7981844, u'sha256': u'e1c4f82aa1307c1adeaa5ecda128e40ccda8218125a2ac55648ddd28fc891789', u'type': u'data', u'size': 222}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7982068, u'sha256': u'2c425784a743bf039284173a45ea182390259320206b6ef7ba3f70b08472fd8b', u'type': u'data', u'size': 170}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7982240, u'sha256': u'a0075def5e6f7b08d1473d74aeee76ac823169d838b632e48b521fe559765e0e', u'type': u'data', u'size': 102}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7982344, u'sha256': u'fccddd6cade095ec8f852d0ac9a710c01944e362bb15ee9c573985c9cac15490', u'type': u'data', u'size': 250}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7982596, u'sha256': u'21155bfbd1a4fa2e2f4823c18733950ce06d6889dee5c527d876f5bcdd5a3c32', u'type': u'data', u'size': 74}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7982672, u'sha256': u'2eeca570a971b547b86049dd9f195e6df3f7b158801dfb8d67c46b05337be66f', u'type': u'data', u'size': 162}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7982836, u'sha256': u'c820e8af046926cfe2ab4407973bffc5fe64b8ead90510ea0e7b5ed2afa86a5e', u'type': u'data', u'size': 44}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7982880, u'sha256': u'7b5e9e303cff45da49f090841cd1eb2512ffbe48380b1c82049690f676669868', u'type': u'data', u'size': 56}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7982936, u'sha256': u'39e65dceaa4d7074aece961470f1edecd096b213d62a0788b4aae93ae45635db', u'type': u'data', u'size': 268}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7983204, u'sha256': u'4e24bb9ec4012bf78a1fbd18a028229dad85864ace478b41103e26a3c16bbe46', u'type': u'data', u'size': 62}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7983268, u'sha256': u'05bfcefc8d196d95b44710fc1dde3b5b6d4c68b18768029d6c2d4812ce95a168', u'type': u'data', u'size': 86}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7983356, u'sha256': u'296b0ddb478baffe4882e02b8c9d33ec4390208d95fdf86974cc23c48305081b', u'type': u'data', u'size': 196}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7983552, u'sha256': u'9e66bf2afc5c9c5f8b3731a8052a385b33933467e20f5aafb94879de20d19fd8', u'type': u'data', u'size': 110}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7983664, u'sha256': u'0a4d57d288728d2f895c5da4a40ca0e637fb423dd32830eff4abbc75acd7f9ad', u'type': u'data', u'size': 280}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7983944, u'sha256': u'316fa00454eba818c57960279eeb17e3a1594a22e532c8e68e02722bbd388a64', u'type': u'data', u'size': 218}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 7984164, u'sha256': u'7057117876cfe86190979ddfeae2fb6178ff6bae9e147a2a1ae60de959884b3d', u'type': u'data', u'size': 172}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 7984336, u'sha256': u'fadd6f9b86396d8627b32a64e4998579d3b98038e5a0687fdda055bb70706fc6', u'type': u'MS Windows icon resource - 6 icons, 48x48', u'size': 90}

## CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

## SCREENSHOTS



Computer
7:31 PM