VALKYRIE COMODO

Summary

File Name: b205887a3a508292114e32d15e9a1d459ed53061

File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

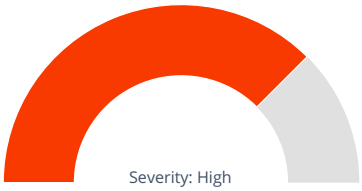
SHA1: b205887a3a508292114e32d15e9a1d459ed53061

MD5: 8a2e7ac98d1b90027d2302978b9f2a0b

MALWARE

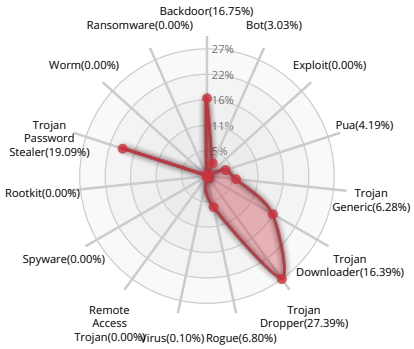
Valkyrie Final Verdict

DETECTION SECTION

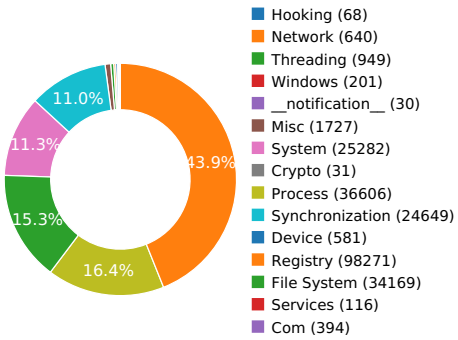


Verdict: Malware

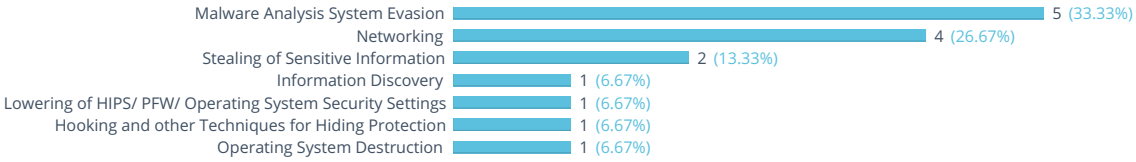
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (5 unique times)	Show sources
Starts servers listening on 127.0.0.1:0	
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system	Show sources
Attempts to modify proxy settings	

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

OPERATING SYSTEM DESTRUCTION

At least one process apparently crashed during execution	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects VirtualBox through the presence of a registry key	Show sources
Checks the version of Bios, possibly for anti-virtualization	Show sources
A process attempted to delay the analysis task by a long amount of time.	Show sources
Tries to unhook or modify Windows functions monitored by Cuckoo	Show sources
Attempts to repeatedly call a single API many times in order to delay analysis time	Show sources

VALKYRIE COMODO

Behavior Graph

02:49:04 02:51:42 02:54:19

PID 2916

02:49:04 **Create Process** The malicious file created a child process as b205887a3a508292114e32d15e9a1d459ed53061.exe **(PPID 2868)**

02:49:04 NtAllocateVirtualMem

PID 2052

02:49:08 **Create Process** The malicious file created a child process as eb5osassgqg.exe **(PPID 2916)**

02:49:09 02:49:09 NtReadFile **[4 times]**

PID 1620

02:49:10 **Create Process** The malicious file created a child process as eb5osassgqg.tmp **(PPID 2052)**

02:49:11 NtDelayExecution

PID 2100

02:49:11 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:49:12 __anomaly__

02:49:14 connect

02:49:14 NtDelayExecution

02:49:14 GetSystemTimeAsFileT

02:49:15 GetSystemTime

02:49:15 02:49:15 GetSystemTimeAsFileTi **[2 times]**

02:49:15 RegQueryValueExW

02:49:15 02:49:18 GetSystemTimeAsFileTi **[11 times]**

02:49:18 GetSystemTime

02:49:19 02:49:23 GetSystemTimeAsFileTi **[10 times]**

02:49:23 GetSystemTime

02:49:24 02:49:24 GetSystemTimeAsFileTi **[4 times]**

02:49:24 GetSystemTime

02:49:24 GetSystemTimeAsFileT

02:49:26 02:49:26 GetSystemTime **[2 times]**

02:49:26 GetSystemTimeAsFileT

02:49:34 02:49:35 GetSystemTime **[4 times]**

02:49:35 02:49:36 GetSystemTimeAsFileTi **[3 times]**

02:49:36 GetSystemTime

02:49:37 GetSystemTimeAsFileT

PID 2736

02:49:23 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:49:24 __anomaly__

PID 1724

02:49:36 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:49:37 __anomaly__

PID 1712

02:49:50 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:49:51 __anomaly__

PID 716

02:50:04 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:50:05 __anomaly__
02:50:06 connect
02:50:06 GetSystemTimeAsFileT
02:50:07 GetSystemTime
02:50:07 02:50:10 GetSystemTimeAsFileTi **[6 times]**
02:50:10 02:50:10 GetSystemTime **[2 times]**
02:50:10 02:50:12 GetSystemTimeAsFileTi **[6 times]**
02:50:12 GetSystemTime
02:50:12 GetSystemTimeAsFileT
02:50:13 GetSystemTime
02:50:13 02:50:13 GetSystemTimeAsFileTi **[4 times]**
02:50:14 02:50:14 GetSystemTime **[2 times]**
02:50:14 02:50:19 GetSystemTimeAsFileTi **[5 times]**
02:50:22 GetSystemTime
02:50:23 GetSystemTimeAsFileT
02:50:25 GetSystemTime
02:50:26 02:50:29 GetSystemTimeAsFileTi **[4 times]**
02:50:35 02:50:38 GetSystemTime **[12 times]**
02:50:42 GetSystemTimeAsFileT
02:50:43 02:50:53 GetSystemTime **[26 times]**
02:50:54 GetSystemTimeAsFileT
02:50:54 02:50:55 GetSystemTime **[2 times]**
02:50:56 02:51:00 GetSystemTimeAsFileTi **[7 times]**
02:51:02 GetSystemTime
02:51:02 GetSystemTimeAsFileT
02:51:02 02:51:04 GetSystemTime **[2 times]**
02:51:07 GetSystemTimeAsFileT
02:51:07 02:51:08 connect **[2 times]**
02:51:09 GetSystemTime
02:51:10 02:51:10 GetSystemTimeAsFileTi **[2 times]**
02:51:10 02:51:11 GetSystemTime **[2 times]**
02:51:11 GetSystemTimeAsFileT
02:51:14 GetSystemTime
02:51:15 02:51:19 GetSystemTimeAsFileTi **[2 times]**
02:51:21 02:51:24 GetSystemTime **[3 times]**
02:51:25 GetSystemTimeAsFileT

02:51:25 GetSystemTime

02:51:25 02:51:26 GetSystemTimeAsFileTi [3 times]

02:51:27 connect

02:51:27 02:51:35 GetSystemTimeAsFileTi [11 times]

PID 2376

02:50:19 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:50:20 __anomaly__

PID 2084

02:50:31 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:50:32 __anomaly__

PID 1920

02:50:45 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:50:46 __anomaly__

PID 3012

02:50:55 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:50:56 __anomaly__

PID 2696

02:51:04 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:51:06 __anomaly__

PID 2272

02:51:13 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:51:15 __anomaly__

PID 984

02:51:20 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:51:22 __anomaly__

PID 1976

02:51:28 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

PID 2764

02:51:38 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:51:40 __anomaly__

PID 2280

02:51:48 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

02:51:49 __anomaly__

PID 3044

02:54:19 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1620)**

PID 460

02:49:15 **Create Process** The malicious file created a child process as services.exe **(PPID 352)**

02:49:16 Create Process

02:49:31 Create Process

02:49:39 Create Process

02:50:01 Create Process

02:50:09

02:50:19 Create Process

PID 1612

02:49:16 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

PID 2080

02:49:34 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

02:49:35 NtDelayExecution

02:49:40 RegOpenKeyExW

PID 224

02:49:46 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

02:49:46 LdrLoadDll

02:49:47 Create Process

02:49:47 Create Process

PID 1388

02:49:48 **Create Process** The malicious file created a child process as WerFault.exe **(PPID 224)**

PID 2816

02:49:48 **Create Process** The malicious file created a child process as WerFault.exe **(PPID 224)**

PID 2532

02:50:16 **Create Process** The malicious file created a child process as mscorsvw.exe **(PPID 460)**

PID 2824

02:50:26 **Create Process** The malicious file created a child process as mscorsvw.exe **(PPID 460)**

PID 2164

02:50:37 **Create Process** The malicious file created a child process as sppsvc.exe **(PPID 460)**

PID 584

02:49:30 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

02:50:02 RegOpenKeyExW

PID 1672

02:50:35 **Create Process** The malicious file created a child process as WmiPrvSE.exe **(PPID 584)**

02:50:38 NtDelayExecution

02:50:57 RegQueryValueExW

PID 752

02:51:13 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

PID 876

02:51:34 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\sysnative\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64*
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\b205887a3a508292114e32d15e9a1d459ed53061.exe.config
C:\Users\user\AppData\Local\Temp\b205887a3a508292114e32d15e9a1d459ed53061.exe
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Users\user\AppData\Local\Temp\b205887a3a508292114e32d15e9a1d459ed53061.exe.Local\
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows
C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework64\v4.0.30319
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\fusion.localgac
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll

C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.INI
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\ole32.dll
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\b205887a3a508292114e32d15e9a1d459ed53061.config
C:\Users\user\AppData\Local\Temp\b205887a3a508292114e32d15e9a1d459ed53061.INI
C:\Windows\sysnative\l_intl.nls
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.INI
C:\Windows\Globalization\en-us.nlp
C:\Users\user\AppData\Roaming\okjvcpzimba
C:\Users\user\AppData\Roaming
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\091b931d0f6408001747dbbbb05dbe66\System.Configuration.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Configuration\2.0.0.0__b03f5f7f11d50a3a\System.Configuration.INI
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Xml\ee795155543768ea67eecddc686a1e9e\System.Xml.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Xml\2.0.0.0__b77a5c561934e089\System.Xml.INI
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Users\user\AppData\Roaming\okjvcpzimba\eb5osassgqg.exe
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\rasapi32.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\ws2_32.dll
C:\Windows\Globalization\en.nlp
C:\Windows\sysnative\tzres.dll
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\winhttp.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\iphlpapi.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\shell32.dll
\??\MountPointManager
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.2916.13284562

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,AMD64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CseOn
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TailCallOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeInline
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeCalliOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\NewGCCalc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TURNOFFDEBUGINFO
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableHotCold
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\Latest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\index20

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\LegacyPolicyTimeStamp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System,2.0.0.0,,b77a5c561934e089,MSIL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System.Xml,2.0.0.0,,b77a5c561934e089,MSIL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System.Configuration,2.0.0.0,,b03f5f7f11d50a3a,MSIL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\159a66b8\424bd4d8\8f\DisplayName

MODIFIED FILES

C:\Users\user\AppData\Roaming\okjvcpzimba\eb5osassgqg.exe
C:\Users\user\AppData\Local\Temp\is-4LGGU.tmp\eb5osassgqg.tmp
C:\Users\user\AppData\Local\Temp\is-FUMBU.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-FUMBU.tmp\idp.dll
C:\Users\user\AppData\Local\Temp\is-FUMBU.tmp\itdownload.dll
C:\Users\user\AppData\Local\Temp\is-FUMBU.tmp\psvince.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\parent.lock
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\trash14474
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.tmp
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\doomed\19097
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cert8.db

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\key3.db
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\permissions.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\content-prefs.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs.js
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs-1.js
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-shm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
\??\WMIDataDevice
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
C:\Users\user\AppData\Local\CrashDumps\2100.dmp
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps.json
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps-1.json
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\formhistory.sqlite
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\9BBE93EE66A24A6574E0B0B292F1184CC816B4A0
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-shm
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\A99600C554190746CFE12AB84669C4348512333A
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\B1BF484310B181937E88AFC02D2B2F23B1FBCC38
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\SiteSecurityServiceState.txt
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\mimeTypes.rdf
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing-backup
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenservicelock.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenrootstorelock.dat

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenofflinequeuelock.dat
C:\Windows\Microsoft.NET\ngenservice_pri3_lock.dat
C:\Windows\Microsoft.NET\ngennicupdatelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenservicelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenrootstorelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenofflinequeuelock.dat
\??\SPDevice
C:\Windows\SoftwareDistribution\ReportingEvents.log
\Device\LanmanDatagramReceiver

RESOLVED APIS

advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx

kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCMapStringEx
kernel32.dll.GetTickCount64
advapi32.dll.EventRegister
mscoree.dll.#142
mscoreei.dll.RegisterShimImplCallback
mscoreei.dll.OnShimDllMainCalled
mscoreei.dll._CorExeMain
shlwapi.dll.UrlIsW
version.dll.GetFileVersionInfoSizeW
version.dll.GetFileVersionInfoW
version.dll.VerQueryValueW
kernel32.dll.InitializeCriticalSectionAndSpinCount
msvcrt.dll._set_error_mode
msvcrt.dll.?set_terminate@@YAP6AXXZP6AXXZ@Z
kernel32.dll.FindActCtxSectionStringW
kernel32.dll.GetSystemWindowsDirectoryW
mscoree.dll.GetProcessExecutableHeap
mscoreei.dll.GetProcessExecutableHeap
mscorwks.dll._CorExeMain
mscorwks.dll.GetCLRFunction
advapi32.dll.RegisterTraceGuidsW
advapi32.dll.UnregisterTraceGuids
advapi32.dll.GetTraceLoggerHandle
advapi32.dll.GetTraceEnableLevel
advapi32.dll.GetTraceEnableFlags
advapi32.dll.TraceEvent
mscoree.dll.IEE
mscoreei.dll.IEE
mscorwks.dll.IEE
mscoree.dll.GetStartupFlags
mscoreei.dll.GetStartupFlags
mscoree.dll.GetHostConfigurationFile
mscoreei.dll.GetHostConfigurationFile
mscoreei.dll.GetCORVersion
mscoree.dll.GetCORSystemDirectory
mscoreei.dll.GetCORSystemDirectory_RetAddr
mscoreei.dll.CreateConfigStream
ntdll.dll.RtlVirtualUnwind
kernel32.dll.IsWow64Process

advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation
advapi32.dll.InitializeAcl

DELETED FILES

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.2916.13284562
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2916.13284562
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2916.13284578
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\doomed
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.log
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.tmp
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\doomed\19097
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\trash14474\12328
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\trash14474
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs-1.js
C:\Users\user\AppData\Local\CrashDumps\OLLYDBG.EXE.3040.dmp
C:\Users\user\AppData\Local\CrashDumps\2100.dmp
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps-1.json
C:\Users\user\AppData\Local\Temp\mozilla-temp-files
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-wal
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\B1BF484310B181937E88AFC02D2B2F23B1FBCC38
C:\Users\user\AppData\Local\Mozilla\updates\E7CF176E110C211B\update.test
C:\Program Files (x86)\Mozilla Firefox\update.test
C:\Program Files (x86)\update.test
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing
C:\Windows\Microsoft.NET\ngenserviceclientlock.dat
C:\Windows\Microsoft.NET\ngenservice_pri0_lock.dat
C:\Windows\Microsoft.NET\ngenservice_pri1_lock.dat
C:\Windows\Microsoft.NET\ngenservice_pri2_lock.dat

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\v4.0
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\standards\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\AppPatch
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000\mscorwks.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\b205887a3a508292114e32d15e9a1d459ed53061.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_CURRENT_USER\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\LocalIntranet
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\NIUsageMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\LastModTime
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\GACChangeNotification\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,AMD64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\6e395930\14689ee5
HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CseOn
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TailCallOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeInline
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeCalliOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\NewGCCalc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TURNOFFDEBUGINFO
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableHotCold
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\internal\jit\Perf

EXECUTED COMMANDS

C:\Users\user\AppData\Roaming\okjvcpzimba\eb5osassgqg.exe /VERYSILENT
http://laserveradedomaina.com/redirect/57a764d042bf8/
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
C:\Windows\system32\svchost.exe -k netsvcs
C:\Windows\System32\svchost.exe -k WerSvcGroup
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
C:\Windows\system32\sppsvc.exe
C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 1940
C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 1936

READ FILES

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\b205887a3a508292114e32d15e9a1d459ed53061.exe.config
C:\Users\user\AppData\Local\Temp\b205887a3a508292114e32d15e9a1d459ed53061.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
\Device\KsecDD
C:\Windows\sysnative\l_intl.nls
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\091b931d0f6408001747dbbbb05dbe66\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Xml\ee795155543768ea67eecddc686a1e9e\System.Xml.ni.dll
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\sysnative\tzres.dll
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Roaming\okjvcpzimba\eb5osassgqg.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\is-FUMBU.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-FUMBU.tmp\idp.dll
C:\Users\user\AppData\Local\Temp\is-FUMBU.tmp\itdownload.dll
C:\Users\user\AppData\Local\Temp\is-FUMBU.tmp\psvince.dll
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Program Files (x86)\Mozilla Firefox\mozglue.dll
C:\Windows\System32\version.dll
C:\Program Files (x86)\Mozilla Firefox\msvcr120.dll
C:\Program Files (x86)\Mozilla Firefox\msvcp120.dll
C:\Program Files (x86)\Mozilla Firefox\dependentlibs.list

C:\Program Files (x86)\Mozilla Firefox\nss3.dll
C:\Windows\System32\winmm.dll
C:\Windows\System32\wsock32.dll
C:\Program Files (x86)\Mozilla Firefox\sandboxbroker.dll
C:\Program Files (x86)\Mozilla Firefox\lgpllibs.dll
C:\Program Files (x86)\Mozilla Firefox\xul.dll
C:\Program Files (x86)\Mozilla Firefox\icuin56.dll
C:\Program Files (x86)\Mozilla Firefox\icuuc56.dll
C:\Program Files (x86)\Mozilla Firefox\icudt56.dll
C:\Windows\System32\netapi32.dll
C:\Windows\System32\netutils.dll
C:\Windows\System32\srvcli.dll
C:\Windows\System32\msimg32.dll
C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\wtsapi32.dll
C:\Windows\System32\pdh.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004b.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Crash Reports\InstallTime20160502172042
C:\Users\user\AppData\Local\Mozilla\updates\E7CF176E110C211B\updates\0\update.status
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\parent.lock
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\compatibility.ini
C:\Program Files (x86)\Mozilla Firefox\omni.ja
C:\Program Files (x86)\Mozilla Firefox\browser\omni.ja
C:\Windows\System32\tzres.dll
C:\Program Files (x86)\Mozilla Firefox\chrome.manifest

MUTEXES

Global\CLR_CASOFF_MUTEX
Global\.net clr networking
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000

Local\!IETld!Mutex
Local\FirefoxStartupMutex
Local\MSCTF.Asm.MutexDefault1
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
Local\WininetStartupMutex
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex
Local\WERReportingForProcess2100
DBWinMutex
Global\32085519-c546-11e8-b76c-0800275ed07b
Global\MozillaUpdateMutex-AWkbzLFmEHPmIFtactC8kpT7UdM=

STARTED SERVICES

FontCache
WerSvc

MODIFIED REGISTRY KEYS

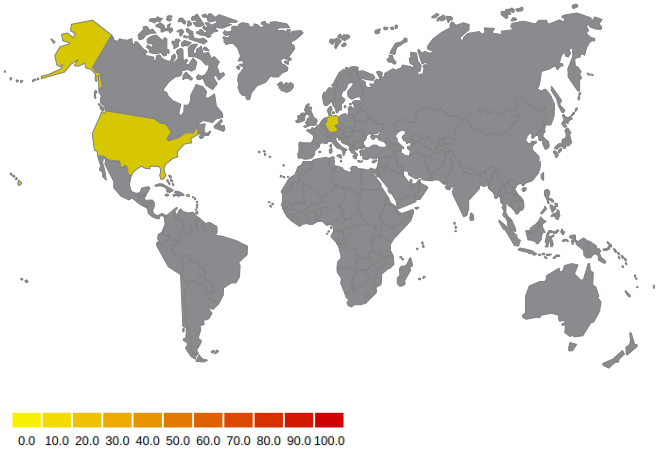
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\b205887a3a508292114e32d15e9a1d459ed53061_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\b205887a3a508292114e32d15e9a1d459ed53061_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\b205887a3a508292114e32d15e9a1d459ed53061_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\b205887a3a508292114e32d15e9a1d459ed53061_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\b205887a3a508292114e32d15e9a1d459ed53061_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\b205887a3a508292114e32d15e9a1d459ed53061_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\b205887a3a508292114e32d15e9a1d459ed53061_RASAPI32\FileDirectory
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Winmgmt\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WerSvc\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_64\Start
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ProcessID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ThrottleDrege
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Winmgmt\Parameters\ServiceDllUnloadOnStop
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
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\Wow6432Node\Microsoft\Windows\Windows Error Reporting\Debug\ExceptionRecord
HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting\Debug\UIHandles\FirstLevelConsentDialog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug\UIHandles\FirstLevelConsentDialog
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Accessibility, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\AspNetMMCExt, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\AuditPolicyGPManagedStubs.Interop, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\BDATunePIA, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/aspnet_intern.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/aspnet_merge.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/AxImp.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/lc.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/ResGen.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SecAnnotate.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/sgen.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SqlMetal.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SvcUtil.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/TlbExp.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/TlbImp.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/WinMDExp.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/wsdl.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/xsd.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/xsltc.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/ComSvcConfig.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/dfsvc.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/MSBuild.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/SMSvcHost.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/WsatConfig.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ComSvcConfig, Version=3.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\CustomMarshalers, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=x86\1\RuntimeVersion

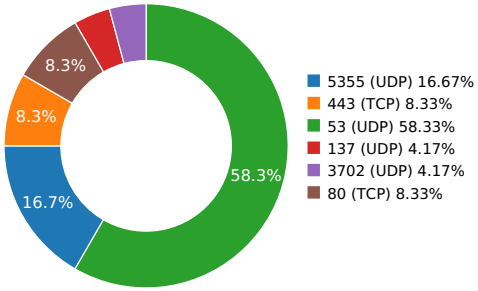
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\dfsvc, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ehexthost32, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ehiExtens, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\EventViewer, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\mcstoredb, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Activities.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.ApplicationId.Framework, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.ApplicationId.RuleWizard, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Conversion.v3.5, Version=3.5.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Conversion.v4.0, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Engine, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Engine, Version=3.5.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Engine, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Framework, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Framework, Version=3.5.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Tasks, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Tasks.v3.5, Version=3.5.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Tasks.v4.0, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	69.195.158.194	United States	19969	Joe's Datacenter, LLC	Malware Process
laserveradedomaina.com	176.31.115.114	France	16276		Malware Process
secure.informaction.com	69.195.158.198	United States	19969	Joe's Datacenter, LLC	Malware Process
a652.dscb.akamai.net	23.192.125.97	United States	20940	Akamai Technologies, Inc.	Malware Process
asedownloadgate.com	46.105.121.115	France	16276		Malware Process
notification.adblockplus.org	148.251.12.230	Germany	24940		Malware Process
easylist-downloads.adblockplus.org	148.251.66.238	Germany	24940		Malware Process
ocsp.comodoca.com	23.192.125.97	United States	20940	Akamai Technologies, Inc.	OS Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
asedownloadgate.com	80	GET	1.1		1	11.4068050385
Path: /safe_download/582369/AdsShow.exe **URI:** http://asedownloadgate.com/safe_download/582369/AdsShow.exe						

DNS QUERIES

Request	Type
asedownloadgate.com	A
Answers - 46.105.121.115 (A)	
notification.adblockplus.org	A

Request	Type
Answers - 136.243.55.39 (A) - 78.46.39.215 (A) - 94.130.73.110 (A) - 46.4.7.165 (A) - easylist-downloads.adblockplus.org (CNAME) - 176.9.139.5 (A) - 5.9.15.86 (A) - 176.9.122.53 (A) - 178.63.70.146 (A) - 78.47.138.56 (A) - 46.4.115.44 (A) - 148.251.66.238 (A) - 144.76.137.80 (A) - 94.130.73.103 (A) - 176.9.26.105 (A) - 95.216.27.32 (A) - 94.130.104.89 (A) - 78.46.93.235 (A) - 136.243.22.80 (A) - 94.130.104.85 (A) - 148.251.139.76 (A)	
easylist-downloads.adblockplus.org	A
Answers - 88.198.17.12 (A) - 94.130.73.111 (A) - 94.130.228.214 (A) - 148.251.12.230 (A) - 144.76.219.20 (A) - 144.76.153.101 (A) - 94.130.104.87 (A) - 94.130.73.107 (A) - 144.76.100.145 (A) - 144.76.197.80 (A)	
easylist-downloads.adblockplus.org	AAAA
Answers - 2a01:4f9:2a:1b61::2 (AAAA) - 2a01:4f9:2a:1b5a::2 (AAAA) - 2a01:4f8:110:50e6::2 (AAAA) - 2a01:4f8:200:9218::2 (AAAA)	
secure.informaction.com	A
Answers - 69.195.158.196 (A) - 69.195.158.198 (A) - 69.195.158.195 (A) - 69.195.158.197 (A) - 69.195.158.194 (A)	
laserveradedomaina.com	A
Answers - 188.165.209.131 (A) - 94.23.44.92 (A) - 176.31.106.195 (A) - 176.31.252.74 (A) - 176.31.252.54 (A) - 176.31.107.87 (A) - 176.31.115.114 (A) - 188.165.210.24 (A)	
secure.informaction.com	AAAA
laserveradedomaina.com	AAAA
ocsp.comodoca.com	A
Answers - ocsp.comodoca.com.edgesuite.net (CNAME) - a652.dscb.akamai.net (CNAME) - 23.67.251.41 (A) - 23.67.251.42 (A)	
a652.dscb.akamai.net	A

Request	Type
a652.dscb.akamai.net	AAAA
Answers - 2600:140a:c000::173b:9a11 (AAAA) - 2600:140a:c000::173b:9a10 (AAAA)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
11.4068050385	Sandbox	46.105.121.115	80
117.878004074	Sandbox	94.130.104.85	443
136.787969112	Sandbox	69.195.158.194	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.11538314819	Sandbox	224.0.0.252	5355
6.11640501022	Sandbox	224.0.0.252	5355
6.12476301193	Sandbox	239.255.255.250	3702
6.15320706367	Sandbox	192.168.56.255	137
8.64026093483	Sandbox	224.0.0.252	5355
8.66885495186	Sandbox	224.0.0.252	5355
11.2617940903	Sandbox	8.8.4.4	53
75.8303670883	Sandbox	8.8.4.4	53
116.247184038	Sandbox	8.8.4.4	53
116.272173166	Sandbox	8.8.4.4	53
116.296137094	Sandbox	8.8.4.4	53
136.288366079	Sandbox	8.8.4.4	53
136.730343103	Sandbox	8.8.4.4	53
136.75209713	Sandbox	8.8.4.4	53
136.776510954	Sandbox	8.8.4.4	53
136.782562971	Sandbox	8.8.4.4	53
136.831022024	Sandbox	8.8.4.4	53
154.621286154	Sandbox	8.8.4.4	53
155.926640034	Sandbox	8.8.4.4	53
155.963572025	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Storage\Permanent\Chrome\Idb\2918063365piupsah.Sqlite-Shm **C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Storage\Permanent\Moz-Safe-About+Home\Idb\818200132aebmoouht.Sqlite-Shm**	**Type :** FoxPro FPT, blocks size 0, next free block index 417475840 **MD5 :** b7c14ec6110fa820ca6b65f5aec85911 **SHA-1 :** 608eeb7488042453c9ca40f7e1398fc1a270f3f4 **SHA-256 :** fd4c9fda9cd3f9ae7c962b0ddf37232294d55580e1aa165aa0612 **SHA-512 :** d8d75760f29b1e27ac9430bc4f4ffcec39f1590be5aef2bfb5a535 **Size :** 32.768 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	b205887a3a508292114e32d15e9a1d459ed53061
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	b205887a3a508292114e32d15e9a1d459ed53061
MD5:	8a2e7ac98d1b90027d2302978b9f2a0b
First Seen Date:	2018-10-01 06:29:54.918394 (21 days ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-10-01 06:29:54.918394 (21 days ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'C:\\Users\\Roock\\source\\repos\\shIn\\shIn\\obj\\Release\\Lighters.pdb\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x u'GUID': u'{9e4ac44e-1ce9-4ad9-b8f1-b4deabc1c9be}', u'timestamp': u'2018-09-26 09:15:29'}]
Number Of Sections	3
Trid	[[82.9, u'Generic CIL Executable (.NET, Mono, etc.)'], [7.4, u'Win32 Dynamic Link Library (generic)'], [5.1, u'Win32 Executable (generic)'], [2.2, u'Generic Win/DOS E
Compilation Time Stamp	0x5BAB4E31 [Wed Sep 26 09:15:29 2018 UTC]
Translation	0x0000 0x04b0
LegalCopyright	SHikha
Assembly Version	0.1.4.6
InternalName	Lighters.exe
FileVersion	8.7.4.4
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	8.7.4.4
FileDescription	Hezr
OriginalFilename	Lighters.exe
Entry Point	0x403276 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	7680
Ssdeep	96:ZHPjm7Kz5kudIGRrdZf5l5xiJZUZ2TZ4WwDezdub7aXzNt:ZHGKzSudIcTlriJZicZrOOB
Sha256	105981495176f0adebef6f8ff49cac1b18bb49cec6bc2bfe69bb8707008766ca
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/b/2/0/5/b205887a3a508292114e32d15e9a u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:09:26 09:15:29+00:00', u'EXE:I
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x127c	0x1400	5.07205561654	45882945569a99812cff6246547fe4be
.rsrc	0x4000	0x580	0x600	4.01904583112	60a3262a143baabc96bdd68ceb9a2339
.reloc	0x6000	0xc	0x200	0.0815394123432	3508c79d3b6a124f665ff43475517c46

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 16528, u'sha256': u'03f4600e6b12f4ea3bc82f50afda3966a5444daacbbcb57545b6323cb2020331', u'type': u'SysEx File - IDP', u'size': 752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 17296, u'sha256': u'539dc26a14b6277e87348594ab7d6e932d16aabb18612d77f29fe421a9f1d46a', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 490}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS


Mozilla Firefox (Not Responding)
Search or enter address

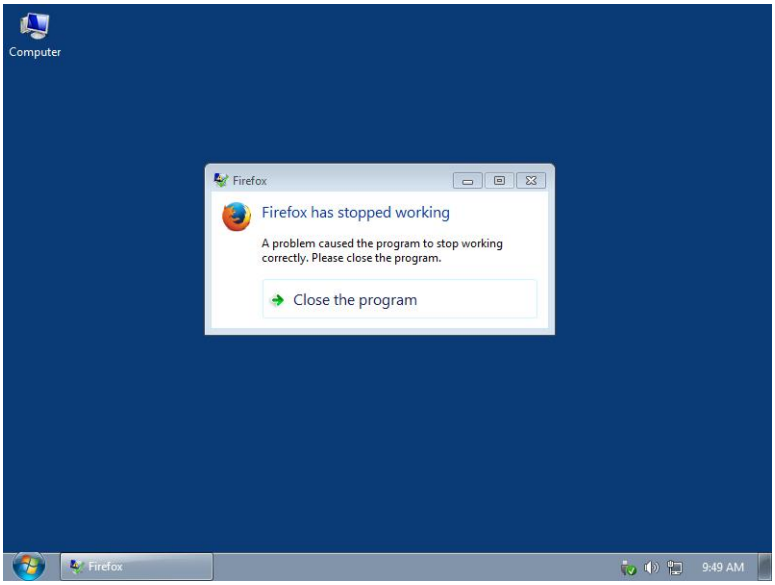

Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
Mozilla Firefox (N...
9:51 AM


New Tab
Search or enter address


Mozilla Firefox
Mozilla Firefox
9:51 AM


Mozilla Firefox (Not Responding)


Mozilla Firefox (Not ...
9:51 AM


Computer
Firefox
Firefox has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Firefox
9:49 AM

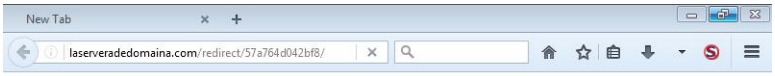

Computer
9:49 AM


Mozilla Firefox (Not Responding)
Search or enter address


Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
Mozilla Firefox (N...
9:51 AM


Mozilla Firefox (Not Responding)
Search or enter address


Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
Mozilla Firefox (N...
9:51 AM


New Tab
laserveradedomaina.com/redirect/57a764d042bf8/


Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
9:51 AM


New Tab
Search or enter address


Mozilla Firefox
9:51 AM


New Tab
Search or enter address


Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
9:51 AM


Mozilla Firefox (Not Responding)


9:51 AM