VALKYRIE COMODO

Summary

File Name: luxxx.exe

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

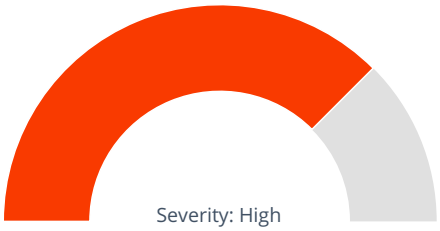
SHA1: 51e5b1e7bf928da55c2654ceefaff3df07a513ef

MD5: 76ba4ab044d1aec759c52282132eefb4

MALWARE

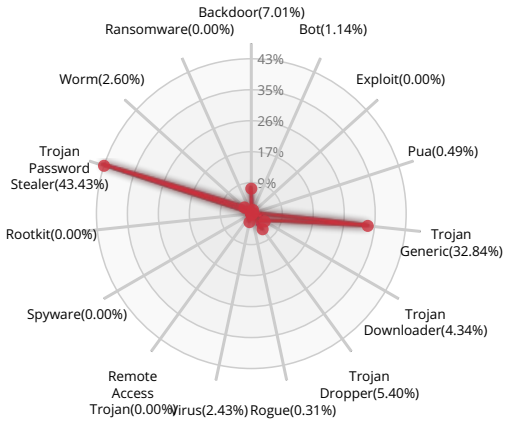
Valkyrie Final Verdict

DETECTION SECTION

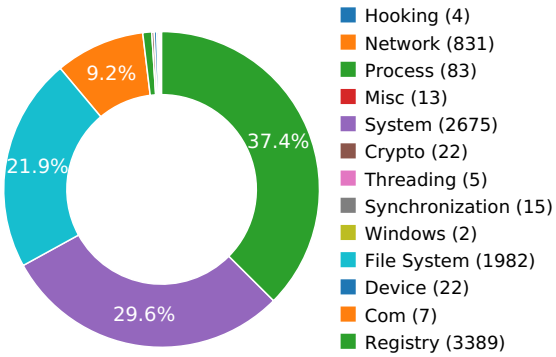


Verdict: Malware

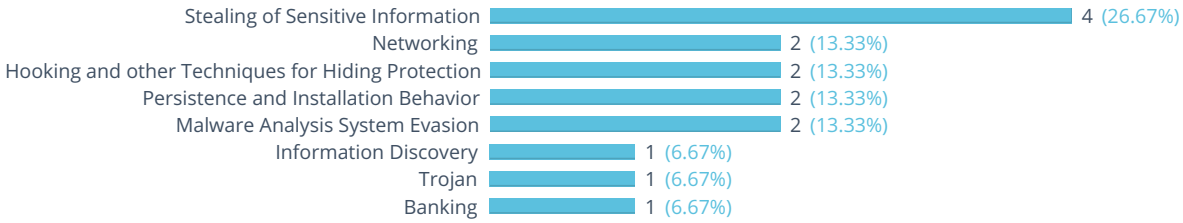
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

TROJAN

Exhibits behavior characteristic of Pony malware	Show sources

NETWORKING

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

STEALING OF SENSITIVE INFORMATION

Steals private information from local Internet browsers	Show sources
Collects information about installed applications	Show sources
Harvests credentials from local FTP client softwares	Show sources
Harvests information related to installed mail clients	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

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

BANKING

Contacts C&C server HTTP check-in (Banking Trojan)	Show sources

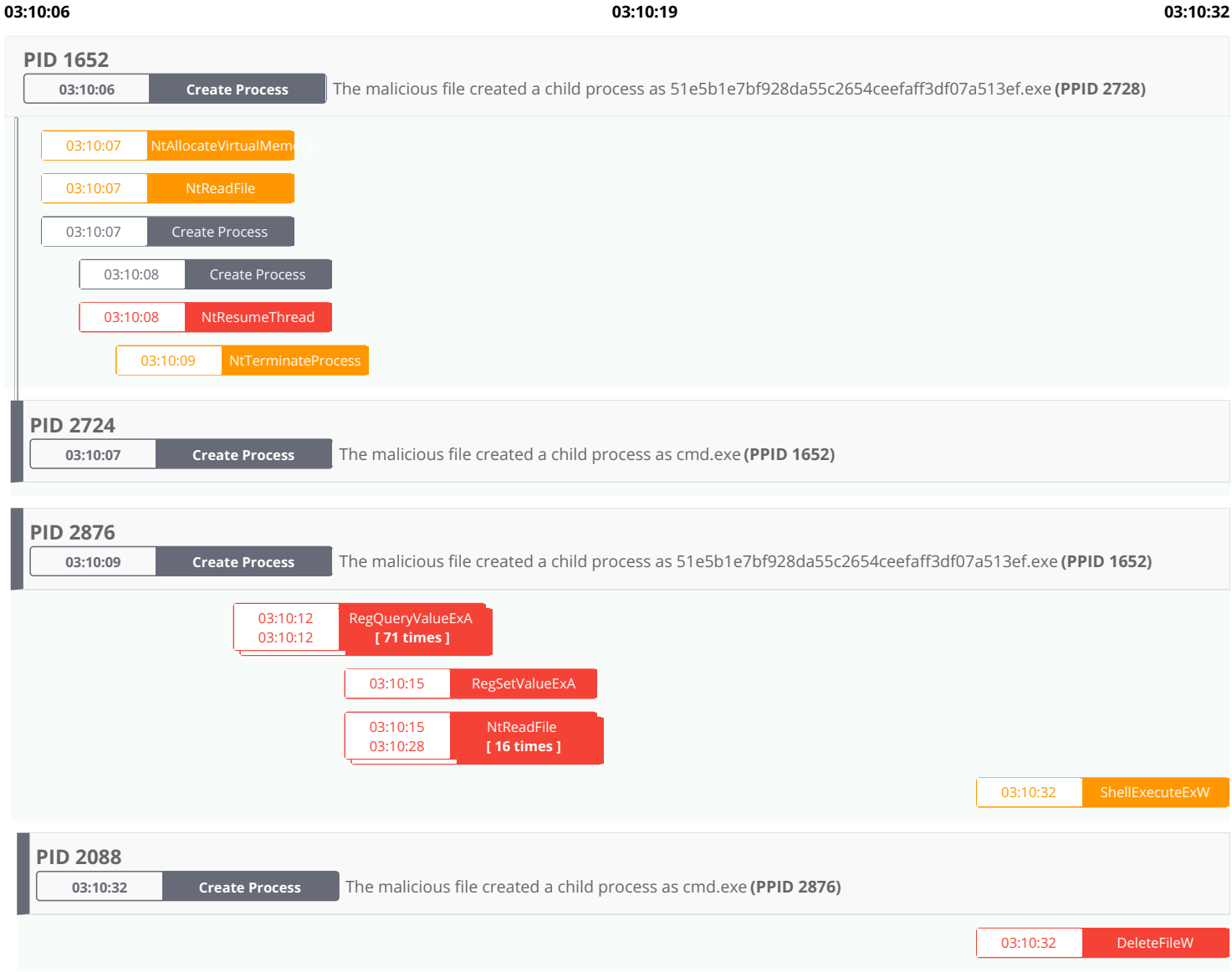
PERSISTENCE AND INSTALLATION BEHAVIOR

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

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time	Show sources
A process created a hidden window	Show sources

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\WindowsShell.Manifest
C:\
C:\Users\user\AppData\Local\Temp\his.dat
C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.exe
C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.ex_
C:\Users\user\AppData\Local\CSIDL_X
C:\Users\user\AppData\Local\CSIDL_
C:\myapp.exe
C:\Windows\explorer.exe\
C:\Users\user\AppData\Local\Temp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\x.vbs
\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\HWID
C:\Windows\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\Windows\wcx_ftp.ini
C:\Users\user\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\Users\user\wcx_ftp.ini
C:\Users\user\AppData\Roaming\GHISLER\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\ProgramData\GHISLER\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\ProgramData\GHISLER\wcx_ftp.ini
C:\Users\user\AppData\Local\GHISLER\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini

C:\Users\user\AppData\Local\GHISLER\wcx_ftp.ini
C:\tools\totalcmdx32\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\tools\totalcmdx32\wcx_ftp.ini
C:\tools\totalcmd\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\tools\totalcmd\wcx_ftp.ini
C:\Windows\win.ini
C:\Program Files (x86)\Common Files\Ipswitch\WS_FTP*.*
C:\Users\user\AppData\Roaming\Ipswitch*.*
C:\ProgramData\Ipswitch*.*
C:\Users\user\AppData\Local\Ipswitch*.*
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP\sm.dat
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP*.*
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Pro*.*
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Lite*.*
C:\Users\user\AppData\Roaming\CuteFTP\sm.dat
C:\Users\user\AppData\Roaming\CuteFTP*.*
C:\ProgramData\GlobalSCAPE\CuteFTP\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP*.*
C:\ProgramData\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP Pro*.*
C:\ProgramData\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP Lite*.*
C:\ProgramData\CuteFTP\sm.dat
C:\ProgramData\CuteFTP*.*
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP\sm.dat
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP*.*
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Pro*.*
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Lite*.*
C:\Users\user\AppData\Local\CuteFTP\sm.dat
C:\Users\user\AppData\Local\CuteFTP*.*
C:\Program Files (x86)\GlobalSCAPE\CuteFTP\sm.dat

C:\Program Files (x86)\GlobalSCAPE\CuteFTP*.*
C:\Program Files (x86)\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Program Files (x86)\GlobalSCAPE\CuteFTP Pro*.*
C:\Program Files (x86)\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Program Files (x86)\GlobalSCAPE\CuteFTP Lite*.*
C:\Program Files (x86)\CuteFTP\sm.dat
C:\Program Files (x86)\CuteFTP*.*
C:\Users\user\AppData\Roaming\FlashFXP\3\Sites.dat
C:\Users\user\AppData\Roaming\FlashFXP\4\Sites.dat

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\PathCompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE40\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IEData\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 46.0.1 (x86 en-US)\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 46.0.1 (x86 en-US)\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PIL-py2.7\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PIL-py2.7\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Universal Extractor_is1\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Universal Extractor_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WIC\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{19A5926D-66E1-46FC-854D-163AA10A52D3}\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{19A5926D-66E1-46FC-854D-163AA10A52D3}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{1F5C7BAE-1E1A-7C93-1B90-84CE308AFC1C}\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{1F5C7BAE-1E1A-7C93-1B90-84CE308AFC1C}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{26A24AE4-039D-4CA4-87B4-2F83218091F0}\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{26A24AE4-039D-4CA4-87B4-2F83218091F0}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{29D3773E-54F4-23C2-D523-236A4453B845}_is1\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{29D3773E-54F4-23C2-D523-236A4453B845}_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{34B86C7D-4103-201B-3A13-03934DB11543}\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{34B86C7D-4103-201B-3A13-03934DB11543}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{37464E70-B0B9-9DFF-649A-CBE169BAD657}\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{37464E70-B0B9-9DFF-649A-CBE169BAD657}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{56AD3004-0B49-967F-F682-B05650B61A78}\UninstallString

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.ex_
C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\x.vbs
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\8104140.bat

RESOLVED APIS

kernel32.dll.IsProcessorFeaturePresent
comctl32.dll.InitCommonControlsEx
dwmapi.dll.DwmIsCompositionEnabled
lpk.dll.LpkEditControl

comctl32.dll.HIMAGELIST_QueryInterface
comctl32.dll.DrawShadowText
comctl32.dll.DrawSizeBox
comctl32.dll.DrawScrollBar
comctl32.dll.SizeBoxHwnd
comctl32.dll.ScrollBar_MouseMove
comctl32.dll.ScrollBar_Menu
comctl32.dll.HandleScrollCmd
comctl32.dll.DetachScrollBars
comctl32.dll.AttachScrollBars
comctl32.dll.CCSetScrollInfo
comctl32.dll.CCGetScrollInfo
comctl32.dll.CCEnableScrollBar
comctl32.dll.QuerySystemGestureStatus
uxtheme.dll.#49
uxtheme.dll.CloseThemeData
kernel32.dll.GetModuleFileNameW
kernel32.dll.CreateFileW
kernel32.dll.VirtualAlloc
kernel32.dll.GetFileSize
kernel32.dll.ReadFile
kernel32.dll.CloseHandle
shell32.dll.SHGetSpecialFolderPathW
kernel32.dll.CopyFileW
kernel32.dll.SetFileAttributesW
kernel32.dll.GetProcAddress
kernel32.dll.GetModuleHandleA
kernel32.dll.GetModuleFileNameA
kernel32.dll.CreateProcessA
kernel32.dll.CreateProcessW
kernel32.dll.OpenMutexA
kernel32.dll.CreateMutexA
kernel32.dll.CreateFileA
kernel32.dll.GetSystemDirectoryA
kernel32.dll.GetSystemDirectoryW

kernel32.dll.MoveFileExW
shell32.dll.SHGetSpecialFolderPathA
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryValueExA
advapi32.dll.RegQueryValueExW
advapi32.dll.RegSetValueExA
advapi32.dll.RegSetValueExW
advapi32.dll.RegCloseKey
kernel32.dll.CreateDirectoryW
kernel32.dll.Sleep
kernel32.dll.GetFileTime
kernel32.dll.SetFileTime
kernel32.dll.DeleteFileW
kernel32.dll.ExitProcess
kernel32.dll.GetTickCount
kernel32.dll.GetCurrentProcess
kernel32.dll.GlobalAlloc
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.EqualSid
advapi32.dll.LookupAccountSidA
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.Process32First
kernel32.dll.Process32Next
kernel32.dll.Module32First
kernel32.dll.Module32Next
ntdll.dll.NtUnmapViewOfSection
kernel32.dll.VirtualAllocEx
kernel32.dll.WriteProcessMemory
kernel32.dll.GetThreadContext
kernel32.dll.SetThreadContext
kernel32.dll.ResumeThread

kernel32.dll.SuspendThread
kernel32.dll.TerminateProcess
ntdll.dll.NtReadVirtualMemory

DELETED FILES

C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.exe
C:\Users\user\AppData\Local\Temp\8104140.bat

REGISTRY KEYS

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\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\PathCompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar

HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE40\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IEData\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 46.0.1 (x86 en-US)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 46.0.1 (x86 en-US)\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 46.0.1 (x86 en-US)\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++\UninstallString

EXECUTED COMMANDS

C:\Windows\system32\cmd.exe /c echo on error resume next:CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.exe",1: >"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\x.vbs"
C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.exe
C:\Users\user\AppData\Local\Temp\8104140.bat "C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.exe"

READ FILES

C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\WindowsShell.Manifest
C:\Users\user\AppData\Local\Temp\his.dat
C:\Users\user\AppData\Local\CSIDL_X
C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.exe
C:\Users\user\AppData\Local\Temp\51e5b1e7bf928da55c2654ceefaff3df07a513ef.ex_
C:\Users\user\AppData\Local\CSIDL_
C:\myapp.exe
\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\HWID

C:\Windows\win.ini
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data-journal
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data-journal
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Users\user\AppData\Local\Temp\Client Hash
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\8104140.bat

MUTEXES

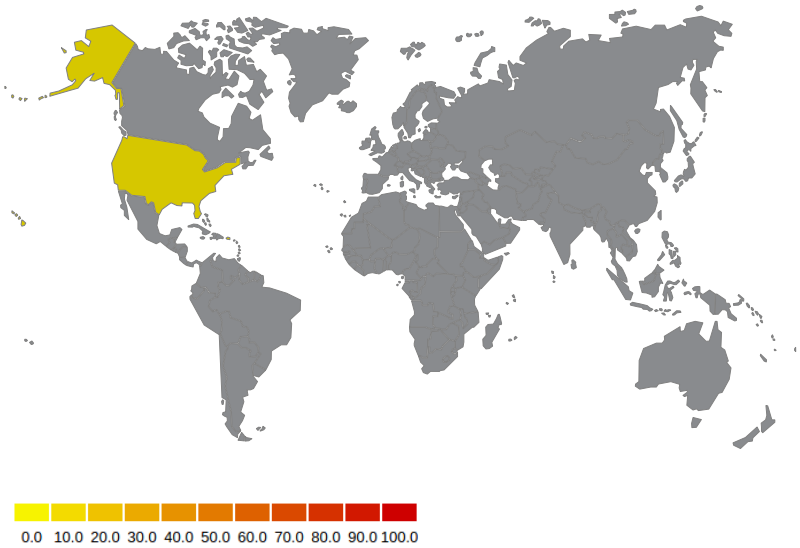
qazwsxedc
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!

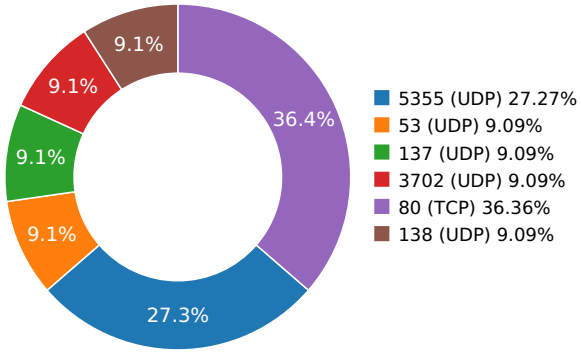
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\WinRAR
HKEY_CURRENT_USER\Software\WinRAR\HWID
HKEY_CURRENT_USER\Software\WinRAR\Client Hash

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 Communications, Inc.	Malware Process
crystaltown-hk.com	5.56.133.98	United States	35017	1 Gbits Com	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
crystaltown-hk.com	80	POST	1.0	Mozilla/4.0 (compatible; MSI...	1	29.8026521206
Path: /gift/luxx/gate.php **URI:** http://crystaltown-hk.com/gift/luxx/gate.php						
crystaltown-hk.com	80	GET	1.0	Mozilla/4.0 (compatible; MSI...	1	30.678508997
Path: /gift/luxx/shit.exe **URI:** http://crystaltown-hk.com/gift/luxx/shit.exe						

DNS QUERIES

Request	Type
crystaltown-hk.com	A
Answers - 5.56.133.98 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
29.8026521206	Sandbox	5.56.133.98	80
30.678508997	Sandbox	5.56.133.98	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.05622220039	Sandbox	224.0.0.252	5355
3.05752205849	Sandbox	224.0.0.252	5355
3.07773399353	Sandbox	239.255.255.250	3702
3.07971119881	Sandbox	192.168.56.255	137
5.61046409607	Sandbox	224.0.0.252	5355
9.0782930851	Sandbox	192.168.56.255	138
29.4537220001	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 645ccdde38bb039eb271a4f120e6be5f **SHA-1 :** 475a264964d84a2c6c335202262fa6c76275a515 **SHA-256 :** a9b45e98f41bfcc23bc82cf17b3381b9820a2be6c **SHA-512 :** 0f5aa71c7c0b1a574c4a6c306a24006ad175e7c8 **Size :** 49.152 Kilobytes.
C:\Users\User\AppData\Local\Temp\8104140.Bat	**Type :** ASCII text, with CRLF, CR line terminators **MD5 :** 3880eeb1c736d853eb13b44898b718ab **SHA-1 :** 4eec9d50360cd815211e3c4e6bdd08271b6ec8e6 **SHA-256 :** 936d9411d5226b7c5a150ecaf422987590a8870c **SHA-512 :** 3eaa3dddd7a11942e75acd44208fbe3d3ff8f400 **Size :** 0.094 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Start up\X.Vbs	**Type :** ASCII text, with CRLF line terminators **MD5 :** f23975e16f2022b9d838d4ead51823c6 **SHA-1 :** 10b793ce151092abf3b0298037fc3f59561d727c **SHA-256 :** 03b89ef34a8c9fb88e6a8d09a4ba4e7016694c0e **SHA-512 :** 8f6726f09f067a63ca0b68f9aba96a1b31ffbca59 **Size :** 0.14 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** de20f795b0ea29cbcb8daf8951530db4 **SHA-1 :** 81d7e8a0197a0ea9eba76e4dc856d10aa5ec04d9 **SHA-256 :** f891c989c74d22028cc0dfcd564c186fe6857592c **SHA-512 :** 06ed0fdb0abfcdbc16a7f5adb92ed0c59ba788f08 **Size :** 180.224 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 2ed7b584633888df7f0114fa4ac6dc69 **SHA-1 :** fa8067b3241b8d9258d9fc88f5bd80fca5433b10 **SHA-256 :** 69a0d29dc846c82d785231dbf94e4c4b731ad58 **SHA-512 :** 678165bd37def22a10615aded1384e97413fce1f **Size :** 32.768 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	luxxx.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	51e5b1e7bf928da55c2654ceefaff3df07a513ef
MD5:	76ba4ab044d1aec759c52282132eefb4
First Seen Date:	2017-04-13 11:52:44.604765 (2 years ago)
Number Of Clients Seen:	6
Last Analysis Date:	2017-04-13 11:52:44.604765 (2 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	4
Compilation Time Stamp	0x58E0AC1E [Sun Apr 2 07:45:34 2017 UTC]
LegalCopyright	(C) 2003
InternalName	CmbShowHis
FileVersion	1, 0, 0, 1
CompanyName	
PrivateBuild	
LegalTrademarks	
Comments	
ProductName	CmbShowHis
SpecialBuild	
ProductVersion	1, 0, 0, 1
FileDescription	CmbShowHis
OriginalFilename	CmbShowHis.EXE
Translation	0x040e 0x04b0
Entry Point	0x13a9e25 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	355170
Sha256	6f6391e6e2d6d0c0f366094d37665ab06cbfba91cb434df461c48fde96e87ed3
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x22667	0x23000	6.599764	-
.rdata	0x24000	0x8b80	0x9000	5.005100	-
.data	0x2d000	0x8e28	0x5000	3.399323	-
.rsrc	0x36000	0x2478	0x3000	3.887771	-

PE Imports

- KERNEL32.dll
  - FileTimeToLocalFileTime
  - GetTickCount
  - RtlUnwind
  - ExitProcess

- TerminateProcess
- GetCommandLineA
- HeapAlloc
- RaiseException
- HeapReAlloc
- HeapSize
- GetACP
- GetTimeZoneInformation
- LCMapStringA
- LCMapStringW
- UnhandledExceptionFilter
- FreeEnvironmentStringsA
- FreeEnvironmentStringsW
- GetEnvironmentStrings
- GetEnvironmentStringsW
- FileTimeToSystemTime
- GetStdHandle
- GetEnvironmentVariableA
- GetVersionExA
- HeapDestroy
- HeapCreate
- VirtualFree
- IsBadWritePtr
- SetUnhandledExceptionFilter
- GetStringTypeA
- GetStringTypeW
- IsBadReadPtr
- IsBadCodePtr
- SetStdHandle
- CompareStringA
- CompareStringW
- SetEnvironmentVariableA
- SetErrorMode
- GetProfileStringA
- GetFileTime
- GetFileSize
- GetFileAttributesA
- GetOEMCP
- GetCPInfo
- SizeofResource
- GetProcessVersion
- WritePrivateProfileStringA
- GlobalFlags
- TlsGetValue
- LocalReAlloc
- TlsSetValue
- EnterCriticalSection
- GlobalReAlloc
- LeaveCriticalSection
- TlsFree
- GlobalHandle
- DeleteCriticalSection
- TlsAlloc
- InitializeCriticalSection
- LocalAlloc
- MulDiv
- SetLastError
- GetThreadLocale
- GetFullPathNameA
- lstrcpynA
- GetVolumeInformationA
- FindFirstFileA
- FindClose
- SetEndOfFile
- UnlockFile
- LockFile
- FlushFileBuffers
- SetFilePointer
- WriteFile
- ReadFile
- CreateFileA
- GetCurrentProcess
- DuplicateHandle
- GetLastError
- LoadLibraryA

    - FreeLibrary
    - GetVersion
    - lstrcatA
    - GlobalGetAtomNameA
    - GlobalAddAtomA
    - GlobalFindAtomA
    - lstrcpyA
    - GetModuleHandleA
    - GetProcAddress
    - FormatMessageA
    - LocalFree
    - MultiByteToWideChar
    - WideCharToMultiByte
    - lstrlenA
    - InterlockedDecrement
    - InterlockedIncrement
    - GlobalUnlock
    - GlobalFree
    - LockResource
    - FindResourceA
    - LoadResource
    - CloseHandle
    - GlobalLock
    - GlobalAlloc
    - GlobalDeleteAtom
    - lstrcmpA
    - lstrcmpiA
    - GetCurrentThread
    - GetCurrentThreadId
    - GetStartupInfoA
    - VirtualProtect
    - GetModuleFileNameA
    - OpenProcess
    - GetThreadTimes
    - DeleteFileW
    - GetFileType
    - GetSystemTimeAsFileTime
    - HeapFree
    - GetModuleFileNameW
    - CreateFileW
    - SetHandleCount
    - VirtualAlloc
- USER32.dll
    - SetRect
    - GetNextDlgGroupItem
    - MessageBeep
    - DestroyMenu
    - InvalidateRect
    - InflateRect
    - RegisterClipboardFormatA
    - PostThreadMessageA
    - ScreenToClient
    - CopyRect
    - GetTopWindow
    - IsChild
    - GetCapture
    - WinHelpA
    - wsprintfA
    - GetClassInfoA
    - RegisterClassA
    - GetMenu
    - GetMenuItemCount
    - GetSubMenu
    - GetMenuItemID
    - GetWindowTextLengthA
    - GetWindowTextA
    - GetDlgCtrlID
    - CreateWindowExA
    - GetClassLongA
    - SetPropA
    - UnhookWindowsHookEx
    - GetPropA
    - CallWindowProcA
    - RemovePropA
    - DefWindowProcA

- GetMessageTime
- GetMessagePos
- GetForegroundWindow
- CopyAcceleratorTableA
- SetWindowLongA
- PtInRect
- OffsetRect
- IntersectRect
- SystemParametersInfoA
- GetWindowPlacement
- GetWindowRect
- MapDialogRect
- SetWindowPos
- GetWindow
- SetWindowContextHelpId
- EndDialog
- SetActiveWindow
- IsWindow
- CreateDialogIndirectParamA
- GetDlgItem
- GetMenuCheckMarkDimensions
- LoadBitmapA
- GetMenuState
- ModifyMenuA
- SetMenuItemBitmaps
- CheckMenuItem
- EnableMenuItem
- GetFocus
- GetNextDlgTabItem
- GetMessageA
- TranslateMessage
- DispatchMessageA
- GetActiveWindow
- GetKeyState
- CallNextHookEx
- ValidateRect
- IsWindowVisible
- PeekMessageA
- GetCursorPos
- SetWindowsHookExA
- GetParent
- GetLastActivePopup
- LoadIconA
- FindWindowW
- DrawIcon
- UnregisterClassA
- HideCaret
- ShowCaret
- ExcludeUpdateRgn
- DrawFocusRect
- IsWindowEnabled
- GetWindowLongA
- MessageBoxA
- SetCursor
- PostQuitMessage
- PostMessageA
- EnableWindow
- IsIconic
- DefWindowProcW
- CreateWindowExW
- CreateDialogParamW
- GetDoubleClickTime
- CharNextA
- LoadStringA
- GetSysColorBrush
- SetForegroundWindow
- SendMessageA
- GetSystemMetrics
- DefDlgProcA
- IsWindowUnicode
- GetClientRect
- GetClassNameA
- GetDesktopWindow
- LoadCursorA
- GrayStringA

    - DrawTextA
    - TabbedTextOutA
    - EndPaint
    - BeginPaint
    - GetWindowDC
    - ReleaseDC
    - GetDC
    - ClientToScreen
    - CharUpperA
    - ShowWindow
    - MoveWindow
    - SetWindowTextA
    - IsDialogMessageA
    - UpdateWindow
    - SendDlgItemMessageA
    - DestroyWindow
    - AdjustWindowRectEx
    - GetSysColor
    - RegisterWindowMessageA
    - SetFocus
    - MapWindowPoints
- GDI32.dll
    - SetBkMode
    - SetMapMode
    - SetViewportOrgEx
    - OffsetViewportOrgEx
    - SetViewportExtEx
    - ScaleViewportExtEx
    - SetWindowExtEx
    - ScaleWindowExtEx
    - DeleteObject
    - GetStockObject
    - GetDeviceCaps
    - GetViewportExtEx
    - GetWindowExtEx
    - CreateSolidBrush
    - PtVisible
    - RectVisible
    - TextOutA
    - ExtTextOutA
    - Escape
    - GetTextColor
    - GetBkColor
    - DPtoLP
    - LPtoDP
    - GetMapMode
    - PatBlt
    - SelectObject
    - RestoreDC
    - SaveDC
    - DeleteDC
    - GetObjectA
    - SetBkColor
    - SetTextColor
    - GetClipBox
    - CreateBitmap
    - Polyline
    - GetCharacterPlacementW
    - CreateDIBitmap
    - GetTextExtentPointA
    - BitBlt
    - CreateCompatibleDC
    - IntersectClipRect
- comdlg32.dll
    - GetFileTitleA
- WINSPOOL.DRV
    - ClosePrinter
    - DocumentPropertiesA
    - OpenPrinterA
- ADVAPI32.dll
    - RegSetValueExA
    - RegOpenKeyExA
    - RegCreateKeyExA
    - RegCloseKey
- COMCTL32.dll

- None
- oledlg.dll
  - None
- ole32.dll
  - CoFreeUnusedLibraries
  - OleInitialize
  - CoTaskMemAlloc
  - CoTaskMemFree
  - CreateILockBytesOnHGlobal
  - StgCreateDocfileOnILockBytes
  - StgOpenStorageOnILockBytes
  - CoGetClassObject
  - CLSIDFromString
  - CLSIDFromProgID
  - CoRegisterMessageFilter
  - CoRevokeClassObject
  - OleFlushClipboard
  - OleIsCurrentClipboard
  - OleUninitialize
- OLEPRO32.DLL
  - None
- OLEAUT32.dll
  - VariantTimeToSystemTime
  - SysAllocStringLen
  - SysFreeString
  - VariantCopy
  - VariantChangeType
  - SysAllocString
  - SysAllocStringByteLen
  - SysStringLen
  - VariantClear

PE Resources

RT_CURSOR
RT_BITMAP
RT_ICON
RT_DIALOG
RT_STRING
RT_GROUP_CURSOR
RT_GROUP_ICON
RT_VERSION

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS