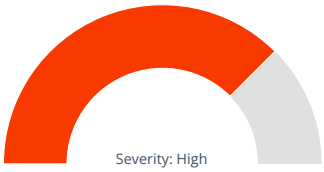
VALKYRIE COMODO

Summary

File Name: virussign.com_5c9bbe8e5b749efba278eabd96c9cbe1.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: 3b48a7ed61ab4ca62ecd8591bfdec38c3cf0493d
MD5: 5c9bbe8e5b749efba278eabd96c9cbe1

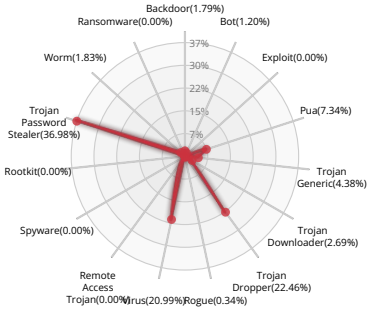
MALWARE
Valkyrie Final Verdict

DETECTION SECTION

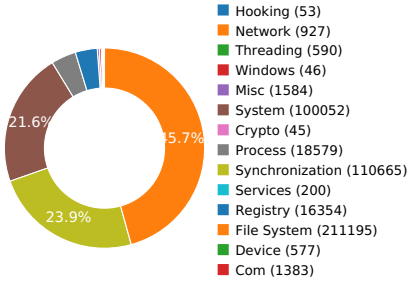


Verdict: Malware

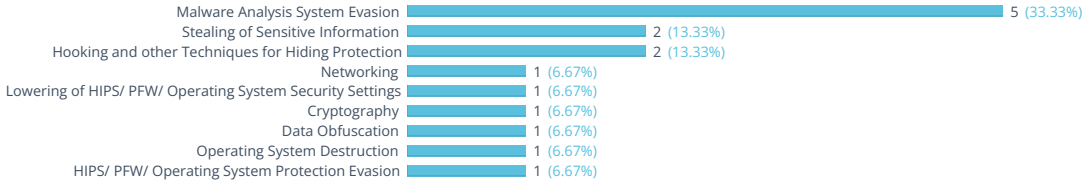
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

Starts servers listening on 127.0.0.1:42424, :0, 0.0.0.0:2002

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys Show sources

CRYPTOGRAPHY

At least one IP Address, Domain, or File Name was found in a crypto call Show sources

STEALING OF SENSITIVE INFORMATION

Sniffs keystrokes Show sources

Steals private information from local Internet browsers Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Likely virus infection of existing system binary Show sources

DATA OBFUSCATION

Drops a binary and executes it Show sources

OPERATING SYSTEM DESTRUCTION

At least one process apparently crashed during execution Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time Show sources

Attempts to identify installed analysis tools by a known file location Show sources

A process attempted to delay the analysis task by a long amount of time. Show sources

Detects VirtualBox through the presence of a file Show sources

Creates a hidden or system file Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory Show sources

VALKYRIE COMODO

Behavior Graph

10:47:34 **10:50:35** **10:53:36**

PID 2652

10:47:34 **Create Process** The malicious file created a child process as 3b48a7ed61ab4ca62ecd8591bfdec38c3cf0493d.exe **(PPID 1480)**

10:47:34 VirtualProtectEx

10:47:34 10:47:34 NtWriteFile **[13 times]**

PID 452

10:47:35 **Create Process** The malicious file created a child process as services.exe **(PPID 348)**

10:47:41 Create Process
10:47:42 Create Process
10:47:43 Create Process
10:47:44 Create Process
10:47:45 Create Process
10:47:47 Create Process
10:47:49 Create Process
10:47:50 Create Process
10:48:40 Create Process
10:48:48 Create Process
10:48:54 Create Process
10:49:01 Create Process
10:49:10 Create Process
10:49:23 Create Process
10:49:34 Create Process
10:49:49 Create Process
10:49:59 Create Process
10:50:01 Create Process
10:50:15 Create Process
10:50:22 Create Process
10:50:31 Create Process
10:50:45 Create Process
10:50:53 Create Process
10:51:02 Create Process
10:51:16 Create Process
10:52:04 Create Process

PID 2472

10:47:42 **Create Process** The malicious file created a child process as alg.exe **(PPID 452)**

10:47:42 10:47:59 NtWriteFile **[249 times]**
10:47:59 10:47:59 NtCreateFile **[2 times]**
10:47:59 10:48:00 NtWriteFile **[11 times]**
10:48:00 NtCreateFile
10:48:00 10:48:00 NtWriteFile **[13 times]**
10:48:00 NtCreateFile
10:48:00 10:48:00 NtWriteFile **[11 times]**
10:48:00 NtCreateFile
10:48:00 10:48:00 FindFirstFileExW **[2 times]**
10:48:00 NtCreateFile
10:48:00 10:48:00 NtWriteFile **[7 times]**
10:48:00 NtCreateFile
10:48:00 NtWriteFile

10:48:00 [7 times]
10:48:00 NtCreateFile
10:48:00 10:48:00 NtWriteFile [12 times]
10:48:01 NtCreateFile
10:48:01 10:48:01 NtWriteFile [12 times]
10:48:01 NtCreateFile
10:48:01 10:48:01 NtWriteFile [12 times]
10:48:01 NtCreateFile
10:48:01 10:48:01 NtWriteFile [12 times]
10:48:01 NtCreateFile
10:48:01 10:48:01 NtWriteFile [12 times]
10:48:01 NtCreateFile
10:48:01 10:48:01 NtWriteFile [11 times]
10:48:01 NtCreateFile
10:48:01 10:48:02 NtWriteFile [12 times]
10:48:02 10:48:02 NtCreateFile [2 times]
10:48:02 10:48:12 NtWriteFile [278 times]
10:48:14 FindFirstFileExW
10:48:14 10:48:40 NtWriteFile [501 times]

PID 904
10:47:43 **Create Process** The malicious file created a child process as aspnet_state.exe **(PPID 452)**

PID 260
10:47:44 **Create Process** The malicious file created a child process as mscorsvw.exe **(PPID 452)**

PID 1992
10:47:45 **Create Process** The malicious file created a child process as mscorsvw.exe **(PPID 452)**

PID 504
10:47:46 **Create Process** The malicious file created a child process as GoogleUpdate.exe **(PPID 452)**

PID 2456
10:47:51 **Create Process** The malicious file created a child process as GoogleUpdate.exe **(PPID 504)**

10:47:56 Create Process
10:47:57 Create Process
10:47:57 Create Process
10:48:02 Create Process
10:48:55 10:51:26 NtWriteFile [136 times]

PID 1164
10:48:04 **Create Process** The malicious file created a child process as GoogleUpdate.exe **(PPID 2456)**

10:51:09 10:51:14 NtReadFile [14 times]

PID 1268
10:49:48 **Create Process** The malicious file created a child process as explorer.exe **(PPID 1164)**

10:53:36 SetWindowsHookExW

PID 1772
10:49:51 **Create Process** The malicious file created a child process as ehtray.exe **(PPID 1268)**

PID 2160
10:48:05 **Create Process** The malicious file created a child process as GoogleCrashHandler.exe **(PPID 2456)**

PID 2576
10:48:05 Create Process The malicious file created a child process as GoogleCrashHandler64.exe **(PPID 2456)**

PID 1864
10:48:12 Create Process The malicious file created a child process as GoogleUpdate.exe **(PPID 2456)**

PID 1764
10:47:48 Create Process The malicious file created a child process as ODSERV.EXE **(PPID 452)**

PID 2868
10:47:51 Create Process The malicious file created a child process as OSE.EXE **(PPID 452)**

PID 3064
10:47:52 Create Process The malicious file created a child process as rpcapd.exe **(PPID 452)**

10:47:53 NtDelayExecution

PID 1896
10:48:57 Create Process The malicious file created a child process as svchost.exe **(PPID 452)**

10:48:58 LdrLoadDll
10:48:58 Create Process

PID 2900
10:48:58 Create Process The malicious file created a child process as WerFault.exe **(PPID 1896)**

PID 1908
10:49:05 Create Process The malicious file created a child process as svchost.exe **(PPID 452)**

10:49:15 RegOpenKeyExW

PID 2744
10:49:11 Create Process The malicious file created a child process as mscorsvw.exe **(PPID 452)**

10:49:12 NtTerminateProcess

PID 1304
10:49:17 Create Process The malicious file created a child process as mscorsvw.exe **(PPID 452)**

PID 3016
10:49:25 Create Process The malicious file created a child process as dllhost.exe **(PPID 452)**

PID 2968
10:49:35 Create Process The malicious file created a child process as ehrecvr.exe **(PPID 452)**

10:49:40 NtDelayExecution

10:50:47
10:50:47 NtSetInformationFile **[2 times]**

PID 2672
10:49:42 Create Process The malicious file created a child process as ehsched.exe **(PPID 452)**

10:49:49 NtDelayExecution

PID 2812
10:49:52 Create Process The malicious file created a child process as FXSSVC.exe **(PPID 452)**

PID 3100
10:50:00 Create Process The malicious file created a child process as taskhost.exe **(PPID 452)**

PID 3216
10:50:02 Create Process The malicious file created a child process as msdtc.exe **(PPID 452)**

PID 3580
10:50:15 Create Process The malicious file created a child process as msiexec.exe **(PPID 452)**

PID 3780
10:50:21 Create Process The malicious file created a child process as svchost.exe **(PPID 452)**

PID 3892

10:50:31 | Create Process | The malicious file created a child process as perfhost.exe **(PPID 452)**

10:50:32 | NtDelayExecution

PID 3108

10:50:48 | Create Process | The malicious file created a child process as Locator.exe **(PPID 452)**

PID 3252

10:50:58 | Create Process | The malicious file created a child process as alg.exe **(PPID 452)**

PID 3416

10:51:12 | Create Process | The malicious file created a child process as snmptrap.exe **(PPID 452)**

PID 852

10:48:00 | Create Process | The malicious file created a child process as svchost.exe **(PPID 452)**

10:48:08 | NtDelayExecution

PID 556

10:49:02 | Create Process | The malicious file created a child process as svchost.exe **(PPID 452)**

10:49:21 | Create Process

10:50:21 | Create Process

PID 568

10:49:20 | Create Process | The malicious file created a child process as WmiPrvSE.exe **(PPID 556)**

PID 3268

10:50:04 | Create Process | The malicious file created a child process as ehrec.exe **(PPID 556)**

PID 1020

10:49:51 | Create Process | The malicious file created a child process as svchost.exe **(PPID 452)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES
C:\Users\user\AppData\Local\Temp\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\sysnative\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\system\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\api-ms-win-core-fibers-l1-1-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\sysnative\wbem\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\sysnative\WindowsPowerShell\v1.0\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\Scripts\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\sysinternals\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-fibers-l1-1-1.DLL
C:\Users\user\AppData\Local\Temp\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\sysnative\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\system\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\api-ms-win-core-localization-l1-2-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\sysnative\wbem\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\sysnative\WindowsPowerShell\v1.0\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-localization-l1-2-1.DLL
C:\Python27\api-ms-win-core-localization-l1-2-1.DLL
C:\Python27\Scripts\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\sysinternals\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\
C:\Users\user\AppData\Roaming\20503a4e5d0020a4.bin
C:\Users\user\AppData\Local\bin\java.dll
C:\Users\user\AppData\Local\jre\bin\java.dll
C:\Windows\sysnative\alg.exe
C:\Windows\sysnative\
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\imageres.dll
C:\Windows\sysnative\imageres.dll
\Device\KsecDD
C:\Windows\Temp
C:\Users\user\AppData\Local\Temp

C:\Windows\sysnative\Tasks\Microsoft\Windows\WDI\ResolutionHost
C:\Windows\sysnative\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
C:\Windows\sysnative\LogFiles\Scm\fb3c354d-297a-4eb2-9b58-090f6361906b
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
C:\Windows\sysnative\config\systemprofile\AppData\Roaming\20503a4e5d0020a4.bin
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework\v4.0.30319\
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
C:\Windows\sysnative\dllhost.exe
C:\Windows\ehome\ehrecvr.exe
C:\Windows\ehome\ehsched.exe
C:\Windows\sysnative\FXSSVC.exe
C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
C:\Program Files (x86)\Google\Update\
C:\Windows\sysnative\msdtc.exe
C:\Windows\sysnative\msiexec.exe
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE12\
C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE
C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\
C:\Windows\SysWOW64\perfhost.exe
C:\Program Files (x86)\WinPcap\rpcapd.exe
C:\Program Files (x86)\WinPcap\
C:\Windows\sysnative\Locator.exe
C:\Windows\sysnative\snmptrap.exe
C:\Windows\sysnative\sppsvc.exe
C:\Windows\sysnative\vds.exe

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\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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 NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\WOW64
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\RequiredPrivileges
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Public
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir (x86)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramW6432Dir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonW6432Dir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18\ProfileImagePath
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local AppData
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\Environment
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\ErrorControl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Tag
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\DependOnService
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\DependOnGroup
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Group
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\WOW64
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Environment
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\ErrorControl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\Tag
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\DependOnService
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\DependOnGroup

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\Group
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\ErrorControl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\Tag
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\DependOnService
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\DependOnGroup
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\Group
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\Start

MODIFIED FILES

C:\Users\user\AppData\Roaming\20503a4e5d0020a4.bin
C:\Windows\sysnative\alg.exe
C:\Windows\sysnative\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
C:\Windows\sysnative\config\systemprofile\AppData\Roaming\20503a4e5d0020a4.bin
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE
C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE
C:\Program Files (x86)\WinPcap\rpcapd.exe
C:\bevevnhfi\bin\execsc.exe
C:\bevevnhfi\bin\fQWmJDsb.exe
C:\bevevnhfi\bin\loader.exe
C:\bevevnhfi\bin\loader_x64.exe
C:\bevevnhfi\bin\yFFKvqC.exe
C:\mctrlc\bin\execsc.exe
C:\mctrlc\bin\FoNQWrug.exe
C:\mctrlc\bin\loader.exe
C:\mctrlc\bin\loader_x64.exe
C:\mctrlc\bin\qyCwoNN.exe
C:\nidguu\bin\execsc.exe
C:\nidguu\bin\loader.exe
C:\nidguu\bin\loader_x64.exe
C:\nidguu\bin\nURNEMUK.exe
C:\nidguu\bin\rhfuTcC.exe
C:\Program Files\7-Zip\7z.exe
C:\Program Files\7-Zip\7zFM.exe
C:\Program Files\7-Zip\7zG.exe
C:\Program Files\7-Zip\Uninstall.exe
C:\Program Files\DVD Maker\DVDMaker.exe
C:\Program Files\Internet Explorer\ieinstal.exe

C:\Program Files\Internet Explorer\ielowutil.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\Program Files\MPC-HC\CrashReporter\sendrpt.exe
C:\Program Files\MPC-HC\mpc-hc64.exe
C:\Program Files\MPC-HC\unins000.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxControl.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDrvInst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxTray.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxWHQLFake.exe
C:\Program Files\Sandboxie\32\SbieSvc.exe
C:\Program Files\Sandboxie\License.exe
C:\Program Files\Sandboxie\SandboxieBITS.exe
C:\Program Files\Sandboxie\SandboxieCrypto.exe
C:\Program Files\Sandboxie\SandboxieDcomLaunch.exe
C:\Program Files\Sandboxie\SandboxieRpcSs.exe
C:\Program Files\Sandboxie\SandboxieWUAU.exe
C:\Program Files\Sandboxie\SbieCtrl.exe
C:\Program Files\Sandboxie\SbieIni.exe
C:\Program Files\Sandboxie\SbieSvc.exe
C:\Program Files\Sandboxie\Start.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\A3DUtility.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroBroker.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32Info.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroTextExtractor.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AdobeCollabSync.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\Eula.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\LogTransport2.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AcrobatUpdater.exe
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\ReaderUpdater.exe
C:\Program Files (x86)\Common Files\Adobe\Updater6\AdobeUpdaterInstallMgr.exe
C:\Program Files (x86)\Common Files\Adobe\Updater6\Adobe_Updater.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE
C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE
C:\Program Files (x86)\Common Files\microsoft shared\EQUATION\EQNEDT32.EXE
C:\Program Files (x86)\Common Files\microsoft shared\ink\mip.exe
C:\Program Files (x86)\Common Files\microsoft shared\ink\pipanel.exe

RESOLVED APIS

user32.dll.wsprintfW
kernel32.dll.GetModuleFileNameW

kernel32.dll.HeapDestroy
kernel32.dll.HeapCreate
kernel32.dll.HeapAlloc
kernel32.dll.HeapFree
kernel32.dll.GetProcAddress
kernel32.dll.GetModuleHandleW
kernel32.dll.WaitForSingleObject
kernel32.dll.GetEnvironmentVariableW
kernel32.dll.GetTempPathW
kernel32.dll.CreateProcessW
kernel32.dll.GetFileAttributesW
kernel32.dll.EnterCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.InitializeCriticalSection
kernel32.dll.GetWindowsDirectoryW
kernel32.dll.GetVolumeInformationW
kernel32.dll.GetComputerNameW
kernel32.dll.LocalFree
kernel32.dll.OpenMutexW
kernel32.dll.CreateMutexW
kernel32.dll.GetCurrentThread
kernel32.dll.GetLogicalDriveStringsW
kernel32.dll.GetDriveTypeW
kernel32.dll.TerminateThread
kernel32.dll.GetCurrentProcessId
kernel32.dll.ProcessIdToSessionId
kernel32.dll.RaiseException
kernel32.dll.RtlCaptureContext
kernel32.dll.RtlLookupFunctionEntry
kernel32.dll.RtlVirtualUnwind
kernel32.dll.IsDebuggerPresent
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.SetUnhandledExceptionFilter
kernel32.dll.TerminateProcess
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.SetLastError
kernel32.dll.GetCurrentThreadId
kernel32.dll.GetACP
kernel32.dll.GetStringTypeW
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.TlsAlloc
kernel32.dll.TlsGetValue
kernel32.dll.TlsSetValue
kernel32.dll.TlsFree
kernel32.dll.GetTickCount
kernel32.dll.FreeLibrary
kernel32.dll.LoadLibraryExW

kernel32.dll.LCMapStringW
kernel32.dll.DeleteCriticalSection
kernel32.dll.IsValidCodePage
kernel32.dll.GetOEMCP
kernel32.dll.GetCPInfo
kernel32.dll.ExitProcess
kernel32.dll.GetModuleHandleExW
kernel32.dll.GetProcessHeap
kernel32.dll.HeapReAlloc
kernel32.dll.FindFirstFileW
kernel32.dll.FindClose
kernel32.dll.FindNextFileW
kernel32.dll.CreateFileW
kernel32.dll.GetFileTime
kernel32.dll.GetFileSizeEx
kernel32.dll.SetFileTime
kernel32.dll.lstrcmpiW
kernel32.dll.GetFileSize
kernel32.dll.WriteFile
kernel32.dll.GetLastError
kernel32.dll.GetCurrentProcess
kernel32.dll.WideCharToMultiByte
kernel32.dll.MultiByteToWideChar
kernel32.dll.SetFilePointerEx
kernel32.dll.ReadFile
kernel32.dll.VirtualFree
kernel32.dll.VirtualAlloc

DELETED FILES

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000000.db
C:\ProgramData\Microsoft\Windows NT\MSFax\Queue\TST4777.tmp
C:\ProgramData\Microsoft\Windows NT\MSFax\TST4A76.tmp
C:\ProgramData\Microsoft\Windows NT\MSFax\TST4BEE.tmp
C:\programdata\microsoft\eHome\mcepg2-0\Blocks.mem
C:\programdata\microsoft\eHome\Counter.mem
C:\programdata\microsoft\eHome\mcepg2-0\Root.mem

DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ASP.NET_4.0.30319\Names\fEZJsTooKvr4dQDIYl6YQ2PuZIGlvBbzJ4V6ELivqNyCAlsxr7SRWDcnLNKhZwTDrImQ9q1sYNZAL9rUgI359tEXE9lQ5e5j2t49w0SB0pGkIN2jtv8CGm
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Update\uid
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Update\old-uid
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\en-US\ndis.sys.mui[MofResourceName]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\monitor.sys[MonitorWMI]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\ndis.sys[MofResourceName]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fax\Receipts\Password

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\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\Software\JavaSoft\Java Runtime Environment
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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 NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\3b48a7ed61ab4ca62ecd8591bfdec38c3cf0493d.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\WOW64

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\RequiredPrivileges
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Public
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Default
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir (x86)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramW6432Dir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonW6432Dir
HKEY_USERS\S-1-5-18
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18\ProfileImagePath
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local AppData
HKEY_USERS\.DEFAULT\Environment
HKEY_USERS\.DEFAULT\Volatile Environment
HKEY_USERS\.DEFAULT\Volatile Environment\0
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ALG\Environment
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\ErrorControl

EXECUTED COMMANDS

C:\Windows\System32\alg.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc
"C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE"
"C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE"
"C:\Program Files (x86)\WinPcap\rpcapd.exe" -d -f "C:\Program Files (x86)\WinPcap\rpcapd.ini"
C:\Windows\System32\svchost.exe -k WerSvcGroup
C:\Windows\system32\svchost.exe -k netsvcs
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
C:\Windows\ehome\ehRecvr.exe
C:\Windows\ehome\ehsched.exe
C:\Windows\system32\fxssvc.exe
C:\Windows\System32\msdtc.exe
C:\Windows\system32\msiexec.exe /V

C:\Windows\System32\svchost.exe -k netsvcs
C:\Windows\SysWow64\perfhost.exe
C:\Windows\system32\locator.exe
C:\Windows\System32\snmptrap.exe
C:\Windows\System32\vds.exe
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe /c
"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /cr
"C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleCrashHandler.exe"
"C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleCrashHandler64.exe"
"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /ua /installsource core
C:\Windows\system32\WerFault.exe -u -p 2472 -s 352
C:\Windows\system32\wbem\wmiprvse.exe -Embedding
C:\Windows\ehome\ehRec.exe -Embedding
C:\Windows\ehome\ehtray.exe /nav:-2

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\sysnative\alg.exe
C:\Windows\Fonts\staticcache.dat
C:\Windows\sysnative\imageres.dll
\Device\KsecDD
C:\Windows\sysnative\LogFiles\Scm\fb3c354d-297a-4eb2-9b58-090f6361906b
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE
C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE
C:\Program Files (x86)\WinPcap\rpcapd.exe
C:\bevevnhfi\bin\execsc.exe
C:\bevevnhfi\bin\fQWmJDsb.exe
C:\bevevnhfi\bin\loader.exe
C:\bevevnhfi\bin\loader_x64.exe
C:\bevevnhfi\bin\yFFKvqC.exe
C:\mctrlc\bin\execsc.exe
C:\mctrlc\bin\FoNQWrug.exe
C:\mctrlc\bin\loader.exe
C:\mctrlc\bin\loader_x64.exe
C:\mctrlc\bin\qyCwoNN.exe
C:\nidguu\bin\execsc.exe
C:\nidguu\bin\loader.exe
C:\nidguu\bin\loader_x64.exe
C:\nidguu\bin\nURNEMUK.exe
C:\nidguu\bin\rhfuTcC.exe
C:\Program Files\7-Zip\7z.exe
C:\Program Files\7-Zip\7zFM.exe
C:\Program Files\7-Zip\7zG.exe
C:\Program Files\7-Zip\Uninstall.exe

C:\Program Files\DVD Maker\DVDMaker.exe
C:\Program Files\Internet Explorer\ieinstal.exe
C:\Program Files\Internet Explorer\ielowutil.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\Program Files\MPC-HC\CrashReporter\sendrpt.exe
C:\Program Files\MPC-HC\mpc-hc64.exe
C:\Program Files\MPC-HC\unins000.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxControl.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDrvInst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxTray.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxWHQLFake.exe
C:\Program Files\Sandboxie\32\SbieSvc.exe
C:\Program Files\Sandboxie\License.exe
C:\Program Files\Sandboxie\SandboxieBITS.exe
C:\Program Files\Sandboxie\SandboxieCrypto.exe
C:\Program Files\Sandboxie\SandboxieDcomLaunch.exe
C:\Program Files\Sandboxie\SandboxieRpcSs.exe
C:\Program Files\Sandboxie\SandboxieWUAU.exe
C:\Program Files\Sandboxie\SbieCtrl.exe
C:\Program Files\Sandboxie\SbieIni.exe
C:\Program Files\Sandboxie\SbieSvc.exe
C:\Program Files\Sandboxie\Start.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\A3DUtility.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroBroker.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32Info.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroTextExtractor.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AdobeCollabSync.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\Eula.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\LogTransport2.exe
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AcrobatUpdater.exe
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\ReaderUpdater.exe
C:\Program Files (x86)\Common Files\Adobe\Updater6\AdobeUpdaterInstallMgr.exe
C:\Program Files (x86)\Common Files\Adobe\Updater6\Adobe_Updater.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE
C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE
C:\Program Files (x86)\Common Files\microsoft shared\EQUATION\EQNEDT32.EXE

MUTEXES

Global\Multiarch.m0yv-20503a4e5d0020a4483a4627-b

Global\Multiarch.m0yv-20503a4e5d0020a4-inf
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\Multiarch.m0yv-20503a4e5d0020a49ea72c54-b
Global\G{D19BAF17-7C87-467E-8D63-6C4B1C836373}
Global\G{B5665124-2B19-40e2-A7BC-B44321E72C4B}
Global\OfficeSourceEngineMutex
Global\G{D0BB2EF1-C183-4cdb-B218-040922092869}
Global\G{6885AE8E-C070-458d-9711-37B9BEAB65F6}
Global\G{66CC0160-ABB3-4066-AE47-1CA6AD5065C8}
Local\WERReportingForProcess2472
Global\\xe5\x88\x90\xc2\x94
http://www.microsoft.com/windowsxp/mediacenter/ehtray.exe/singleinstancemutex
Global\MSDTC_STATS_EVENT
Global\MSDTC_STATS_FILE
Global\CLR_CASOFF_MUTEX
RasPbFile
Global\MCStoreOpen_b4cae1f9a3aead62bebb934ca33cadb730c8d3ed
Global\MCStoreSyncMem_5ea381292eeb3ed3e61dc84a3dbd4d7f59767eca
Global\MCStoreSyncMem_7715dc857070a1523dea43f32f1fe67c1ce58e0b
Global\MCStoreSyncMem_71bdfe29063ac557a4e7b3205ed180408457fcd4
Global\eHome_DbMutex_1
Global__?_c:_programdata_microsoft_ehome_mcepg2-0.db
Global__?_c:_programdata_microsoft_ehome_mcepg2-0.db:x

STARTED SERVICES

WerSvc
aspnet_state
clr_optimization_v4.0.30319_32
clr_optimization_v4.0.30319_64
gupdate
odserv
ose
rpcapd
clr_optimization_v2.0.50727_32
clr_optimization_v2.0.50727_64
COMSysApp
ehRecvr
ehSched
Fax
MSDTC
msiserver
PerfHost
RpcLocator
SNMPTRAP
vds
BITS

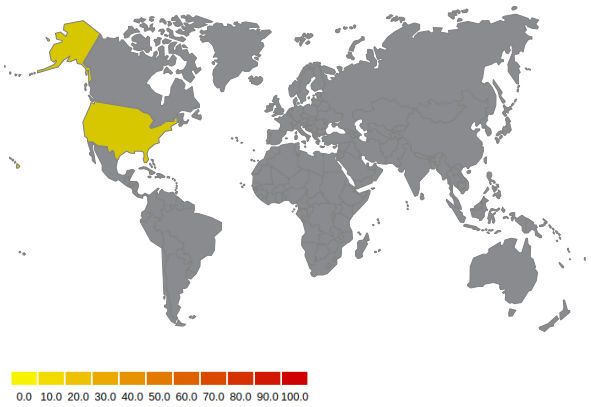
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_state\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_64\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\gupdate\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\gupdate\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\odserv\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\odserv\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ose\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ose\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\rpcapd\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\rpcapd\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WerSvc\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Winmgmt\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_32\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v2.0.50727_64\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\COMSysApp\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\COMSysApp\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ehRecvr\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ehRecvr\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ehRecvr\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ehSched\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ehSched\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ehSched\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Fax\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Fax\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Fax\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\MSDTC\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\MSDTC\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\MSDTC\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\msiserver\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\msiserver\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\BITS\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\PerfHost\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\PerfHost\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\PerfHost\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\RpcLocator\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\RpcLocator\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\RpcLocator\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SNMPTRAP\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SNMPTRAP\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SNMPTRAP\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\vds\Start

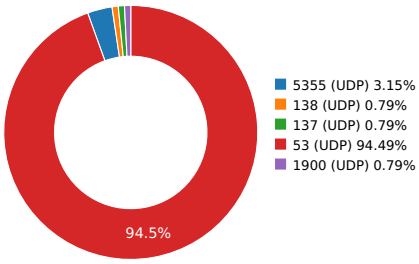
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\vds\Type
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Update\LastCodeRedCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\PreviousServiceShutdown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ProcessID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Update\LastStartedAU
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug\ExceptionRecord
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ThrottleDrege
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Winmgmt\Parameters\ServiceDllUnloadOnStop
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\IDE\DiskVBOX_HARDDISK_____1.0____\5&33d1638a&0&0.0.0_0-{05901221-D566-11d1-B2F0-00A0C9062910}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\advapi32.dll[MofResourceName]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\en-US\advapi32.dll.mui[MofResourceName]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\ACPI.sys[ACPIMOFResource]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\en-US\ACPI.sys.mui[ACPIMOFResource]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\ndis.sys[MofResourceName]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\en-US\ndis.sys.mui[MofResourceName]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\mssmbios.sys[MofResource]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\en-US\mssmbios.sys.mui[MofResource]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\HDAudBus.sys[HDAudioMofName]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\en-US\HDAudBus.sys.mui[HDAudioMofName]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\intelppm.sys[PROCESSORWMI]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\en-US\intelppm.sys.mui[PROCESSORWMI]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\System32\Drivers\portcls.SYS[PortclsMof]

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process
www.aieov.com	173.255.194.134	United States	63949	Akamai Technologies, Inc.	Malware Process
przvgke.biz	172.234.222.138	United States	63949	Akamai Technologies, Inc.	Malware Process
ssbzmoy.biz	18.141.10.107	United States	16509	Amazon Technologies Inc.	Malware Process
npukfztj.biz	44.221.84.105	United States	14618	Amazon.com, Inc.	Malware Process
xlfhhhm.biz	47.129.31.212	Canada	16509	Amazon Technologies Inc.	Malware Process
knjghuig.biz	18.141.10.107	United States	16509	Amazon Technologies Inc.	Malware Process
					Malware Process
lrxdmhrr.biz	54.244.188.177	United States	16509	Amazon Technologies Inc.	Malware Process
deoci.biz	18.208.156.248	United States	14618	Amazon Technologies Inc.	Malware Process
ifsaia.biz	13.251.16.150	Singapore	16509	Amazon Technologies Inc.	Malware Process
gytujflc.biz	208.100.26.245	United States	32748	Steadfast	Malware Process
pywolwnvd.biz	54.244.188.177	United States	16509	Amazon Technologies Inc.	Malware Process
nqwjmb.biz	35.164.78.200	United States	16509	Amazon Technologies Inc.	Malware Process
myups.biz	165.160.13.20	United States	19574	Corporation Service Company	Malware Process
saytjshyf.biz	44.221.84.105	United States	14618	Amazon.com, Inc.	Malware Process
dwrqljrr.biz	54.244.188.177	United States	16509	Amazon Technologies Inc.	Malware Process
lpuegx.biz	82.112.184.197	Russian Federation	43267	"Vysokie tehnologii" LLC, our trademark is...	Malware Process
bumxkqgxu.biz	44.221.84.105	United States	14618	Amazon.com, Inc.	Malware Process
cvgrf.biz	54.244.188.177	United States	16509	Amazon Technologies Inc.	Malware Process
clients2.google.com	142.250.72.110	United States	15169	Google LLC	Malware Process
qaynky.biz	13.251.16.150	Singapore	16509	Amazon Technologies Inc.	Malware Process
vcddkls.biz	18.141.10.107	United States	16509	Amazon Technologies Inc.	Malware Process
yunalwv.biz	208.100.26.245	United States	32748	Steadfast	Malware Process
vjaxhpbji.biz	82.112.184.197	Russian Federation	43267	"Vysokie tehnologii" LLC, our trademark is...	Malware Process
gnqgo.biz	18.208.156.248	United States	14618	Amazon Technologies Inc.	Malware Process
oshhkdluh.biz	54.244.188.177	United States	16509	Amazon Technologies Inc.	Malware Process
tbjrpv.biz	34.246.200.160	Ireland	16509	Amazon Technologies Inc.	Malware Process
					Malware Process
fwiwk.biz	172.234.222.138	United States	63949	Akamai Technologies, Inc.	Malware Process
wllvnzb.biz	18.141.10.107	United States	16509	Amazon Technologies Inc.	Malware Process
jpskm.biz	34.211.97.45	United States	16509	Amazon Technologies Inc.	Malware Process
					Malware Process
ytctnunms.biz	3.94.10.34	United States	14618	Amazon Technologies Inc.	Malware Process

DNS QUERIES

Request	Type
pywolwnvd.biz	A
5isohu.com	A
www.aieov.com	A
ssbzmoy.biz	A
cvgrf.biz	A
npukfztj.biz	A
przvgke.biz	A
zlenh.biz	A
knjghuig.biz	A
uhxqin.biz	A
anpmnmxo.biz	A
lpuegx.biz	A
vjaxhpbji.biz	A
xlfhhhm.biz	A
clients2.google.com	A
ifsaia.biz	A
saytjshyf.biz	A
vcddkls.biz	A
fwiwk.biz	A
tbjrpv.biz	A
deoci.biz	A
gytujflc.biz	A
qaynky.biz	A
bumxkqgxu.biz	A
dwrqljrr.biz	A
nqwjmb.biz	A
ytctnunms.biz	A
myups.biz	A
oshhkdluh.biz	A
yunalwv.biz	A
jpskm.biz	A
lrxdmhrr.biz	A
wllvnzb.biz	A
gnqgo.biz	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.86160182953	Sandbox	224.0.0.252	5355
6.88230895996	Sandbox	224.0.0.252	5355
6.93098378181	Sandbox	192.168.56.255	137
9.48566389084	Sandbox	224.0.0.252	5355
10.9663009644	Sandbox	224.0.0.252	5355
12.930824995	Sandbox	192.168.56.255	138
14.2926478386	Sandbox	8.8.4.4	53
14.3323628902	Sandbox	8.8.4.4	53
15.2907259464	Sandbox	8.8.8.8	53
15.3217439651	Sandbox	8.8.8.8	53
21.540158987	Sandbox	8.8.4.4	53
22.5399038792	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
28.7253479958	Sandbox	8.8.8.8	53
29.7123069763	Sandbox	8.8.4.4	53
33.5414829254	Sandbox	8.8.8.8	53
34.5399768353	Sandbox	8.8.4.4	53
43.1628217697	Sandbox	8.8.8.8	53
44.1517548561	Sandbox	8.8.4.4	53
45.5843608379	Sandbox	8.8.8.8	53
46.5713589191	Sandbox	8.8.4.4	53
57.6996719837	Sandbox	8.8.8.8	53
58.6985118389	Sandbox	8.8.4.4	53
65.9786429405	Sandbox	8.8.8.8	53
66.9775149822	Sandbox	8.8.4.4	53
69.6962668896	Sandbox	8.8.8.8	53
70.6960718632	Sandbox	8.8.4.4	53
80.3785259724	Sandbox	8.8.8.8	53
81.3680708408	Sandbox	8.8.4.4	53
81.8754827976	Sandbox	8.8.8.8	53
82.8687508106	Sandbox	8.8.4.4	53
93.8597178459	Sandbox	8.8.8.8	53
94.7753429413	Sandbox	8.8.8.8	53
94.8522868156	Sandbox	8.8.4.4	53
95.7744259834	Sandbox	8.8.4.4	53
105.853304863	Sandbox	8.8.8.8	53
106.85261488	Sandbox	8.8.4.4	53
113.48483777	Sandbox	8.8.8.8	53
114.477793932	Sandbox	8.8.4.4	53
117.852666855	Sandbox	8.8.8.8	53
118.852603912	Sandbox	8.8.4.4	53
128.555824995	Sandbox	8.8.8.8	53
129.55603981	Sandbox	8.8.4.4	53
129.853142977	Sandbox	8.8.8.8	53
130.853108883	Sandbox	8.8.4.4	53
142.079879999	Sandbox	8.8.8.8	53
143.07138896	Sandbox	8.8.4.4	53
143.982754946	Sandbox	8.8.8.8	53
144.977774858	Sandbox	8.8.4.4	53
148.026662827	Sandbox	239.255.255.250	1900
154.610902786	Sandbox	8.8.4.4	53
155.602822781	Sandbox	8.8.8.8	53
162.461875916	Sandbox	8.8.4.4	53
163.446164846	Sandbox	8.8.8.8	53
166.603461981	Sandbox	8.8.8.8	53
167.602697849	Sandbox	8.8.4.4	53
176.910938978	Sandbox	8.8.8.8	53
177.901262999	Sandbox	8.8.4.4	53
179.01617384	Sandbox	8.8.8.8	53
180.008612871	Sandbox	8.8.4.4	53
191.009494781	Sandbox	8.8.8.8	53
191.718409777	Sandbox	8.8.8.8	53
192.009341002	Sandbox	8.8.4.4	53
192.711774826	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
203.008868933	Sandbox	8.8.8.8	53
204.008887768	Sandbox	8.8.4.4	53
210.899957895	Sandbox	8.8.8.8	53
211.899717808	Sandbox	8.8.4.4	53
215.524902821	Sandbox	8.8.8.8	53
216.52482295	Sandbox	8.8.4.4	53
226.123226881	Sandbox	8.8.8.8	53
227.118155956	Sandbox	8.8.4.4	53
227.524945974	Sandbox	8.8.8.8	53
228.524479866	Sandbox	8.8.4.4	53
235.304423809	Sandbox	8.8.8.8	53
236.290169001	Sandbox	8.8.4.4	53
239.524594784	Sandbox	8.8.8.8	53
240.524698973	Sandbox	8.8.4.4	53
241.179987907	Sandbox	8.8.8.8	53
242.168541908	Sandbox	8.8.4.4	53
251.735282898	Sandbox	8.8.8.8	53
252.72753787	Sandbox	8.8.4.4	53
260.312768936	Sandbox	8.8.8.8	53
261.305489779	Sandbox	8.8.4.4	53
263.727841854	Sandbox	8.8.8.8	53
264.727486849	Sandbox	8.8.4.4	53
275.929643869	Sandbox	8.8.4.4	53
275.929945946	Sandbox	8.8.4.4	53
276.915208817	Sandbox	8.8.8.8	53
276.915313959	Sandbox	8.8.8.8	53
287.916174889	Sandbox	8.8.8.8	53
288.914768934	Sandbox	8.8.4.4	53
291.056865931	Sandbox	8.8.8.8	53
292.056903839	Sandbox	8.8.4.4	53
300.400049925	Sandbox	8.8.8.8	53
301.399253845	Sandbox	8.8.4.4	53
310.705623865	Sandbox	8.8.8.8	53
311.69618392	Sandbox	8.8.4.4	53
312.821573973	Sandbox	8.8.8.8	53
313.821704865	Sandbox	8.8.4.4	53
324.844937801	Sandbox	8.8.8.8	53
325.331443787	Sandbox	8.8.8.8	53
325.836836815	Sandbox	8.8.4.4	53
326.321131945	Sandbox	8.8.4.4	53
336.837530851	Sandbox	8.8.8.8	53
337.83677578	Sandbox	8.8.4.4	53
341.075385809	Sandbox	8.8.8.8	53
342.071372986	Sandbox	8.8.4.4	53
349.206597805	Sandbox	8.8.8.8	53
350.196358919	Sandbox	8.8.4.4	53
361.948714972	Sandbox	8.8.8.8	53
362.947046995	Sandbox	8.8.4.4	53
373.946541786	Sandbox	8.8.8.8	53
374.946285963	Sandbox	8.8.4.4	53
386.243490934	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
387.243105888	Sandbox	8.8.8.8	53
398.6546278	Sandbox	8.8.8.8	53
399.649561882	Sandbox	8.8.4.4	53
410.736721992	Sandbox	8.8.8.8	53
411.728099823	Sandbox	8.8.4.4	53
423.992973804	Sandbox	8.8.8.8	53
424.977732897	Sandbox	8.8.4.4	53
436.074210882	Sandbox	8.8.8.8	53
437.071643829	Sandbox	8.8.4.4	53
448.488654852	Sandbox	8.8.8.8	53
449.477669954	Sandbox	8.8.4.4	53
460.478328943	Sandbox	8.8.8.8	53
461.477654934	Sandbox	8.8.4.4	53

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Javacpl.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 64e01bbb18db9e55bd62859aa84aff6b **SHA-1 :** 4a1da05e02790820fd409ab1b6f8722e2696b90c **SHA-256 :** 1170d0a3c1dc29d71994adffc1d9a15197547b8863b90f778adc8811b04b9 **SHA-512 :** 768f48278a061e7b27faa9051e8fdad3c7edf3f834eb7c8dd0d9df27660793 **Size :** 1563.648 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Policytool.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** d94ac19bc4158dd24ecb857f2a184599 **SHA-1 :** a10600b132b1654b24adb49ea685ebdb1e8671de **SHA-256 :** f75f660897b72703badf897974163098beeb2762e5ffc4e530ec6690fa42a9 **SHA-512 :** 9bc7ebe25796b8f9667f4ba40583d8a389f514c523f9539e099b776dc915f3 **Size :** 590.848 Kilobytes.
C:\Program Files (X86)\Google\Chrome\Application\48.0.2564.103\Nacl64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 2fd303b97b164f44e94ec7e408e91665 **SHA-1 :** 9d151d69b10df8faaf2089739a5f193503f09ecd **SHA-256 :** 8bf9d61d12790aa0aaf81c90885951a30e053b32719eacc3df345deff6ec05 **SHA-512 :** 26b0581d8bd60f42724c46d24b3b035c81493a33e0103c2f71e03fed1d692 **Size :** 2732.544 Kilobytes.
C:\Program Files (X86)\Google\Update\GoogleUpdate.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** bb82b31b36287c97455455a68a5a485f **SHA-1 :** 2ea3e7efffd49b03b702ff6cecdb38af248aab08 **SHA-256 :** 6580c717397abda741ca9f9e367eba8546d070b7636fc8881e2bb7a0fe905 **SHA-512 :** 756ffa3bdc834a981913e84c0ed113e575d766c74640c23a708c88e786d51 **Size :** 1640.448 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Tnameserv.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 5e0aca0a33c98160b3f7e3e7807481a7 **SHA-1 :** 476f675c925bc71ff5259b12a1b97be63ab423f7 **SHA-256 :** 65f18cd73d518510308a299cb428e8383be77161087b25f9c4835067cde65 **SHA-512 :** ae974899d8b0f139c294310095300fc15e06ec9afb22e4aa36f9e4aa5b10a3 **Size :** 591.36 Kilobytes.
C:\Program Files (X86)\Common Files\Adobe\Updater6\Adobe_Updater.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** c98c5b92214a597808339db17d8c2ca7 **SHA-1 :** 254c2797d7a959ffd09c06c3999e97c15e315876 **SHA-256 :** 7c490080a406465cb19c1ae11f10bb912c4186b5411a4f638c84de3d7700f **SHA-512 :** 366033332ec7f739cfe6d3c9ab23fd9714e61870782a9ccf77aae6a502f8a0l **Size :** 3095.04 Kilobytes.
C:\Nidguu\Bin\NURNEMUK.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** b0844118a790db2b40da196cf0e0a4ed **SHA-1 :** 93ae20ecdade9c68a731eaf41fca6d78e54a3263 **SHA-256 :** 69d8bd5427fd2095700ed9a95385463f120bddb17e3bd39ccface1fadf654 **SHA-512 :** d78e157d8ffca54d0cf330ca67408606f262fac6d2ea2bfe724b3693339f434 **Size :** 1593.344 Kilobytes.
C:\Windows\Microsoft.NET\Framework\V2.0.50727\Ngen_service.Log	**Type :** Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** c1ce18c9d41c2125ce6a99ef80b97b93 **SHA-1 :** ebfc418cdb9cb4b06122fc379024d871ec262286 **SHA-256 :** eeb682a476199b40238f01bf40646bcae201bb55fbbdf86a3e95a7fd1a251 **SHA-512 :** 2c82826c227773c3c159aaa506ff90238f5cee35f424f36c16a214af5efeadf7 **Size :** 1219.95 Kilobytes.
C:\Windows\Ehome\Ehsched.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 4b75b33fae42f760befb242fa7ae1728 **SHA-1 :** 7febe52bd491b4711004f3d1b558991b3c3e553d **SHA-256 :** 20ee967de9a1779e0057aa1735cdfcc7278e3a01de9e13fa5932232356c3d **SHA-512 :** 34e120691f939f5c9e81f3ebcaa83bdb51b75aad32f0241e3d048453271f0l **Size :** 1625.6 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Kinit.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** a3195bd8ea09b292ba4f433a85195005 **SHA-1 :** efa3d385bf743f078ca18cdf067890e7d7a035fa **SHA-256 :** 005aaedb4dcbafd58cef33b19465b0a30c436b627e11a3ed2313ee7e8a547 **SHA-512 :** 79fb2fc4641993d77cf73d8b0e8bf27cd6365f80e343c09d7bb771e23ff99bl **Size :** 590.848 Kilobytes.
C:\Mctrlc\Bin\QyCwoNN.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 1c1808c49626baf9079a03534a459e17 **SHA-1 :** f807db840d24577183366c13c496e040429a98b9 **SHA-256 :** 47ee48041f11bd350bfb89e8e028deec03abff0147123f91b73e444c10381 **SHA-512 :** ca3b3f5c0918d5e563b48fd0b2ae76a214575e4cb4bded0172dd31a4e7a7 **Size :** 1577.984 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Adobe\Reader 9.0\Reader\AdobeCollabSync.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 085f2793b208290dae2ef3961eeaaebf **SHA-1 :** 514ba6f9e4be829046e4cd10e74fb88ae6214d9b **SHA-256 :** eafde8d27627558cf4e93d50d2df5a10bc44c1f5d5b31317aed3e0b613832 **SHA-512 :** 4b95561ff613c5543d405f7392b81ca89b1e220f43c3cf164b010df5510faa **Size :** 2043.904 Kilobytes.
C:\Program Files\Sandboxie\32\SbieSvc.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 58075942e76d13ede7995facc16e11f0 **SHA-1 :** 6a332345237ba4ccae6f7ba4f347c3656cd3188e **SHA-256 :** 94f7480a4bf757571360b488123f95890c0c9aecaa9c606ab452d66bbdc80 **SHA-512 :** eecb255800ad9f509c3cb0787c8dad19cce3c1df1d18c4f3823d7b6db0d3b **Size :** 1637.376 Kilobytes.
C:\Program Files\MPC-HC\Mpc-Hc64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** a0c95e481a7ef70e0b5d64e0f5ef7ed4 **SHA-1 :** 5f95ad26e202f9e7424552f20f66c156b40bbcb9 **SHA-256 :** 1dd924fec4553c3dcdc427a8010dff5d38f85de50cb9061510b11f9bf12171 **SHA-512 :** 06c0a8b44d64ca7cd0cd7bc03ed3d85d935501038920b839cffd51a7d2aa **Size :** 12779.008 Kilobytes.
C:\Program Files (X86)\Common Files\Java\Java Update\Jusched.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 6a0a05881c55882bc341364677fe4590 **SHA-1 :** 8f3ddec38b2d935bfeb8fa569dd13b7f92760d7d **SHA-256 :** f7ade2dc54f5ae9070fcdfee2cbd2eb76fe61ddbbd9331dac43a1b8416f739 **SHA-512 :** 4fb2be0568a413bcebe7c815a86e37b4494b740a860a739eb3b464866321 **Size :** 1168.384 Kilobytes.
C:\Nidguu\Bin\Loader.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** f84f31c96875e56bd3195790618738c7 **SHA-1 :** 5bac8809ac4739fd7f175978e6ad688819374066 **SHA-256 :** e8886952a12d9a7613a2454efcf1de2886e004ce7f8442346799740ea7813 **SHA-512 :** 61032121557a1e0ccb8becb5d3fbfddc20a6b990b8116ad1e658fe7692bcd **Size :** 1577.984 Kilobytes.
C:\Windows\Sysnative\LogFiles\Scm\9435f817-Fed2-454e-88cd-7f78fda62c48	**Type :** data **MD5 :** 97e6c9048ec0c17f857e84a14998896d **SHA-1 :** e4f23c4a5534269d0df34a69f6c9e4d9d7608e39 **SHA-256 :** 42f73b4182a670cbad397f1d0f19de5285561ab2afbf9f6bec78a7e45e54ac **SHA-512 :** d5701845041af1d61be87d80189dcb9137ad5a6a76da9fbebb68a9c7b9c4 **Size :** 0.012 Kilobytes.
C:\Program Files\Sandboxie\SandboxieCrypto.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** b455fa322b8b50d4ed0645963f2e69c0 **SHA-1 :** 68d01d6c3426f022a329d9e4dc0a65936dc22061 **SHA-256 :** 3de9916c2b7fca32724ad6cf886942132a43579bcd1122c44951f05e5d680 **SHA-512 :** 79680e40f658a87d01cce17161501558ffdce372b8959def7e1f258a90c3ef **Size :** 1510.912 Kilobytes.
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxControl.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** f4541c9e10a99606c2595cc0faf19d67 **SHA-1 :** ba50175c657cb5174c355e6b235dbe0a1c925ccc **SHA-256 :** 13818a3bcf29d0439a1d44e6770b4060151e0ed9454eb1772478745b953c **SHA-512 :** d65450330273890c9edc47842856f632a02a9e934d31adf6f41cdfd5a5139 **Size :** 1859.072 Kilobytes.
C:\Programdata\Microsoft\EHome\Mcepg2-0.Db	**Type :** data **MD5 :** 443f1105b798e6fbca5eb8b86538e575 **SHA-1 :** 03d7a47203c635afaca32e05be92047dbb7f49c8 **SHA-256 :** 31acede97f1c7c06541a9cab7b9afdd99cef5905745353fc49117e4ea260fd **SHA-512 :** 5b6aeed30b25dafcba714ce51d72c3f810396516cab49ea4ad50e3c0f3b9c **Size :** 20.48 Kilobytes.
C:\Program Files (X86)\Notepad++\Notepad++.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** ab0eac897177cc974b4486e1a2e4c279 **SHA-1 :** 9bb02d4cd58aab2593cf5cb35e02b554271c5555 **SHA-256 :** b7bc6089d56501e05e5321718644c1d4e8e319f4c9c8d1a08eb11a6b2309 **SHA-512 :** ab78f38fa9e21439a45c8347455ba1932135c5d0cbb803add2c5568c43f63 **Size :** 2641.408 Kilobytes.
C:\Programdata\Microsoft\EHome\Counter.Mem	**Type :** data **MD5 :** 33cdeccccebe80329f1fdbee7f5874cb **SHA-1 :** 3da89ee273be13437e7ecf760f3fbd4dc0e8d1fe **SHA-256 :** 7c9fa136d4413fa6173637e883b6998d32e1d675f88cddff9dcbcf331820f4 **SHA-512 :** 991294f43425a5b80f8a5907ca7cdbb611401282585a58bb415077005428 **Size :** 0.008 Kilobytes.
C:\Program Files\Sandboxie\Start.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 5d20c5acead9cc117b8d92c034587de0 **SHA-1 :** 189b1bc332c4ecb111e82ac987887f22a4930846 **SHA-256 :** 2ab6051741ad37b80c5c9b0521b9c96d15bebc092e4eac5bd8c79974260d **SHA-512 :** 387316e605cfa2ef8024368da1a63c339a4883697aff01a1cedbd57b2242ec **Size :** 1629.696 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Mozilla Firefox\Crashreporter.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** b4b6e1285d0c93905a1a28d63422263b **SHA-1 :** e46bae4f2baa98c1eecfa6561b776c91b7b45c5f **SHA-256 :** dd470025d3c027ade0ddc2fa61e791ceb732dd029c1f9c6be950e7409c5dc **SHA-512 :** 75ae5764096b118949da7d765f282a4813ed829cee4d6720b99701d5ed72 **Size :** 855.552 Kilobytes.
C:\Users\User\AppData\Roaming\20503a4e5d0020a4.Bin	**Type :** data **MD5 :** 0fd3d7ec15afc2bdf101bf992379afbb **SHA-1 :** 75e1dc15f8f64212e081d026a1d2e84316bde870 **SHA-256 :** 745f4d707a3d7b472e6683a5f97bd13894ab10ec014fb8c9ad94fe9fc34d7a **SHA-512 :** b18d021626698ce86bf60a614ce9d8c8c79f56d175d4886c11e3aa24419f7 **Size :** 12.32 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Jjs.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 1d206377808658c3c936a3f4bf9f61d4 **SHA-1 :** 80feb10be96a2f3dc8964826121b78df8b1f6ebe **SHA-256 :** f89ef66351797dd756d0f253b3b45c9363d3b2fa68de68e20b82d3f9b692e **SHA-512 :** 804f9ac6dd76d5a1ce9f287ce1c71a79201b35e97f929bbd3281bb4dfc446a **Size :** 590.848 Kilobytes.
C:\Programdata\Microsoft\EHome\Mcepg2-0\Root.Mem	**Type :** data **MD5 :** debf14e30240c25648882dfdde607497 **SHA-1 :** 2dc895dafd796327bd3ebe58e47fe95566d9b30a **SHA-256 :** 541369e7fa5965cb3449d11c19f61cf7ddd90d3df1d4ab21dbb75f80183b5 **SHA-512 :** b1445d9eafce241db4e301dd351cf80ed58bb72eff23872aa256092df8898 **Size :** 2.172 Kilobytes.
C:\Bevevnhfi\Bin\FQWmJDsb.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** df8b9245791dd4b25b76731e17328ee2 **SHA-1 :** 44a12ebb7e06b1a3f7b364a0bff91fe46f32fa9d **SHA-256 :** aa0dbfb5d3095125c61c2e896144e1817e24164cb8e95743b9c04206fc14e **SHA-512 :** ab360625ca6004fc115918337a7937061dd05f7ba51f96e97232652f1bf8ee **Size :** 1593.344 Kilobytes.
C:\Bevevnhfi\Bin\Loader_x64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** f9a71f3baafeb2a497d4c85c7e2dca92 **SHA-1 :** 395f2651cf059d579b9f4ec2a9fa06b406d03799 **SHA-256 :** ec86b5ef406db78e98db17280a8de928f51cf349418783d6324d3317979e4 **SHA-512 :** d2ba8478152222d961714229fd7f8131b7e608cccccad008b94eaecf7a8a5 **Size :** 1593.344 Kilobytes.
C:\Mctrlc\Bin\FoNQWrug.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 203ca798d1ceed9760a21066f08403dc **SHA-1 :** 7b54f0499a9ca2f62fc5406c495eceb36f0c8735 **SHA-256 :** ccbf3b5fef0c6021bf42c428a20bd621c07e4c90fe34246d63d5e2e2f3e5314 **SHA-512 :** 8073912fd3beefd7fd11de7aaa464cc90888cca3931c20c9792ef543af0b54 **Size :** 1593.344 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Ktab.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 0b2e6a269c6c7ec35d5c70487b80c201 **SHA-1 :** b63e1efed3177827af667f75e65010e457bf6ecb **SHA-256 :** d76ac037b56d4e35ad38f4287fd8f67d789c4f86f07318379ed4ee8fef8142 **SHA-512 :** 18e9f03fce28f88002bd15f402508eafe99ec0267483ced2d05d7591b46931 **Size :** 590.848 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Javaws.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 296c2326ff1f5055bc382adea7a76312 **SHA-1 :** 614d03c3ed58bdaef3b6643005f71b5c3907f686 **SHA-256 :** 79952a6ad683da354a634d63d1c90c3ddb13308f8512c72cea8553a637fb9 **SHA-512 :** 5a2c32b11dee162981fdcc3d7842b85d09f96a7dc64ae22a8bc5066b203e3 **Size :** 1761.792 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 8c9e07944aeea1c185af9a5f9a414122 **SHA-1 :** 008d9d5946f2fef4db9f16f5faed329513484e9b **SHA-256 :** 40fd5e2f8a58d75dd05dd6d611a6c04adde3d51b467a5257e4e5a3b81e11 **SHA-512 :** dd1d87b8553a6d421f6cc70846b9ae02037c300631de73926a377d09cea6 **Size :** 1639.424 Kilobytes.
C:\Program Files (X86)\Google\Update\1.3.29.5\GoogleUpdate.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** d8de2212f95b31431d65ddc906e98708 **SHA-1 :** 673429dbdaa2f9f7026bfa067bd6322dccc7b0a6 **SHA-256 :** ee8fe4f779d5ac46d7b5a03e7c991c4d54bb87548a220873321dad148221 **SHA-512 :** 8c5e48464588e633c6a57dededf7d6102dc1ae6a12c126dc20d53ad3fca58 **Size :** 1640.448 Kilobytes.
C:\Program Files (X86)\Mozilla Firefox\Webapprt-Stub.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** cba2e2669ca1964156574b996bb6de62 **SHA-1 :** 3f303fb05551511c0b770961614659a8b4536a5d **SHA-256 :** 440f32acad8b67fa65310861be2c4cf85fa6e5ddb656865ca3f9aa4b72f79d **SHA-512 :** b30b8ad451bb6bca8ea029a311878c7a2da8705d1576296100657981bd4 **Size :** 802.304 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Adobe\Reader 9.0\Reader\AcroRd32Info.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 9e25c3ac55a75ffad2dadac3f60374ca **SHA-1 :** 2915ba246904b0027c7767e546d8033f1c7d38b6 **SHA-256 :** 9c139dc88a8fc9071feb892070341572c262df8649f4a053d9b45c4aa3278 **SHA-512 :** ed037e4214d2e06a4fb2cecf4efa74fecc287b73f67de42444ccb39a1af10a2 **Size :** 1509.376 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Pack200.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** ec6779e2eb550fa27fd750ecf528b0ec **SHA-1 :** f5f6946b71e5beb4692795a76d6aa178851f0402 **SHA-256 :** 548613a2a08090417c1154a902aa84b21ce398041bc763ce4b06325e5241 **SHA-512 :** e7d9c3582850b165c5d1d641ee76b9b530b12f0fda40864c3ddb39527dee **Size :** 590.848 Kilobytes.
C:\Program Files (X86)\Adobe\Reader 9.0\Reader\A3DUtility.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 82057e661281e364123f0d879cb4d7f7 **SHA-1 :** ae74ed37d8548560a8ff6573dbd391c9b953dbe3 **SHA-256 :** 89e2debdd0ce969305cdf51d225d57ced5c1d05ae560fa072a329473844a9 **SHA-512 :** 7e7b1bca1277f8ffbc558d10bd8678db88def8481c2a24b42115ec32904f03 **Size :** 1744.896 Kilobytes.
C:\Bevevnhfi\Bin\Loader.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 9cc4a860f8a204bb94ad45392e85bcb4 **SHA-1 :** b596f54e5aea099f6fb44bcd01904ead66a1b847 **SHA-256 :** adda51307939fa0e0cd3a6c5dec8009ae3d45aef4c6a1c67ff0bf83263a1aa **SHA-512 :** 3d6f91f0d898d76bbdd8ad6b0c5def5b01f4a4d1ccefbf3375ed60a13ce129 **Size :** 1577.984 Kilobytes.
C:\Mctrlc\Bin\Loader_x64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 7a8076d2cda19aa4218aa56db29af75e **SHA-1 :** 7a2ee22d2ad6ad0252a4145905c85112000b5301 **SHA-256 :** 892686d044eb2dc89f5122a85fa27fc0533b0cd790dfadc57c1847e997508e **SHA-512 :** 46ee5149430ef676a54275b03be6b2cfd8ed07756f36cfd0a03a3ce49a7a2b **Size :** 1593.344 Kilobytes.
C:\Program Files (X86)\Mozilla Firefox\Maintenanceservice.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** a694d51b69d8f69654678c456aa89478 **SHA-1 :** 7c2eb91168ebc0e7e9bd4c0e6e80d0862fbb4941 **SHA-256 :** b397d616e1d4dd82a2fb4606529e6796395c36d593041c10d622bd5bf577 **SHA-512 :** 2c05c6217537c217903f5d916509da1df77d7a23f64bde2364c6d5d2df7b6 **Size :** 719.36 Kilobytes.
C:\Program Files (X86)\Google\Chrome\Application\48.0.2564.103\Installer\Chrmstp.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 7aab8b546de34a4814dda79282b7be0b **SHA-1 :** 5126b484eb90f4edefc543ed4e115c0fe9c29929 **SHA-256 :** 23657fe55f0548ed73d47a64bbf70c9b48b65c3af05d00821b393807fcf8b8 **SHA-512 :** 89be2ac96b54dabfebd8aed230164a9fa20957eb77372b078219f2e44b74 **Size :** 1657.344 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\OFFICE12\OFFDIAG.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 826d1a0a288938e411b14597d298619c **SHA-1 :** 107464611cc5a9e4e3d76f05e5ea8dfd21cd671e **SHA-256 :** 575338d1ad542955036de011d4b5022f5111d7c1d6c549aef4cf29bc1bf03 **SHA-512 :** 312531814835126a1295373d76de21bb0edae4ad0601140cd1f5c9e77eb6 **Size :** 3446.272 Kilobytes.
C:\Nidguu\Bin\Loader_x64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 337136b87cadb7e38f5a8252ce7504d0 **SHA-1 :** 06f27b2b5652b10097f0307dcb611ff0c8c3a2e8 **SHA-256 :** 8a5813fdf6bb3233cc31d66bd249cdb5f96add099e6747a24689aa5a9cdb3 **SHA-512 :** 3e2b68f9b7b3cbbb3df678eee6451304f608086809155ecce4c84650cf35e7 **Size :** 1593.344 Kilobytes.
C:\Program Files (X86)\Adobe\Reader 9.0\Reader\AcroRd32.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 1436ac16dad14c05a6cdc6b0d410a176 **SHA-1 :** a9af465d2f09f2bfcee6e340a1fd1d266a3452ca **SHA-256 :** bcfbbba18400fbf06e54a2b741a95367f017080e90474566837390 93b5a6c **SHA-512 :** ad00ee389166714d13703bfb16cb49e2644df2d26c6cf32afdac259f40bf26 **Size :** 1851.392 Kilobytes.
C:\Program Files\MPC-HC\CrashReporter\Sendrpt.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 2c2d8e6971d5a992cc593a93bb0207c7 **SHA-1 :** 9cf1f0e836ca59d6011c7b329c0d92f059602dcf **SHA-256 :** 01fef3dd0f03d495d1b406b4a4de1177c760013ce40e0cc635409710052a7 **SHA-512 :** c8f84ab90771051486845ff1fe60ad2b4f2f46b6b49b9694ee131d85b7845 **Size :** 1355.776 Kilobytes.
C:\Windows\Microsoft.NET\Framework\V4.0.30319\Mscorsvw.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** e7626742975 59b8136c9910daba5a01b **SHA-1 :** 85d9240f57fe7cd89f3321a6cbf92aeab8844a86 **SHA-256 :** 1cf49990aedc4edc6d44ea8c11c42e024ecf8444aeab060d6c40385549251 **SHA-512 :** 68ce456dc87a9fc00b29bf37e5b7063cbe72a371760efd021dd5ce985e964 **Size :** 1587.712 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Windows\DtcInstall.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** a2f33215a824f996cf347193f3a6647d **SHA-1 :** 967e0e74669ace1a2af2609c677f5909de5a8c5d **SHA-256 :** 18784d0dd330761fa4ff860ab76e6ed6d1e4e035a85e51af1b0165a7b751e **SHA-512 :** f69080d74a77200e514059cdec0349086f9191e72816945b3ad4b4b8b200 **Size :** 3.183 Kilobytes.
C:\Programdata\Microsoft\EHome\Mcepg2-0\Blocks.Mem	**Type :** data **MD5 :** ef2e0d18474b2151ef5876b1e89c2f1d **SHA-1 :** aef9802fcf76c67d695bc77322bae5400d3bbe82 **SHA-256 :** 3381de4ca9f3a477f25989dfc8b744e7916046b7aa369f61a9a2f7dc0963ec **SHA-512 :** e81185705a3bd73645bf2b190bbf3aee060c1c72f98fa39665f254a755b0a5 **Size :** 196.608 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Java-Rmi.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 6ff056c7e37f7c7c7d8fe7d2ff344a2d **SHA-1 :** 52827b17f8af501f9b8a39438ec88d22c932dd12 **SHA-256 :** 4b2092b72dde3fbc5f2624769e29f11e6d36ecf7e24c54ce51fcea67d826b0 **SHA-512 :** 1f2d04de126c847633b52587a601562c87a75a0a49be86b2d2351079e954 **Size :** 1508.352 Kilobytes.
C:\Windows\Sysnative\Snmptrap.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** dddcc15efa8819f98b2fa5280322cca2 **SHA-1 :** e93f45bb8ac9f7116ad0f98e9e246fb95c6a20bf **SHA-256 :** 85e60adeb98950005cad026a35810d56d5ae56347e11bb3393a7280a6f03 **SHA-512 :** acbf245e4095cc45265ee17b617c672400324e0be9a9a3f3eb93587c3c809 **Size :** 1512.96 Kilobytes.
C:\Windows\Sysnative\Msdtc\MSDTC.LOG	**Type :** data **MD5 :** 517f82d80327655af41136c642f72f36 **SHA-1 :** 0ff9cec5885818285f24ea96314dbbf535d80b42 **SHA-256 :** fedc813824f92c2349e36b1e9ae0295577a21ae945f9d80ab8c3f5476efe17 **SHA-512 :** a693b372873a0c48b402e619c34373cb9a4352f962865c0f504bae5538b6f **Size :** 4194.304 Kilobytes.
C:\Program Files (X86)\Common Files\Java\Java Update\Jucheck.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 00dd575b498c3e00094bb16fff85634a **SHA-1 :** 086bc0a3972c393716ba3eb6cfc9f11b462e5d20 **SHA-256 :** 0741aa2920ad249cf8e587c4e64dbdc23cafa6c82fe90a0232712516611d8l **SHA-512 :** 40a6273e1ab4acdccfa9f56aa816c727cef7840d6637ff7562c661d03e7ceb7 **Size :** 1506.304 Kilobytes.
C:\Program Files\7-Zip\7zFM.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** e28565f9de0fd7929a875b761769b494 **SHA-1 :** b1348583d65733905f1822b6b2a0cc3056ec0e59 **SHA-256 :** 3698d4e55f48065e755fe686d4c6ef827fbadb079f9a31334aeac5404461e4 **SHA-512 :** 4cc18dd90af90f04e281b57c1a8ca18b0284721088c6574dbef2a27c6236cf **Size :** 1416.704 Kilobytes.
C:\Program Files (X86)\Mozilla Firefox\Plugin-Hang-Ui.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** a9a5d0f6d677d108be43d02daaffdabe **SHA-1 :** 5ff785d1f292240e0900c16c080e093a8cfe9b81 **SHA-256 :** 322ef57fa9ed435c63f1317210724b6dbc5c73fdc651a58c6d1dac8e4707e8 **SHA-512 :** ffbbffa14dd1c6ff701620e4d1885d0bb8646d620d7a954c95317c840cc7a8 **Size :** 743.424 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\OFFICE12\ACECNFLT.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 94680d7966ba71904de97f3d9c5ed6c2 **SHA-1 :** 2230fb97fa6f0baa022e499c6d309fa535403da0 **SHA-256 :** 7bf5fe28206e8d70197627a20f6fe9b0235e8bddf5794f853505567a4b099c **SHA-512 :** a0d5d55bec9731e119ea762fe5e0297d8a9001f668889e3feebc4ea494db6 **Size :** 1548.288 Kilobytes.
C:\Windows\Appcompat\Programs\RecentFileCache.Bcf	**Type :** data **MD5 :** d3047b7d6adefb3b2d4bee4dfce417a5 **SHA-1 :** b7c38f10ee3f17b3928b2340afbf8b5259ebf6ce **SHA-256 :** 9f89a2968fb87241808f0cd6ca4cba0f2fcbb8e60626db03efc91cf359f016d **SHA-512 :** c713e4787777f58f999daf90ff2c8baf99874ea872f54924298416ad14cee18 **Size :** 1.28 Kilobytes.
C:\Windows\Sysnative\Vds.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 1ac429fe2e3d4982b4337db30db588d4 **SHA-1 :** 22c14c7b8cfe2dbf0de24fe56afc56c3788ae816 **SHA-256 :** d9389e1cea36f33a3a89396c6268973635ca45ef2bde88e76d9430ed51c53 **SHA-512 :** 0886de58148c91644bf15176e89fbd7dd7a99275233fa6f708239e6a02255 **Size :** 2033.664 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Rmiregistry.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** d4c91f628c224ea817e1e88a8add67af **SHA-1 :** 849145f8b1912437eee8e791a0aaa68fe13c9794 **SHA-256 :** b20461a9d33181ffd0f067278c21c89fab959c4b15fdaba4cae8c229317a88 **SHA-512 :** a35e2f398ff0a757d19eea2d063a2675e45d07b91601cbd649d6ce85b52e8 **Size :** 590.848 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Windows\Microsoft.NET\Framework64\V2.0.50727\Ngen_service.Log	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 2e0025ed62f46220e4a0cc4089457638 **SHA-1 :** 70b3ad7afddfd0316a2cef77ccfbd045cb1504e0 **SHA-256 :** 21741e2f753defdaf96c813f4244d8c8cb2d86a91689bf34b8e3fd0fdda701 **SHA-512 :** a7ab1f501023571af1c2b8f8bc7801a410a27e8688c92fa1f62019cf93b738 **Size :** 1274.882 Kilobytes.
C:\Program Files\Sandboxie\SandboxieBITS.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** e1ab4ea21013a682811ab31952e79723 **SHA-1 :** f650c781feba30ef27450197d3acd1cdde656ead **SHA-256 :** 5935c38847424247b4ed9335158de7d004f6e35564e19a6cc8f1f3a2271af **SHA-512 :** 728a65eb47411e85b1af7521ea8ba708da00c23dbae360d60ce3244d5e84 **Size :** 1508.352 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\MSInfo\OINFOP12.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** f5908ef9cf401ecaaa7833e47eae2bf9 **SHA-1 :** 063985539a031e77e208158903b1545eda78f945 **SHA-256 :** fa13c987ab4f90a5e08cb396c76db85a31b94879ff93caf2f9371f183801ae8 **SHA-512 :** 4601f85533aaaab4e0b1e1fd77300ca8667406e594bd620dd7b14bfa6044 **Size :** 1580.032 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Rmid.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** a723a22e5863a95bc1b0c6c5819ad4ce **SHA-1 :** bd3b478b708716f0322c749a90852dbb939ebcee **SHA-256 :** dffbb320b62f22d281eff94dd4df08c9c53c41f882b173dc23d482d8d1d135 **SHA-512 :** 1946662e947b105ecd05101055899072eb18338e0c0d6531436ec82a72d3 **Size :** 590.848 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 3d0e397ffda898aff3c35b9c9a8be54d **SHA-1 :** 9f7a667e3ed069f4a9760ba3c03afb8b01e6203a **SHA-256 :** 49de67c336f904e9f713738083dc1e45ad6ce576e784d2a146d5f08885e50 **SHA-512 :** 8d69c425eb1ae4ded56bf18f51f64bb1f3f6cd73aa551597f09c39e4d2f35a **Size :** 2035.712 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\OFFICE12\MSE7.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 8a74ee8d322402e61c856a1590b30754 **SHA-1 :** 29f904b28b7fbaf9a3e1ddf74c3bb1ecb584a0c0 **SHA-256 :** b0546668192216d91812a5b482e61775218d7addce43613583939fd1ca31 **SHA-512 :** 1032dd45a7280a873cbade2183204894541696105 24b96d120d6951a2f66 **Size :** 1541.632 Kilobytes.
C:\Program Files (X86)\Google\Update\1.3.29.5\GoogleUpdateComRegisterShell64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 00ee5a46d93d7d2546962a9c4e1db805 **SHA-1 :** f006e7915f5065f9b3f80fbae857399584a5427f **SHA-256 :** b3c93d128bcab44e531ffc717971bb5c42d61689799713d5e34b7050efb45 **SHA-512 :** 00cd42e715061a0942842b10be9d3ed6060051036a35e409cd03619c9e4c **Size :** 1625.088 Kilobytes.
C:\Program Files (X86)\Notepad++\Updater\Gpup.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 4004152f30a51e65c470c8cd1ddfec00 **SHA-1 :** 1320c2c59764a42876d5ef03fa50a6d37e0ee977 **SHA-256 :** c33ec6be7f9e8993210a2b1e83b4ae3fca6c6f5c5cd7704805620b4c9141f3 **SHA-512 :** 6e25ccdecfb7f21f00909a609ba0952c63db2fc85a83c7acdaf9297a28dcba **Size :** 859.136 Kilobytes.
C:\Program Files\7-Zip\Uninstall.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** c5a958aba58190c6918319052a153fcc **SHA-1 :** c3d6445303de2766014c27f7d5c919dbd2eae37a **SHA-256 :** dae702c8ee3950bf52d81e49beabd1f02c6cd639b9a69b0f3ba9cdb724b1a **SHA-512 :** 1c14bf7bfafb98a8df54ccde323dd742dbea8ce9281608b88bfe5b6b87b5a **Size :** 1513.984 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Java.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 7bda3ce9f9486214d39edfc7db26c164 **SHA-1 :** 47c553fc521d6d69495bcdec1a287534b9f1f198 **SHA-256 :** 92d67fef818cc00a5fb3fa046a7848a48b0551e6125a9ebcc50ea839a22b04 **SHA-512 :** 0f70dd0af9d1cf08c5c1bf1c85f2ff1f04d2456d563d2c05118fc084b7783f6c **Size :** 1685.504 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Klist.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 43b7f886f83642b24657a22af0f94e01 **SHA-1 :** ee2537f1f5e4528878b79d5fbb3e2d0b9a7e2c64 **SHA-256 :** 90c36dad9a1a7c6e2e8564fd2ccf4c29694d9a07a5c2a8c1f222fe086e886c **SHA-512 :** 761e1291edad2e67894372a2e9317ed0570997701083755e7bf031f39365 **Size :** 590.848 Kilobytes.
C:\Program Files (X86)\Mozilla Firefox\Plugin-Container.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 422434718d923f98ae40453da77775b5 **SHA-1 :** 1d1d9a8693f080cfd8d499138921f205a3f7581f **SHA-256 :** f9c259d0c43a33c682be8f16001c57c9580587ec05511be2fe777ac18f0077 **SHA-512 :** 141d78c773e39f7d52b57479a55b84a5c272b6698e1f55e3b26f82c403da1 **Size :** 849.92 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Javaw.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 07956a72aedba00c7ef293f00c668383 **SHA-1 :** 3a6b1e09559af763188002da2750bdde7b636b82 **SHA-256 :** f9511b0b407dbc66fe16c7586923c2d5ae6f5132dcd0fbd0def79f245acfc1b **SHA-512 :** afc2699617b3ba3c36645dc9ce664dedf3436b89bccd83412c038b6a7aa38 **Size :** 1686.016 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Ssvagent.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** bcc72792b4c9756e584a4843c7eb358e **SHA-1 :** 7903053f3093c195408c1d6f234c6ef42f690370 **SHA-256 :** ff8d350044337f01675965ae7cb4b3fc27c1a35926c3ea21afbaef01a22e4a2 **SHA-512 :** d9c13ecc33423cb6d27383d473fad93aa770be3f4e872ebc9d02eaaf4f6d18 **Size :** 624.128 Kilobytes.
C:\Program Files (X86)\Google\Chrome\Application\48.0.2564.103\Delegate_execute.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** e3c2e67ff6415662f745c598fa609c21 **SHA-1 :** db1563ef2da7e4baf9ca5ab2e10b871ba2edfd50 **SHA-256 :** 5fa9521f38c6260d20fd6e811e8deb9dfc9cba80e63a10e9562e3f4ae50ea0 **SHA-512 :** b0cd753e874cb167ef70d2c604686914580c8f387b405062cc4604dd578b5 **Size :** 1300.992 Kilobytes.
C:\Program Files (X86)\Mozilla Firefox\Firefox.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** d24135c9011535ed3f89258bc9fea201 **SHA-1 :** d94c78608891122dd1b4778a90e4d32f49f46d26 **SHA-256 :** 9cf5a244f385aa1b71c82338921f0eb1748aa0277c691cf992e128aa32305b **SHA-512 :** 4bcfaa60404910695553d26b5f2c0bc23eb860a7b87f31d64f139055bd919 **Size :** 965.12 Kilobytes.
C:\Nidguu\Bin\RhfuTcC.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 730071b739204ef2033b42a62e96b3cf **SHA-1 :** e221c7621e8e0baa060aba972fbc500e2b2cf8da **SHA-256 :** 44e856ae97a830c1bb1aeeaef0371d85a16fe522f735a83b2792c60d8a529 **SHA-512 :** 701f9e353797d03d1b425dae5065889267dff79a9e8b281a036b3b926be4 **Size :** 1577.984 Kilobytes.
C:\Program Files (X86)\Google\Update\1.3.29.5\GoogleUpdateOnDemand.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** d2c398c162a1d7472546904acc59e31d **SHA-1 :** 647fa39ae7cb82a3877c6d537ceeeed363eab6e0 **SHA-256 :** a508c5f43179465ddda967dbb71c968d793e5274768dbeebb1940502f413 **SHA-512 :** 32e14527f985bbb692a0e37fc405ad757fd5617d526b567e53f9e7ce6cc78e **Size :** 1581.568 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\OFFICE12\MSOXMLED.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** ec5a36b9c7db73ca80bcb4fe2b5e22d8 **SHA-1 :** 735b4981c7cfce3db289b706771b603a95603945 **SHA-256 :** 840e436644e56ea957194077e3068dd0aa6158e65ebe9e5dc76fb18bcf19f **SHA-512 :** bd39b2f0e9c72cae34fb5464055de188e4b8bd4efdcf8fc469a1177d8b987c **Size :** 1550.336 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\OFFICE12\Office Setup Controller\SETUP.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 7cb4f96bfcf71680fd406a3d2c57eba8 **SHA-1 :** aa20e90e805df5a358ee9bceac3a843159f938b0 **SHA-256 :** e0fca2b236aef4bc467a38701fa0880cff9784bd4edeed2e24d517bddbdcde **SHA-512 :** 2833bb6958a87f45ba01aad737f3eaae8bd00e8330393bcf5f727ac2c45a45 **Size :** 1933.312 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\DW\DWTRIG20.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 95146e3c59964b51e3d6308d45f60d2e **SHA-1 :** 9cfe4afc9b217a2410f9bdfa3b5ceeec9d568209 **SHA-256 :** 46ccca48b582fc4ed1ac08cbf961b54260fbcaecb91c5e49bda9a44128cf61 **SHA-512 :** bd24ccfd31fe50fe12bea162efd736ad8e34839ae23aed60955e17a4f6770c **Size :** 1927.168 Kilobytes.
C:\Windows\Sysnative\Msdtc.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 0ae39b50434df07534c242354c103893 **SHA-1 :** a1f5e2d839efd391d841764d250bb73a301d83fa **SHA-256 :** 1ffb786010c603b4b200ee421d3a236cee127dd8c107ae323bd70bd71923 **SHA-512 :** f0a3cac4108ae6a177af8bc383992d40f90e93a142ff40c3ca7ab4bb8202e5 **Size :** 1639.936 Kilobytes.
C:\Program Files (X86)\Common Files\Adobe\Updater6\AdobeUpdaterInstallMgr.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** ff4992815dc0713dc3af7eaeca671cab **SHA-1 :** e28d60fc479a5bb8f9756a5692941b0252480991 **SHA-256 :** c8fc0c7f4c7614d6657202603f9014ffc0094b180bb9f6d7b8925aee21960f8 **SHA-512 :** 0d01930de42c3e68f4407cee7dcaf89b1900123f67560485d0a9969be4c09 **Size :** 1589.248 Kilobytes.
C:\Windows\Registration\{02D4B3F1-FD88-11D1-960D-00805FC79235}.{BB1BBD67-ED8C-4496-88C8-4131F3DAEEF5}.Crmlog	**Type :** data **MD5 :** 184bd5b188ba9bf4aa33b9a4f2a46829 **SHA-1 :** c5ee129c5a60c7c9a1973283fed0313043bc6058 **SHA-256 :** e93916fe454f9c68c3f30a00a7361f39e46ea2b1b09b56ceb6f9966cb644e5 **SHA-512 :** 325b28b9494fe38b2dbaff17092e32400c7cfa6729b42c678024d8ded6240 **Size :** 1048.576 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Windows\Sysnative\Dllhost.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 45e6e31bb6788e0137e878cf533a0ca4 **SHA-1 :** abf6225d1efcb021f1822b1cddb2072a31f6d15f **SHA-256 :** 1b98fe5ee8b8e2f4bed49358263bd1d9147213c7b4122f2bb52ca6e1be94 **SHA-512 :** 3af06b8e0fd71f9bbe92e322b76b1eb0885a747cf2f117bc936da91fcbebbe **Size :** 1508.352 Kilobytes.
C:\Windows\Microsoft.NET\Framework64\V4.0.30319\Aspnet_state.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** bef4a6cd92dc3bb44f3198ad00157960 **SHA-1 :** dfcf6f5959975a07a09eaedd917a4e955d03053e **SHA-256 :** e7700a4e59052d15270a005f47301f92d361c98b26757c17d98364fa9c1a7 **SHA-512 :** d4dda1fd7c08e4a9bc1a6ba55d15990dc5799ca35edc6695032cdd23b3e6 **Size :** 1533.952 Kilobytes.
C:\Windows\Sysnative\Locator.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** 17405a721697fd3d2770b76f66ac0591 **SHA-1 :** ca811373f9ac3b22b5cdb4093cca399a82cce7d0 **SHA-256 :** ff435f22c70f1e222f9c096704291fc24aaab6716858f04bfd8fa1a26963fbcb **SHA-512 :** f26a4702db17c52a2083a6ea6cc24b16d71e01e06c2add219c38b4a525dc6 **Size :** 1508.864 Kilobytes.
C:\Program Files\Sandboxie\SandboxieDcomLaunch.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 4c2a5b43a56ce807a64a531e102f6e23 **SHA-1 :** 2235170ac8ae092753b1ecd1486bb59c67361ecb **SHA-256 :** 5f3f2207e8975fc2835a20b33ce8421d32644515b2aae8f3a6be5fd521707(**SHA-512 :** afde60b916969127f3f4e0ef36280aca6880fb6651f110f6f291ba439c9bde4 **Size :** 1515.52 Kilobytes.
C:\Program Files (X86)\Adobe\Reader 9.0\Reader\Reader_sl.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** cc382f13e6a49c7051a418f731a7e7ea **SHA-1 :** 7c0c1a5ba8866dfa111247a6923ccae6b283c767 **SHA-256 :** 5d4fdd2748f851edf00127aa6b71cb76f8c45925c294f05ffa74e957e35d4ff(**SHA-512 :** 7d754e3704d8099bbbe44e3eaf1a7e9c722f1e4d9eadffa06652ef4c73d0b6 **Size :** 1532.928 Kilobytes.
C:\Program Files (X86)\Common Files\Java\Java Update\Jaureg.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 4011768e2d005213cecb487a76e7f700 **SHA-1 :** a3b28c6025f47be82c6df168cfab9c37c2e74d06 **SHA-256 :** 9d3478f1460aca5b3b264e1560993942717af8704d3afef9175035d88df974 **SHA-512 :** c1b59a10f1d75711d6b34ffdb5e59b690d632496e900871de0034f4f79a97 **Size :** 1930.752 Kilobytes.
C:\Windows\Microsoft.NET\Framework64\V4.0.30319\Mscorsvw.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** e36d99243cff7d8621326e57e9dce0c1 **SHA-1 :** 47167036b0b2190dab7d245b55028c1d75ea5156 **SHA-256 :** 1a25999fea30edf24c45ba831093ebe7198f7b963343076aded6de2aa16b0 **SHA-512 :** 46c02e447173724a19e9324a73c51e758d34053111d138a1f962b8835330 **Size :** 1608.192 Kilobytes.
C:\Windows\Sysnative\Msiexec.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** d1c4eb54f0b7b3d0aecd34b25024b813 **SHA-1 :** a9971843672987af2ae598ff0b6ff095ac047d53 **SHA-256 :** 707451f11fb402cd286a1e1d6b3964a42cae8541c2481b9ef15679d24b234 **SHA-512 :** 50dda87268b80140f0d96db3141cb89daf18e0d1978b9eeb23b61cbdd5c5 **Size :** 1629.184 Kilobytes.
C:\Windows\Microsoft.NET\Framework64\V2.0.50727\Mscorsvw.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 52cfadc524672f8548d4c2a8f22c6e70 **SHA-1 :** 855c500bc04a15df0bb39be65ee722d36008f07c **SHA-256 :** 00c27f727bf593e03538a557f24a464bb7206f8400223b49d9a3037914ac3 **SHA-512 :** 77d827cbc86081c5e966dbde540a4fdf81122d7db0d7d9cfafb1048fde661 **Size :** 1585.152 Kilobytes.
C:\Program Files\Sandboxie\SandboxieWUAU.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 0e0f11cdb9d66d8b56c82d7f77565315 **SHA-1 :** 72b1a4ce8ab9a253f956114923e14c29a4029aa1 **SHA-256 :** fa5ef2b95a9790a3fd4d498af29496b2eaf4cd89e78f896a2f5cb755880fc0f(**SHA-512 :** 2a406d6d0ac4fd99c42af376d97ca227d104c80750ffc6df02f86134eb6a3ab **Size :** 1509.376 Kilobytes.
C:\Windows\Sysnative\Config\Systemprofile\AppData\Roaming\20503a4e5d0020a4.Bin	**Type :** data **MD5 :** 6f05a30a7d4630bc9dc1bb680fa2c900 **SHA-1 :** d1336f34c660b5495cb596ec19bf702c74e0d90f **SHA-256 :** 678ef033a6a496515e8756dad4ae377bce664a2d87dfd9b2eb59ef7dbd87 **SHA-512 :** 7dd86aee88df1d83b2939a5fa59c157d04bc2eb0c106724463c5fc01afebd(**Size :** 12.32 Kilobytes.
C:\Program Files (X86)\WinPcap\Rpcapd.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** c19b75dfc1ef808f8c0ce355263ca735 **SHA-1 :** 5e7f6a09a0a5e8c35fdc0870c2e3b8a1f9f7bba0 **SHA-256 :** e78266437c3b4d61fced98d220fa083d73c8d9062229dbcaccc428bca171c **SHA-512 :** adf7d224b5509cc9430d30738e806c139138e58b7d0bdd7848c71b7118e9 **Size :** 1609.728 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files\7-Zip\7zG.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 49b941396593850b52cad955f2afb96d **SHA-1 :** 1573e1cb4c987d8e93115136e844933faa406137 **SHA-256 :** ef1ede9916c6c2a11e0d8388bac0b65424e0bb8577afbd64cd7c45920fd86 **SHA-512 :** 60acb02bf76e8852fcc0c6e1edfffc0d1b5200177384fab6745106762d5c53a **Size :** 2055.68 Kilobytes.
C:\Program Files (X86)\Notepad++\NppIExplorerShell.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** f7dcbb95b2e8e45d0aa468ca5ed29ee7 **SHA-1 :** ff44ef8c84c14b06f475f52c56024b9576afa141 **SHA-256 :** 19d4bb70a5eb92f63054d3221e6793dbc14fb77dd305fbe2f4bdc02b00dbf **SHA-512 :** a5f59f72a930b4088925f8efe53161dc9933c17eb8d3ba56cf498b450d8828 **Size :** 587.264 Kilobytes.
C:\Windows\System32\Config\Systemprofile\AppData\Roaming\20503a4e5d0020a4.Bin	**Type :** data **MD5 :** 89e24e8517090624ab86b99e41ae6076 **SHA-1 :** 2b375505ef2bbe91fe34c272c658b722aba1e414 **SHA-256 :** 0646a1a01be221ab984c2a68ea821efb120904d7c6ee2852a39e3f38e3000 **SHA-512 :** 5dfb074774a3832d5ad75cfc88183e1e42789f66452342d4d590baf99ebdd **Size :** 12.32 Kilobytes.
C:\Windows\Sysnative\Config\Systemprofile\AppData\Local\CrashDumps\Alg.Exe.2472.Dmp	**Type :** Mini DuMP crash report, 9 streams, Sat Nov 9 19:09:23 2024, 0x121 type **MD5 :** 1b51a1afe3f866406d873b0b3531097a **SHA-1 :** 5d7235e286ac725754cd9bb9c364226cf1b9f11d **SHA-256 :** d2f266e65fad60eb25bd23d5d8ad5e58d573ead5d8b922c7088ce1a3b6a8 **SHA-512 :** a0b1ec3d0de7adc9706d9830fcc7836a933ba303c5b2e5de458fe38d5e763 **Size :** 2092.202 Kilobytes.
C:\Windows\Microsoft.NET\Framework\V2.0.50727\Mscorsvw.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** f26e010ff6bdc64d8a032e46ad701986 **SHA-1 :** 153fdff9180edbccc2d5fdbfb159b86b372e857c **SHA-256 :** bf1f97ff07bf85a32a820f118662360bb5357ad941c506257f6048c0786916 **SHA-512 :** bf86fa1e884751a4da269effa67b69a80db84a5b79f61b7d64ebd1f716b7a **Size :** 1561.6 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\Phone Tools\12.0\Debugger\Target\X86\Vsgraphicsremoteengine.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 7969ef469864dc40e8dd9ea437f91630 **SHA-1 :** c6430387bc00c6854ee250deaf9fcc50040cd228 **SHA-256 :** 6750e77089cb481ab96f93e2de540f3a1c3c49a9924648f2ef51a003b3b41a **SHA-512 :** dc1269797adcc418ba7666038f65256f93524437663f5f689ea464142c0386 **Size :** 4574.208 Kilobytes.
C:\Program Files (X86)\Adobe\Reader 9.0\Reader\AcroBroker.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 0c414ddaac907bfe87d2247466e1f063 **SHA-1 :** 0592bf2c1623b2a29514cf0ac2f6eb83fef292a1 **SHA-256 :** 4421f0f4e923cd1f9654d2d4e5576a91f6016331076e8ebfc5fbe9e6da4e47 **SHA-512 :** 9bb46530da891d26874c054d3138d94f5d3f9ed4705d2243e7cdb3d0c535 **Size :** 1773.568 Kilobytes.
C:\Program Files (X86)\Google\Chrome\Application\48.0.2564.103\Installer\Setup.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 951081c69e92859ed5bb5aa27e6a5cf4 **SHA-1 :** 71268cee4c3777a966910b7727f5863a44ff0a03 **SHA-256 :** 76c24227a9fe4a608d4abf9da386d544d0bf1e3fe4d977f48afd53987a4244 **SHA-512 :** 00333a9bbd8abe33ab8ac8db13b28c10fb75c6f3be2e58ea873624c63b4e **Size :** 1657.344 Kilobytes.
C:\Program Files\7-Zip\7z.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** 42f7e85a3b2d2b394a533ae008058388 **SHA-1 :** 8233aad098bb71c0ddb300592aec15076f604a0f **SHA-256 :** 7ae017d7c1c14cfa2f7fb1ab4f46feb8f544516441181021b34f0529d65e859 **SHA-512 :** 47386ad7ad6b45d0c8b3bae42e3404ab6a1fcfe14600c3eeb733d8694818 **Size :** 1945.6 Kilobytes.
C:\Windows\Sysnative\FXSSVC.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** b9061b733278b836dee306381d096b57 **SHA-1 :** 3a18c8e68ffcb4fde8d1e7aed06e00f83274a6f6 **SHA-256 :** 2934bfcdadbd0572a71a2cb4e67c5c547e6dc37067aaa74084dee83f993cfl **SHA-512 :** e4aef988cc067d454c3c6d0bd9956d944f11dc1fe61af6208daade3ab7c76c **Size :** 1269.76 Kilobytes.
C:\Program Files (X86)\Google\Update\1.3.29.5\GoogleUpdateBroker.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 4aebb3379aadc9df4bd0d88c6141d8bb **SHA-1 :** d05ef273476789d7caee2d86d2b348b70216792f **SHA-256 :** 199c789dd762c17303e9554b0f049eea455c641a3c0016dfbcb7418ecf58e5 **SHA-512 :** db5e6149e1de624d1820dfb116aa086768ec0184f8698908a4546fd178f91 **Size :** 1581.568 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Unpack200.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** d26005bb270818cdcc004f9c513023cb **SHA-1 :** 60ccf1a15efa07b1d164761f25dd15b7d9ad622d **SHA-256 :** 7851dcac3fc940e63436952c1b5c7e5a5817f6f4ded3d027efd9455bc7ea4e **SHA-512 :** 7d1ddae12c6a03c3de0ffa68b53dc67f859993c650febab97e875fcaf210ee5 **Size :** 731.648 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Safer Networking\FileAlyzer 2\Unins000.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 543cf00f28b31dcef848cde783d43466 **SHA-1 :** e5c8ed23247c719661c1b81e9703a004b3babf34 **SHA-256 :** 9fb49a3e968622a32087a09758ff81d7b61f3cac2448f3e739d04f2fa16d3b4 **SHA-512 :** 5ef8e32f65793281080394d9937e1fd401a44d83aa800193787a15d9b18b8 **Size :** 1283.072 Kilobytes.
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDrvInst.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** cd204d11a86956a372befc2a7f9c714c **SHA-1 :** 72e5ea27209a452e6fe864850ad285fe0a24126f **SHA-256 :** ec928f94a631c93ef6c31ce47e244c5af7cbed91c634cb435caeda4e76a89b **SHA-512 :** c67e222f8b1f8868a003aff47cd891d7a8e412d3496e6f737ede26e88c3cee **Size :** 1584.64 Kilobytes.
C:\Program Files (X86)\Universal Extractor\Bin\Arc.Exe	**Type :** PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 1a3489b4481d613bed4ae072057acc59 **SHA-1 :** 6f038d84b851c01e884fc67ebde47f632c13f8dd **SHA-256 :** ecf49c286df75dd40dfcd0c1b11a8fdf0b7d7ddf308c51e60d737105dee30e **SHA-512 :** c04355920dc666c2f9523e5c387549418ba9aedd3b74ec9151fc6963b7c46 **Size :** 663.552 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Servertool.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** d121304d7deb58f42506db6b45a0a094 **SHA-1 :** 025e6dd0d0cc2b838e39bc0f6a5f6bbb0b856a77 **SHA-256 :** 4eb1afab9020c9ab4ba7cea74c243f5d69544b47fa7e8a1ded6ab7b279b09 **SHA-512 :** dd814673e64b6a19c02b9176933c37da84a513e2b808a32e083f39663d50 **Size :** 590.848 Kilobytes.
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxTray.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** c9bf141e10770d41b52e1ad949ba1bb0 **SHA-1 :** b9078606738041fef91d097e32a57964d1c56b8a **SHA-256 :** cf60fa2c7676942ff9c9174db087541cbcdf03edb7f2bb424d803a04fd2ebb4 **SHA-512 :** 290c257eb4c7bbcf3750cea063c5dfab1e1735298ce2469514e35f1688cebb **Size :** 2264.576 Kilobytes.
C:\Windows\Sysnative\Alg.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 11c0cef93baa342fd3b5bc5a99df1a72 **SHA-1 :** 547a6307c715dea041670b953a3eeee677736f83 **SHA-256 :** b781907eaeb461fc3a5c99e1c61ace038960f37aab5a50cf2f806da4924a24 **SHA-512 :** 41805da702bae2fa83853c4fd87d76aeb0eaa0ec23a40c5e0c201144ae608 **Size :** 1577.472 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Orbd.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 4c5babc00c1256bb3472f00baec6decd **SHA-1 :** 65a42cc63af76a7a668b86afff493d1c76c2211b **SHA-256 :** b661a7acb2e6bbfaed57f9ef3c66aedd9359ab43cb8e166539e46f062cccfd **SHA-512 :** 00ed0f162439d5c127eb2c3417e2e14d977bdcc35e503c8bf95b7d9ef9941 **Size :** 591.36 Kilobytes.
C:\Program Files (X86)\Google\Update\Download\{8A69D345-D564-463C-AFF1-A69D9E530F96}\48.0.2564.103\48.0.2564.103_chrome_installer.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 4fb02e4ad49287c1dbde25e3ae42d368 **SHA-1 :** 8499a8053c500ee8e5c8122be9dc89851a81ecf5 **SHA-256 :** 592646e8eb449e7dc108595d0532cea3248b8f523dd21c3d962bfb8db861 **SHA-512 :** 191c9454ebdc601631897626bfd3d0e4bf9ec92c7bd35f5105a940a3d4eba **Size :** 44903.936 Kilobytes.
C:\Program Files (X86)\Mozilla Firefox\Updater.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 33c3c5a984621cb507373288d3f7edfe **SHA-1 :** 177ac30f5a14c739af70aaa57114a2cc1b00c462 **SHA-256 :** c58537b19d2d0eecdd88814f0ab0b3d1f23d5ab042b2dcf1c8ccb9e598d70 **SHA-512 :** 6d6e16a94ed9861c76bc2e1f5cbf6b50c6ea832461087d10f63f135baefd13 **Size :** 870.912 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Jp2launcher.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 45e6cd5d5335b1b7ced90613da240731 **SHA-1 :** e77f286a0cef349730926e38fccdc9a7ec1cfbab **SHA-256 :** c3eacad1e8e3f731bf3c48ba157b62088131ec8deb0c7e67ae429dacbb8e0 **SHA-512 :** a57714d45883b7942fa3b7aec0e55dc3670ba2684c02ed41e2894dba7413 **Size :** 652.8 Kilobytes.
C:\Program Files\Sandboxie\SandboxieRpcSs.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** c7cbeb88ae3557a2ad1ee4141eab4880 **SHA-1 :** 1487165aca6fd41afd3ade7a2ab8007d05edfae3 **SHA-256 :** cb177d3d520464d245ef2e221c4245ca4392741bca6f1e3f96d028efb57095 **SHA-512 :** f59170717fe6f18a8c3eeebafb204c6d4fc523d79ad3c65508e4656df92b77 **Size :** 1527.808 Kilobytes.
C:\Mctrlc\Bin\Loader.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** bbffca6b9c7650f26c161993f96f9e7f **SHA-1 :** 8574d8252c3224918325538e032983baf00ab8fd **SHA-256 :** de8c9983a52b01fd600f8909d83aaa8a59be38452be03961a154f38bfa29f **SHA-512 :** ab5077c7d716a8f72d9ee536770b9b0ccb5ba2418939cfd7b8c39c87503a4 **Size :** 1577.984 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Common Files\Microsoft Shared\OFFICE12\Office Setup Controller\ODEPLOY.EXE	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 2278f0a081f6efe8437217e9d6b7e7c6 **SHA-1 :** eeff2645651e2221efdd4e5833e9bddbe05442cc **SHA-256 :** b64df4f1292f475c6068adfb47ba111578214c60e8c6e6a7725e345dd6e52 **SHA-512 :** 793f18f858e4cde53efaddb03019af6a23b5acee9534c13fac3b604fc5de6fc **Size :** 1726.976 Kilobytes.
C:\Program Files (X86)\Universal Extractor\Bin\AspackDie.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 2e7e9cf73f5972924b0e1c3fe92be327 **SHA-1 :** 1c4913f00362c4cbe0b2256a87600c5e622a01c8 **SHA-256 :** 8dc961dcd890589f1637413e7400a392923fdc79abf9482d77265d9f51727 **SHA-512 :** 8001d5440d55c63db2a3c1b7eabbd84686a1c786af2f28ad123f130e4c658 **Size :** 592.384 Kilobytes.
C:\Program Files (X86)\Universal Extractor\Bin\7z.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 5b4c1ce78261e258829d0cb3563d859b **SHA-1 :** 44c11ddab1f7b98e973d3b22c2a8c60d80f40ead **SHA-256 :** f13270844918a3d6e425ca01f467eb4c9456be6025819a854c86e0af64a13 **SHA-512 :** 8d007427c8ae1db7c28d93aec5dba96f00a7a636171ff4d36c3f626d2c08d4 **Size :** 742.4 Kilobytes.
C:\Program Files (X86)\Adobe\Reader 9.0\Reader\AcroTextExtractor.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 63670f8b45a270a5c3a160dceaab5b36 **SHA-1 :** 16d94d2ee4ea8460bc302ffa1f8ae6c34c86d62a **SHA-256 :** 59e855c73463ea1cf3816cc8c0a653078d1a906ddf97f43a19380e24fb92d5 **SHA-512 :** b373d8aecc49d95f6599df5d4f269dec5b6f8b3203fd98c051e91275a7cd93 **Size :** 1522.688 Kilobytes.
C:\Program Files\Sandboxie\SbieCtrl.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** b3c29d3355ffa96eff15d384edcc00c0 **SHA-1 :** d63782de342d44f427645a2205cb51257d3fc765 **SHA-256 :** def8826d7a8638626af9b87bc7a6813f9f95cba3c71f08970132930a6b7ace **SHA-512 :** 804f0f71c8b4a1fc5216d457b4cd7bd569beaffbd3d35238304dc77112b8e7 **Size :** 1359.36 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Jabswitch.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** b1d748f831b0796b16d7414bd7334f72 **SHA-1 :** 066fa23e103e11d62353dcb9b115a231bb0dd534 **SHA-256 :** 3feca0d48587bf5f04b2b602c85ba55a7e0883a2c19575b8aa31ce4455da8 **SHA-512 :** c5ba6da23cffe8bf8cf68dc0cb560f1da607f518c2cd1063c24ea0c88c8a4e0 **Size :** 1526.272 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** c442e1accd171dad199ec07b9388bac7 **SHA-1 :** ec7d4514704600dbf21f43d363b534b8abc43787 **SHA-256 :** 2396963acaf2adce62ec46a691f5e037043ba96f3f28cc9c3374d8085f3fe86 **SHA-512 :** ad6dc2b209fe3cf4863c04d7a5be85ee787c33b93b89423d07de36a3049e5 **Size :** 1933.824 Kilobytes.
C:\Windows\Ehome\Ehrecvr.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 05fbe959c3b267c451158d58e2ed7a5c **SHA-1 :** 956072ba04d856f4d7bc0024c3b19acd56bd6d3e **SHA-256 :** 174f2040f326758c88d0e1a97bf416adef3077c1e485f09e04e765257d551f **SHA-512 :** 1f22a76cfe0a94f93e9fcfe232c150656d38e07117f98aa760bf7fa95c5c12b9 **Size :** 1276.416 Kilobytes.
C:\Program Files\Sandboxie\License.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** e1534883f13b7c7ff75867810aeb3aad **SHA-1 :** bfb752bd794390dd811624e7bed6c3e3d2aae079 **SHA-256 :** 45ebf58f3414f06ca0f50e2612dba749a239a3ad5757321d7ee847fb073d6f **SHA-512 :** 187745ff334c46ec2563c59f88b50465616544a51f74bf1aac391bcd67ee1a3 **Size :** 1618.944 Kilobytes.
C:\Program Files (X86)\Adobe\Reader 9.0\Reader\Eula.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 454850c63b96442ce1c7d2a1fe88bfdb **SHA-1 :** f33bc5bee8aff48de74e8126068aac20d86a5bd4 **SHA-256 :** e4d203e694ab3c65d31155a505fc53b8f3a552c7d190b21591e1f0f570dce **SHA-512 :** 6d529131224f03a48d13ac2bbc06a6a7f5937391b8fc31b83f00d799264c97 **Size :** 1593.344 Kilobytes.
C:\Program Files\Sandboxie\SbieIni.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** e9df867b20abc1ff84e643b63ad5a9d4 **SHA-1 :** 10d33e6fb914bee6c62b51bf62238bc0a246f805 **SHA-256 :** a3f7c818a684546063ae0554b9700608a2c9d9ddd55b2f4a638696a59806a **SHA-512 :** 7746dda0a14096dd180d90caf8d1d50805f88cf66931ac6408381a7318622 **Size :** 1512.448 Kilobytes.
C:\Windows\SysWOW64\Perfhost.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 9e50a0e40330dd5724bb99ade9cd7630 **SHA-1 :** 5c05bdd81c9f3172b399644d953a7fdd29f8968d **SHA-256 :** e6017009f1b0a036a2dda578ecfe8931d4a84e43a6ba5f1fda5bfd6ecbfcd2 **SHA-512 :** 6dff712da1c0cbf1bd5bfcd7f0fa433a72faab5da3c3b8726735afb517f42b4 **Size :** 1519.104 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Common Files\Microsoft Shared\Smart Tag\SmartTagInstall.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** ed342b6ac7acae83f085b5e5ee6c2c3b **SHA-1 :** 289ad2bb03fc0f0e31da92f387be81e1826c0053 **SHA-256 :** 40fef61581c387c3ca990f306e757dcbb9b5f6103c3dceba261f7c4bd6429c **SHA-512 :** 2abea57e9ccde4a44a3d942b60805a9ad3d707a0ff9d94402950a341a512c **Size :** 1507.328 Kilobytes.
C:\Windows\Temp\Fwtsqmfile00.Sqm	**Type :** data **MD5 :** e4be0e1e2c0956c15660d1b27f6f4471 **SHA-1 :** aecabd73c82aba28d500f523dc00ffb0e835d345 **SHA-256 :** 99c0b012fec3c0539e3d8b6f6eec88f0c854aae8c458bbbcfea2007624c142 **SHA-512 :** 2dc48666578d5a4b44de06dacda469d8693271545f75aed8f7286341ba5f3 **Size :** 0.14 Kilobytes.
C:\Bevevnhfi\Bin\YFFKvqC.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** ff05163b4fd87686779f04e38d0190e8 **SHA-1 :** 2828a64752cba0ec7e65a32f01dcaa85027ba61e **SHA-256 :** c8976c5f18318c2a28b8fa02a53dbca2957f8a4814507841190b300231bcfc **SHA-512 :** 4f5192e635d983cf8061ed92569068cb64c73e26584774d64878be8c90a13 **Size :** 1577.984 Kilobytes.
C:\Program Files (X86)\Google\Update\1.3.29.5\GoogleUpdateSetup.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 354b9c4db9daa10dddfd5e4d18e6d446 **SHA-1 :** 13c5913d7e10c0612b82b2f551456fdf411d1bc2 **SHA-256 :** 71d715bd8f0724dc2e24bd255ba0f2190e4ddf5f8dad6825807eb56c1b2fa **SHA-512 :** 6111a37b645364b3c112495626e8e80cc6caceb7cd50bf892f74b7d0446b5 **Size :** 1546.752 Kilobytes.
C:\Program Files (X86)\Universal Extractor\Bin\Bin2iso.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 9cec014174332aa34dcf2d51a96e5f4d **SHA-1 :** 28437d556ac076424cf9e95818740a97276703d9 **SHA-256 :** 464e6841dd5276cfbfbf3cd654386ea3ae53162eb2a7e849bffb67dc7ad9d **SHA-512 :** 57de8c6ad7f4231c1f30a24ee43343372d6fee3618ac5adef84969f2c1813f7 **Size :** 638.976 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\Phone Tools\12.0\Debugger\Target\X86\Dxcap.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 4360573398d41028cb17fae552bd3066 **SHA-1 :** 669d09ffbb3c18c27da557c74cf2d65af490c3c2 **SHA-256 :** a430fbd32bf2c4068587660684ea62ffe7523c6010b0bf776a80b59811d248 **SHA-512 :** b172edd861cf3fe57dba10a2091602905a8f13f42df071ea88d607e0903ed5 **Size :** 1167.872 Kilobytes.
C:\Program Files (X86)\Google\Update\1.3.29.5\GoogleUpdateWebPlugin.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 266048c0ab3eb763fdb8095c379a566a **SHA-1 :** cff4c10aca30ec32c9b98b13e240cdb49f16a1fb **SHA-256 :** c57654b269307099f22146da2eb81081121308968ce15a5bfb4492e6da682 **SHA-512 :** 54452945e010ded773d2d13407f3b9cbc4fa670199e1587683bf9967baf67 **Size :** 1581.568 Kilobytes.
C:\Program Files (X86)\Mozilla Firefox\Wow_helper.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** f14a144c9a5af66d400e41578d0a9030 **SHA-1 :** bad60f0cf98b5bdfb2b40e0ec596b1ae2091610b **SHA-256 :** 0b560895644d1aaf5f0ea5248dcf19da162483b0cefd14e95e4c36cd0f3ff03 **SHA-512 :** 45a0ac6bc447713d08f87ca5ba54557df4f372fcd0fd8d752cf45e4ff761b58 **Size :** 679.424 Kilobytes.
C:\Program Files (X86)\Common Files\Microsoft Shared\DW\DW20.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 0e7a82624ac0d146d94920e78293ec7f **SHA-1 :** 7567d87eab447e7779012727707c483f6f443a27 **SHA-256 :** 42df7a25a7df3d939e925a92bc0ddd6e5e95815f2c536fab3d3416538773c **SHA-512 :** 4446de43ca557e8f4b9f08f8ee81155232afcc24c30a53c45f836e9587c3a2f **Size :** 1387.008 Kilobytes.
C:\Program Files (X86)\Java\Jre1.8.0_91\Bin\Keytool.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 3987d59919c7be28e93e9f6048daaa8d **SHA-1 :** 50feb5f6e9c21926713c860d0be7f566b09854d4 **SHA-256 :** 893fb31f69ffff0b6f8c73adc643892a2ba897f95c2da78b4dc02c99d67da94 **SHA-512 :** 304e2c49366e82675d641e49088a56b585434dfcc52a38a393ee0ebf4acd8 **Size :** 590.848 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	virussign.com_5c9bbe8e5b749efba278eabd96c9cbe1.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
SHA1:	3b48a7ed61ab4ca62ecd8591bfdec38c3cf0493d
MD5:	5c9bbe8e5b749efba278eabd96c9cbe1
First Seen Date:	2024-11-08 22:57:29.177953 (about 13 hours ago)
Number Of Clients Seen:	2
Last Analysis Date:	2024-11-08 22:57:29.177953 (about 13 hours ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	4
File Type Enum	7
Debug Artifacts	[{u'Path': u'c:\\jenkins\\workspace\\8-2-build-windows-x64-cygwin-sans-NAS\\jdk8u421\\1068\\build\\windows-x64\\jdk\\objs\\javaw_objs\\javaw.pdb\x00', u'GUID': u'{9891f28f-2fd4-4bfa-9f00-f464ea908bdf}', u'timestamp': u'2024-06-05 13:07:49'}]
Number Of Sections	7
Trid	[[87.3, u'Win64 Executable (generic)'], [6.3, u'Generic Win/DOS Executable'], [6.3, u'DOS Executable Generic']]
Compilation Time Stamp	0x66606325 [Wed Jun 5 13:07:49 2024 UTC]
LegalCopyright	Copyright \xa9 2024
InternalName	javaw
FileVersion	8.0.4210.9
Full Version	1.8.0_421-b09
CompanyName	Oracle Corporation
ProductName	Java(TM) Platform SE 8
ProductVersion	8.0.4210.9
FileDescription	Java(TM) Platform SE binary
OriginalFilename	javaw.exe
Translation	0x0000 0x04b0
Entry Point	0x14000a924 (.text)
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
File Size	1800192
Ssdeep	12288:8WvMfP4oXJRfDtCxOvUlUMAdB8qr0zw9iXQ40AOzDr5YJjsF/5v3ZkHRik8:WYoXTBCRlatr0zAiX90z/F0jsFB3SQk
Sha256	4faa1da15bd140561572811aa24fac4ef4754e9532784ea3617d822109eba687
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/b/4/8/3b48a7ed61ab4ca62ecd8591bfdec38c3cf0493d', u'EXE:OriginalFileName': u'javaw.exe', u'EXE:ProductName': u'Java(TM) Platform SE 8', u'EXE:InternalName': u'javaw', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:11:08 22:56:30+00:00', u'EXE:InitializedDataSize': 119296, u'File:FileModifyDate': u'2024:11:08 22:55:04+00:00', u'EXE:FileVersionNumber': u'8.0.4210.9', u'EXE:FileVersion': u'8.0.4210.9', u'File:FileSize': u'1758 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'AMD AMD64', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'8.0.4210.9', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win64 EXE', u'EXE:CompanyName': u'Oracle Corporation', u'File:FileName': u'3b48a7ed61ab4ca62ecd8591bfdec38c3cf0493d', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 6.0, u'EXE:FullVersion': u'1.8.0_421-b09', u'EXE:PEType': u'PE32+', u'EXE:TimeStamp': u'2024:06:05 13:07:49+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 2024', u'EXE:LinkerVersion': 14.36, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/b/4/8', u'EXE:FileDescription': u'Java(TM) Platform SE binary', u'EXE:EntryPoint': u'0xa924', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 178688, u'File:FileInodeChangeDate': u'2024:11:08 22:56:09+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'8.0.4210.9'}]
Mime Type	application/x-dosexec
Imphash	7f50f83d25f2da4d5784abfb6c7708d0

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2b940	0x2ba00	6.53499061942	7bc197384b8ffd3497b6cda2aa2f91c1
.rdata	0x2d000	0x116d2	0x11800	5.83926815542	ab680b6211e8428cfe79a7671f5e6cd6
.data	0x3f000	0x2240	0xe00	1.92623397407	22bca0ee661ba38ad7a2d6159f912fcd
.pdata	0x42000	0x1f98	0x2000	5.42459397031	e7b7534033d25407995ab31351ee34e5
_RDATA	0x44000	0x15c	0x200	2.76413452983	35309e5a16b10dda5f9aa5d8b874b036
.rsrc	0x45000	0x81c4	0x8200	6.01596187032	729cdc8d096a9283cdde642b6b9d855e
.reloc	0x4e000	0x170000	0x16f000	3.98415743826	d14457ad155ce48ded4a3b522f8b5a16

PE Imports

- ADVAPI32.dll
  - RegEnumKeyA
  - RegOpenKeyExA
  - RegQueryValueExA
  - RegCloseKey
- USER32.dll

- CharNextExA
- MessageBoxA

- COMCTL32.dll
  - InitCommonControlsEx
- KERNEL32.dll
  - GetTimeZoneInformation
  - HeapSize
  - GetFileSizeEx
  - GetCommandLineA
  - CloseHandle
  - GetLastError
  - QueryPerformanceCounter
  - QueryPerformanceFrequency
  - WaitForSingleObject
  - GetExitCodeProcess
  - GetExitCodeThread
  - CreateProcessA
  - FreeLibrary
  - GetModuleFileNameA
  - GetModuleHandleA
  - GetProcAddress
  - LoadLibraryA
  - LocalFree
  - FormatMessageA
  - FindClose
  - FindFirstFileA
  - FindNextFileA
  - RtlCaptureContext
  - RtlLookupFunctionEntry
  - RtlVirtualUnwind
  - UnhandledExceptionFilter
  - SetUnhandledExceptionFilter
  - GetCurrentProcess
  - TerminateProcess
  - IsProcessorFeaturePresent
  - GetCurrentProcessId
  - GetCurrentThreadId
  - GetSystemTimeAsFileTime
  - InitializeSListHead
  - IsDebuggerPresent
  - GetStartupInfoW
  - GetModuleHandleW
  - SetEndOfFile
  - RtlUnwindEx
  - SetLastError
  - EnterCriticalSection
  - LeaveCriticalSection
  - DeleteCriticalSection
  - InitializeCriticalSectionAndSpinCount
  - TlsAlloc
  - TlsGetValue
  - TlsSetValue
  - TlsFree
  - LoadLibraryExW
  - EncodePointer
  - RaiseException
  - RtlPcToFileHeader
  - GetCommandLineW
  - ExitProcess
  - GetModuleHandleExW
  - SetFilePointerEx
  - CreateThread
  - ExitThread
  - FreeLibraryAndExitThread
  - CreateFileW
  - GetDriveTypeW
  - GetFileInformationByHandle
  - GetFileType
  - PeekNamedPipe
  - SystemTimeToTzSpecificLocalTime
  - FileTimeToSystemTime
  - GetStdHandle
  - WriteFile
  - GetModuleFileNameW
  - ReadFile
  - GetConsoleMode
  - ReadConsoleW
  - HeapAlloc
  - HeapFree
  - FlsAlloc
  - FlsGetValue
  - FlsSetValue
  - FlsFree
  - CompareStringW
  - LCMapStringW
  - MultiByteToWideChar
  - WideCharToMultiByte
  - IsValidCodePage
  - GetACP
  - GetOEMCP
  - GetCPInfo
  - GetEnvironmentStringsW
  - FreeEnvironmentStringsW
  - SetEnvironmentVariableW
  - SetStdHandle
  - GetConsoleOutputCP
  - HeapReAlloc
  - GetFileAttributesExW
  - FlushFileBuffers
  - GetCurrentDirectoryW
  - GetFullPathNameW
  - FindFirstFileExW

- FindNextFileW
- GetStringTypeW
- GetProcessHeap
- WriteConsoleW

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 283456, u'sha256': u'afb87caf3186370a597d066b19f0f74e4acfaf0a8e5e5f569e2da75def3ffc43', u'type': u'data', u'size': 1640}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 285096, u'sha256': u'1ff1edfe7779b95b24553fe1eeac40f72ce79a0bb2cbc8b711b7bf8265d5ee47', u'type': u'data', u'size': 744}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 285840, u'sha256': u'f26171f3baeb9ccf71e80b12f92838a487f434119d12190cc1c8c4efbf0906f0', u'type': u'data', u'size': 488}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 286328, u'sha256': u'46ae400026b2c61a308e02b36c84e994328786a23a51059a72fc0ee038ebac3e', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 286624, u'sha256': u'467e07c1e3bcf890c4a61c9e1a675aab9dff875fc3b95648fe0cb6b5c76c0c11', u'type': u'data', u'size': 3752}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 290376, u'sha256': u'37922e311d3ba1cc04eda58d19f0fb513ba48b50841791aa0e2b4f4241591e06', u'type': u'data', u'size': 2216}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 292592, u'sha256': u'fceb63fb5ea6edbe9a8f50e449e5041a9c8622c7b4a0a0d2bd332fa4298138ef', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 1736}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 294328, u'sha256': u'18830062c5276e87697169f9f359efb15aeb41e8a0ecc79a3c320845f64ca21f', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 295712, u'sha256': u'752046db2d5ba9b48214cfdc907886277a63ca3638eb1d38a00f207878da0a7d', u'type': u'data', u'size': 9640}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 305352, u'sha256': u'f39679918b57ed83da31c7cb81d5ace2b1409700628cb3ece4224c3f143c29fb', u'type': u'data', u'size': 4264}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 309616, u'sha256': u'b72e0c24aaa3ead9220fd1b21e60c2adfe048c83c7bce3e98cb2207615777c30', u'type': u'data', u'size': 2440}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 312056, u'sha256': u'4e7aa9843e2f6b206a9b0fbc7e0edcd910b2cbdb0d103644c8fce426bb90415f', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 313184, u'sha256': u'd2d8ccd68849e94ea6b84f6835d0fe98ffa5c11e74a1138529e3c0b8d8edfe60', u'type': u'MS Windows icon resource - 12 icons, 48x48, 16 colors', u'size': 174}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 313360, u'sha256': u'58b8f3b4285c0e262d58304841df69aae64412981b72d81e3d364a8141176655', u'type': u'data', u'size': 820}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 314180, u'sha256': u'4a3462d35e635faf3b7763ba7ff3e6fd25c32579748f9bdc31c786ff30d3ed14', u'type': u'exported SGML document, ASCII text', u'size': 1661}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS