VALKYRIE COMODO

Summary

File Name: None

File Type:

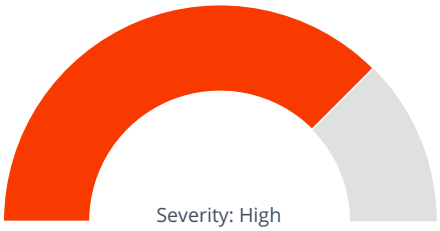
SHA1: 44ee549bd481f02c6c0edc02da5fe6fe5af442f0

MD5: 250bf6b3516e0849ab35549372f622a8

MALWARE

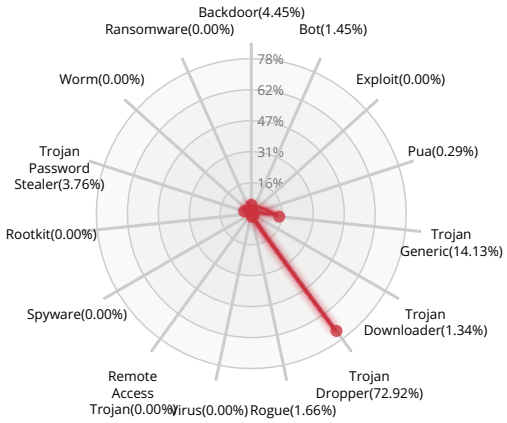
Valkyrie Final Verdict

DETECTION SECTION

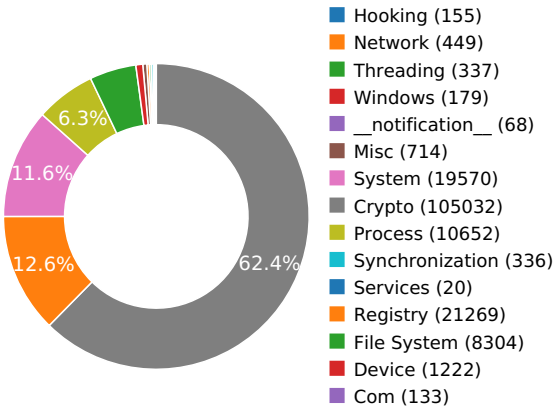


Verdict: Malware

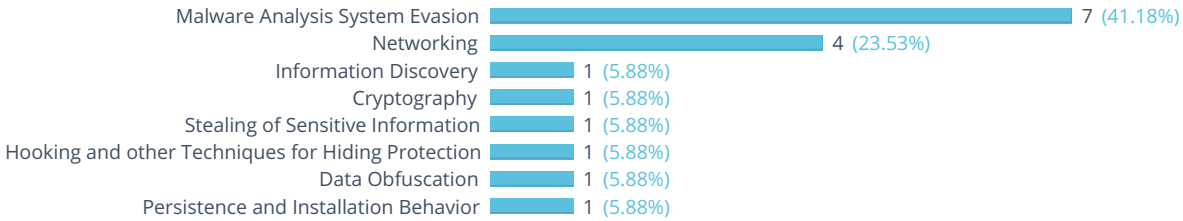
CLASSIFICATION



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 (1 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

CRYPTOGRAPHY

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

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time	Show sources
Detects VMware through the presence of a registry key	Show sources
Checks the presence of disk drives in the registry, possibly for anti-virtualization	Show sources
Attempts to identify installed analysis tools by registry key	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

03:52:44 **03:55:02** **03:57:20**

PID 2464

03:52:44 **Create Process** The malicious file created a child process as 44ee549bd481f02c6c0edc02da5fe6fe5af442f0.exe **(PPID 1636)**

03:52:44 NtAllocateVirtualMem

03:52:46 NtDelayExecution

PID 1828

03:52:46 **Create Process** The malicious file created a child process as 44ee549bd481f02c6c0edc02da5fe6fe5af442f0.exe **(PPID 2464)**

03:52:48 RegSetValueExW

PID 1136

03:52:56 **Create Process** The malicious file created a child process as cmd.exe **(PPID 1828)**

03:52:57 Create Process

03:53:05 NtTerminateProcess

PID 888

03:52:57 **Create Process** The malicious file created a child process as SecondL.exe **(PPID 1136)**

PID 1768

03:53:05 **Create Process** The malicious file created a child process as oqm5r5hfdcd.exe **(PPID 888)**

03:53:05 03:53:05 NtReadFile **[4 times]**

03:53:06 Create Process

PID 1784

03:53:06 **Create Process** The malicious file created a child process as oqm5r5hfdcd.tmp **(PPID 1768)**

03:53:07 RegSetValueExA

03:53:07 NtDelayExecution

PID 2836

03:53:21 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1784)**

03:53:22 __anomaly__

03:53:23 GetSystemTimeAsFileT

03:53:23 connect

03:53:24 GetSystemTime

03:53:24 GetSystemTimeAsFileT

03:53:24 RegQueryValueExW

03:53:24 03:53:28 GetSystemTimeAsFileTi **[9 times]**

PID 2140

03:53:36 **Create Process** The malicious file created a child process as firefox.exe **(PPID 1784)**

03:53:37 __anomaly__

PID 1388

03:53:50 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:53:51 | __anomaly__

PID 2696

03:54:03 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:54:04 | __anomaly__

PID 2784

03:54:14 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:54:15 | __anomaly__

PID 1792

03:54:25 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:54:27 | __anomaly__

PID 3008

03:54:35 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:54:37 | __anomaly__

PID 2692

03:54:43 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:54:44 | __anomaly__

PID 2544

03:54:52 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:54:53 | __anomaly__

PID 264

03:55:00 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:55:01 | __anomaly__

PID 1528

03:55:12 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:55:15 | __anomaly__

PID 1112

03:55:25 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:55:28 | __anomaly__

PID 1736

03:55:40 | Create Process | The malicious file created a child process as firefox.exe **(PPID 1784)**

03:55:43 | __anomaly__

PID 932

03:55:57 Create Process The malicious file created a child process as firefox.exe **(PPID 1784)**

03:55:59 __anomaly__

PID 2920

03:56:18 Create Process The malicious file created a child process as firefox.exe **(PPID 1784)**

03:56:22 __anomaly__

PID 1276

03:56:41 Create Process The malicious file created a child process as firefox.exe **(PPID 1784)**

03:56:45 __anomaly__

PID 2768

03:57:02 Create Process The malicious file created a child process as firefox.exe **(PPID 1784)**

03:57:09 __anomaly__

PID 2756

03:57:20 Create Process The malicious file created a child process as firefox.exe **(PPID 1784)**

PID 952

03:52:58 Create Process The malicious file created a child process as cmd.exe **(PPID 1828)**

03:52:58 Create Process

PID 2596

03:52:58 Create Process The malicious file created a child process as OneTwo.exe **(PPID 952)**

PID 1064

03:53:10 Create Process The malicious file created a child process as cmd.exe **(PPID 2596)**

03:53:10 Create Process

PID 2844

03:53:10 Create Process The malicious file created a child process as 2VCLXBBP8.exe **(PPID 1064)**

03:53:16 RegSetValueExW

03:53:17 NtDelayExecution

PID 2488

03:53:48 Create Process The malicious file created a child process as firefox.exe **(PPID 2844)**

03:53:48 __anomaly__

PID 2056

03:54:00 Create Process The malicious file created a child process as firefox.exe **(PPID 2844)**

03:54:01 __anomaly__

PID 2168

03:54:12 Create Process The malicious file created a child process as firefox.exe **(PPID 2844)**

03:54:13 __anomaly__

VALKYRIE COMODO

PID 3024

03:54:22 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:54:24 | __anomaly__

PID 1360

03:54:32 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:54:33 | __anomaly__

PID 2908

03:54:40 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:54:41 | __anomaly__

PID 3004

03:54:49 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:54:50 | __anomaly__

PID 1612

03:54:54 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:54:56 | __anomaly__

PID 2392

03:55:07 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:55:09 | __anomaly__

PID 3052

03:55:18 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:55:19 | __anomaly__

PID 2760

03:55:32 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:55:35 | __anomaly__

PID 1948

03:55:48 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:55:49 | __anomaly__

PID 1928

03:56:10 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:56:17 | __anomaly__

PID 2824

03:56:33 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:56:38 | __anomaly__

PID 1632

03:56:52 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:56:56 | __anomaly__

PID 2008

03:57:07 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

03:57:10 | __anomaly__

PID 1296

03:57:20 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2844)**

PID 2652

03:52:59 | Create Process | The malicious file created a child process as cmd.exe **(PPID 1828)**

03:53:00 | Create Process

PID 2732

03:53:00 | Create Process | The malicious file created a child process as up.exe **(PPID 2652)**

03:53:07
03:53:07 | RegOpenKeyExW **[21 times]**

03:53:07 | RegQueryValueExW

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\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.exe.config
C:\Users\user\AppData\Local\Temp\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.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\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.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\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.config
C:\Users\user\AppData\Local\Temp\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.INI
C:\Windows\sysnative\l_intl.nls
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
C:\Windows\Globalization\en-us.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\bcrypt.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\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\Globalization\en.nlp
C:\Windows\sysnative\tzres.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.2464.15263312
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2464.15263312
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2464.15263328
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\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

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\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy\Enabled

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy

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

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\SecondL.exe
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\SecondL.exe.config
C:\Users\user\AppData\Local\Temp\config.conf
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\OneTwo.exe
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\OneTwo.exe.config
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\up.exe
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\up.exe.config
C:\Users\user\AppData\Roaming\a022yqeqrbb\oqm5r5hfdcd.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.new
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.888.15275859
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.new
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.888.15275859
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.new
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.888.15275859

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Program Files\2VCLXBBP8J\2VCLXBBP8.exe
C:\Program Files\2VCLXBBP8J\2VCLXBBP8.exe.config
C:\Program Files\2VCLXBBP8J\uninstaller.exe
C:\Program Files\2VCLXBBP8J\uninstaller.exe.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.2596.15277078
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2596.15277093
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2596.15277093
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.2732.15278875
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2732.15278890
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2732.15278875
C:\Users\user\AppData\Local\Temp\is-VGP26.tmp\oqm5r5hfdcd.tmp
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp_isetup_isdecmp.dll
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp\idp.dll
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp\itdownload.dll
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp\psvince.dll
C:\Program Files\2VCLXBBP8J\cast.config
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\parent.lock
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\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\10179

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.2464.15263312

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2464.15263312
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2464.15263328
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.888.15275859
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.new
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.888.15275859
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.new
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.888.15275859
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.new
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.2596.15277078
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2596.15277093
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2596.15277093
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.2732.15278875
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2732.15278890
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2732.15278875
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\10179

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\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.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\3d07fcf9\12ed9530
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\Local\Temp\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.exe 1 true
cmd.exe /k "C:\Users\user\AppData\Local\Temp\\4H89P7ZWCO\SecondL.exe" nimporte & exit
cmd.exe /k "C:\Users\user\AppData\Local\Temp\\4H89P7ZWCO\OneTwo.exe" 57a764d042bf8 & exit
cmd.exe /k "C:\Users\user\AppData\Local\Temp\\4H89P7ZWCO\up.exe" we & exit
C:\Users\user\AppData\Local\Temp\\4H89P7ZWCO\SecondL.exe nimporte

C:\Users\user\AppData\Roaming\a022yqeqrbb\oqm5r5hfdcd.exe /VERYSILENT /p=nimporte

C:\Users\user\AppData\Local\Temp\\4H89P7ZWCO\OneTwo.exe 57a764d042bf8

cmd.exe /k "C:\Program Files\2VCLXBBP8J\2VCLXBBP8.exe" 57a764d042bf8 & exit

C:\Users\user\AppData\Local\Temp\\4H89P7ZWCO\up.exe we

"C:\Users\user\AppData\Local\Temp\is-VGP26.tmp\oqm5r5hfdcd.tmp" /SL5="$C01AC,335632,121344,C:\Users\user\AppData\Roaming\a022yqeqrbb\oqm5r5hfdcd.exe" /VERYSILENT /p=nimporte

http://laserveradedomaina.com/redirect/57a764d042bf8/

"C:\Program Files\2VCLXBBP8J\2VCLXBBP8.exe" 57a764d042bf8

http://letsupdateourdomain.com/redirect/57a764d042bf8

READ FILES

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll

C:\Users\user\AppData\Local\Temp\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.exe.config

C:\Users\user\AppData\Local\Temp\44ee549bd481f02c6c0edc02da5fe6fe5af442f0.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\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp

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

C:\Windows\assembly\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\sysnative\tzres.dll

C:\Windows\sysnative\en-US\KERNELBASE.dll.mui

C:\Users\user\AppData\Local\Temp\config.conf
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\SecondL.exe.config
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\SecondL.exe
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\SecondL.exe.Config
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\OneTwo.exe.config
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\OneTwo.exe
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\OneTwo.exe.Config
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\up.exe.config
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\up.exe
C:\Users\user\AppData\Local\Temp\4H89P7ZWCO\up.exe.Config
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848dc90c7ae0a7dee2\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\6c352ff9e3603b0e69d969ff7e7632f5\System.Windows.Forms.ni.dll
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Roaming\a022yqeqrbb\oqm5r5hfdcd.exe
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp_isetup_isdecmp.dll
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp\idp.dll
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp\itdownload.dll
C:\Users\user\AppData\Local\Temp\is-PGN10.tmp\psvince.dll
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Program Files\2VCLXBBP8J\2VCLXBBP8.exe.config
C:\Program Files\2VCLXBBP8J\2VCLXBBP8.exe
C:\Program Files\2VCLXBBP8J\2VCLXBBP8.exe.Config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorrc.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Data\accc3a5269658c8c47fe3e402ac4ac1c\System.Data.ni.dll
C:\Windows\assembly\GAC_64\System.Data\2.0.0.0__b77a5c561934e089\System.Data.dll
C:\Windows\sysnative\shell32.dll
C:\Windows\sysnative\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

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

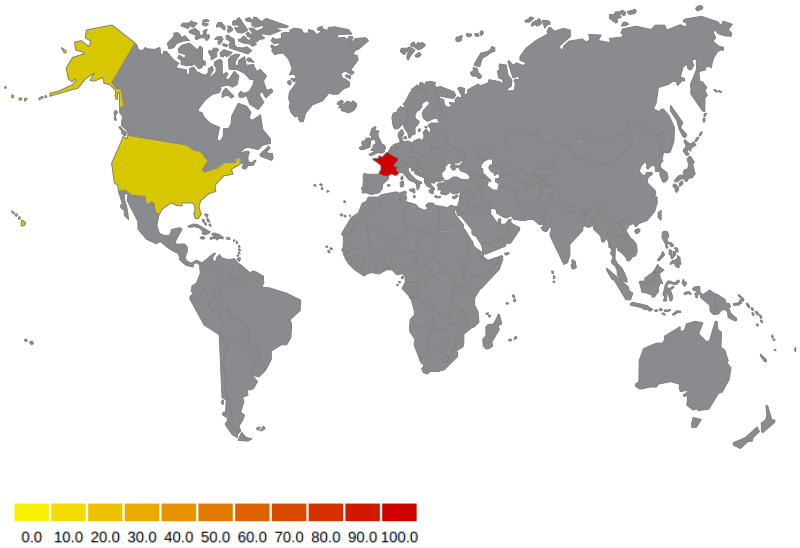
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\OMEWPRODUCT_X65WX
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\44ee549bd481f02c6c0edc02da5fe6fe5af442f0_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\44ee549bd481f02c6c0edc02da5fe6fe5af442f0_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\44ee549bd481f02c6c0edc02da5fe6fe5af442f0_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\44ee549bd481f02c6c0edc02da5fe6fe5af442f0_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\44ee549bd481f02c6c0edc02da5fe6fe5af442f0_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\44ee549bd481f02c6c0edc02da5fe6fe5af442f0_RASAPI32\MaxFileSize

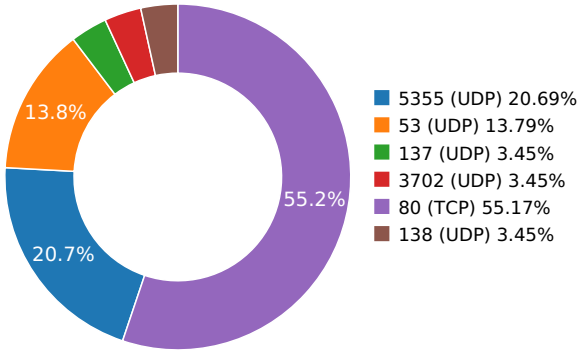
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\44ee549bd481f02c6c0edc02da5fe6fe5af442f0_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\SecondL_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\SecondL_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\SecondL_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\SecondL_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\SecondL_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\SecondL_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\SecondL_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\OneTwo_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\OneTwo_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\OneTwo_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\OneTwo_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\OneTwo_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\OneTwo_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\OneTwo_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\up_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\up_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\up_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\up_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\up_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\up_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\up_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\Run\9167502
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5S1OX8UILO2BUD7
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\2VCLXBBP8_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\2VCLXBBP8_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\2VCLXBBP8_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\2VCLXBBP8_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\2VCLXBBP8_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\2VCLXBBP8_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\2VCLXBBP8_RASAPI32\FileDirectory

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
agent.wizztrakys.com	176.31.252.74	France	16276		Malware Process
www.wizzmonetize.com	176.31.115.114	France	16276		Malware Process
ladomainadeserver.com	176.31.106.195	France	16276		Malware Process
asedownloadgate.com	46.105.121.115	France	16276		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.wizzmonetize.com	80	POST	1.1		1	17.9284639359
Path: /remotes_xml_sections.php **URI:** http://www.wizzmonetize.com/remotes_xml_sections.php						
asedownloadgate.com	80	GET	1.1		1	21.2482359409
Path: /from_backup/747474/AdsShow_installer.exe **URI:** http://asedownloadgate.com/from_backup/747474/AdsShow_installer.exe						
asedownloadgate.com	80	GET	1.1		1	22.1068029404
Path: /3/000000/wizzcaster_installer_v2.exe **URI:** http://asedownloadgate.com/3/000000/wizzcaster_installer_v2.exe						
asedownloadgate.com	80	GET	1.1		1	23.1531741619
Path: /exe/updater.exe **URI:** http://asedownloadgate.com/exe/updater.exe						
asedownloadgate.com	80	GET	1.1		1	28.0881619453
Path: /safe_download/582369/AdsShow.exe **URI:** http://asedownloadgate.com/safe_download/582369/AdsShow.exe						
asedownloadgate.com	80	GET	1.1		1	31.3899040222
Path: /download/3/wizzcaster_v2.exe **URI:** http://asedownloadgate.com/download/3/wizzcaster_v2.exe						
agent.wizztrakys.com	80	POST	1.1		1	31.5296039581
Path: /wemonetize/wizzmonetize/sales_we_DefaultProduct_DefaultPartner_1_load **URI:** http://agent.wizztrakys.com/wemonetize/wizzmonetize/sales_we_DefaultProduct_DefaultPartner_1_load						
asedownloadgate.com	80	GET	1.1		1	33.4033491611
Path: /download/3/wizzcaster_uninstaller_v2.exe **URI:** http://asedownloadgate.com/download/3/wizzcaster_uninstaller_v2.exe						
ladomainadeserver.com	80	POST	1.1		1	41.41771698
Path: /api/v5/config **URI:** http://ladomainadeserver.com/api/v5/config						
ladomainadeserver.com	80	POST	1.1		1	49.2110590935
Path: /api/v5/link **URI:** http://ladomainadeserver.com/api/v5/link						

DNS QUERIES

Request	Type
www.wizzmonetize.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)	
asedownloadgate.com	A
Answers - 46.105.121.115 (A)	
agent.wizztrakys.com	A
ladomainadeserver.com	A

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
17.9284639359	Sandbox	188.165.210.24	80
21.2482359409	Sandbox	46.105.121.115	80
28.0881619453	Sandbox	46.105.121.115	80
31.3899040222	Sandbox	46.105.121.115	80
31.5296039581	Sandbox	176.31.107.87	80
41.41771698	Sandbox	176.31.252.54	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.15581202507	Sandbox	224.0.0.252	5355
7.21978616714	Sandbox	192.168.56.255	137
7.37389802933	Sandbox	224.0.0.252	5355
7.40740704536	Sandbox	239.255.255.250	3702
9.98591399193	Sandbox	224.0.0.252	5355
10.2250511646	Sandbox	192.168.56.255	138
17.4043121338	Sandbox	8.8.4.4	53
18.5451130867	Sandbox	224.0.0.252	5355
21.1403970718	Sandbox	8.8.4.4	53
24.9214229584	Sandbox	224.0.0.252	5355
28.1738770008	Sandbox	224.0.0.252	5355
31.2216830254	Sandbox	8.8.4.4	53
41.1365611553	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-PGN10.Tmp_isetup_isdecmp.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 77d6d961f71a8c558513bed6fd0ad6f1 **SHA-1 :** 122bb9ed6704b72250e4e31b5d5fc2f0476c4b6a **SHA-256 :** 5da7c8d33d3b7db46277012d92875c0b850c8ab **SHA-512 :** b0921e2442b4cdec8cc479ba3751a01c0646a48(**Size :** 24.24 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-PGN10.Tmp\Idp.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b37377d34c8262a90ff95a9a92b65ed8 **SHA-1 :** faeef415bd0bc2a08cf9fe1e987007bf28e7218d **SHA-256 :** e5a0ad2e37dde043a0dd4ad7634961ff3f0d70e8 **SHA-512 :** 69d8da5b45d9b4b996d32328d3402fa37a3d710 **Size :** 221.184 Kilobytes.
C:\Users\User\AppData\Local\Temp\4H89P7ZWCO\OneTwo.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 3e35f3245ee25a530e947a0d5797fe38 **SHA-1 :** bfa03fdb3860250529ddf1d5d1d695addbc36642 **SHA-256 :** 5056cb54c48aeead1737d5d332d2aa3c60de34fc **SHA-512 :** fd6ff0b4302ee73932c4d1ed959ff7727852e989c' **Size :** 212.48 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-VGP26.Tmp\Oqm5r5hfdcd.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 5ec267509d2517e79d53c66f6e9b94ce **SHA-1 :** 35cc1afe77807a44d58c887c5a4c9682f12d2a56 **SHA-256 :** c42453b4837c30061b3df704c1c26492d4de10a2 **SHA-512 :** 5e8614d84a92885b085edce797349e05a8906fb5 **Size :** 782.336 Kilobytes.
C:\Program Files\2VCLXBBP8J\Uninstaller.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 371b854dd3ebdd97d2d426130d048d02 **SHA-1 :** 82020110a0d4d1503be0e39beefa61f9dad37d45 **SHA-256 :** 65cf43d67312e75fbe5f0f21bc51872a8fc7968df8 **SHA-512 :** 3b22970337f244fceb52091b4c5008e6d15aea62 **Size :** 202.24 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-PGN10.Tmp\Psvince.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** d726d1db6c265703dcd79b29adc63f86 **SHA-1 :** f471234fa142c8ece647122095f7ff8ea87cf423 **SHA-256 :** 0afdfed86b9e8193d0a74b5752a693604ab7ca73 **SHA-512 :** 8cccbff39939bea7d6fe1066551d65d21185cef68 **Size :** 43.52 Kilobytes.
C:\Users\User\AppData\Local\Temp\Config.Conf	**Type :** ASCII text, with CRLF line terminators **MD5 :** ba58fc124f9bb6195535ffdb94e23bdd **SHA-1 :** 547b1db522800d27fd1efe611e2eebd9904f7391 **SHA-256 :** ab1a4e466b00aaaeba5cd02db9f2e234c22901c4 **SHA-512 :** eba8697278179879023541d5d524ff94de072ba8 **Size :** 0.047 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Windows\Microsoft.NET\Framework64\V2.0.50727\CONFIG\Security.Config.Cch.2732.15278875 **C:\Windows\Microsoft.NET\Framework64\V2.0.50727\CONFIG\Enterprisesec.Config.Cch.2732.15278875** **C:\Users\User\AppData\Roaming\Microsoft\CLR Security Config\V2.0.50727.312\64bit\Security.Config.Cch.2732.15278890**	**Type :** data **MD5 :** 72a0f232c8a859615d9c622044bbd772 **SHA-1 :** 69b040918049c86db02dc9f7a440a2cfb7ac1809 **SHA-256 :** 74f6952474381681d0061a9d053964a0aebaf59(**SHA-512 :** d771814315a2b89ae8c7f40f5bd3d6d16dda0c25 **Size :** 1.246 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-PGN10.Tmp_isetup_setup64.Tmp	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** e4211d6d009757c078a9fac7ff4f03d4 **SHA-1 :** 019cd56ba687d39d12d4b13991c9a42ea6ba03da **SHA-256 :** 388a796580234efc95f3b1c70ad4cb44bfddc7ba(**SHA-512 :** 17257f15d843e88bb78adcfb48184b8ce22109cc **Size :** 6.144 Kilobytes.
C:\Windows\Microsoft.NET\Framework64\V2.0.50727\CONFIG\Security.Config.Cch **C:\Users\User\AppData\Roaming\Microsoft\CLR Security Config\V2.0.50727.312\64bit\Security.Config.Cch** **C:\Windows\Microsoft.NET\Framework64\V2.0.50727\CONFIG\Enterprisesec.Config.Cch**	**Type :** data **MD5 :** 0d86c45b85ca7126c48f5b87eb9f55cd **SHA-1 :** fa1348ec3093f8f2eac424d78977adc4854987df **SHA-256 :** 1ecc75866038b9751ab491f04916728f9873f876 **SHA-512 :** 5c011a00464c7b63dff9619b301f522d5759bf885 **Size :** 1.244 Kilobytes.
C:\Users\User\AppData\Local\Temp\4H89P7ZWCO\Up.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** dbbc41352104e471080d25bea7a93455 **SHA-1 :** 4a173ed8964a000078cefb7549bc7b8b2d8da00b **SHA-256 :** 50f1be7efd73353859177946b79670c55226279e **SHA-512 :** d523004a62e59ff7ea0d14d97b9193202870c03f **Size :** 2553.344 Kilobytes.
C:\Program Files\2VCLXBBP8J\2VCLXBBP8.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 3d6a321e3ee3a216223111c12a1470bc **SHA-1 :** 1cf13277e9b74440e8e5a76d1b8a5114990a3757 **SHA-256 :** b8f4f117bb2691279f56098b4eafd59ae89d1a78 **SHA-512 :** 2777fdad68e111a6d2a8e495798f0fe4dd80e32e **Size :** 840.704 Kilobytes.
C:\Users\User\AppData\Roaming\A022yqeqrbb\Oqm5r5hfdcd.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 331f4648a2f6cfacb0f84ace8fd05f62 **SHA-1 :** bec6b9ecd372953703f181c025249036427e73f3 **SHA-256 :** 6dcadcf2a0f6e1ae7195d6352ec62458a484bc92 **SHA-512 :** 488495c713e006a4e5e1e13cb0986435991cf74a **Size :** 615.251 Kilobytes.
C:\Windows\Microsoft.NET\Framework64\V2.0.50727\CONFIG\Security.Config.Cch.2596.15277078 **C:\Windows\Microsoft.NET\Framework64\V2.0.50727\CONFIG\Enterprisesec.Config.Cch.2596.15277093** **C:\Users\User\AppData\Roaming\Microsoft\CLR Security Config\V2.0.50727.312\64bit\Security.Config.Cch.2596.15277093**	**Type :** data **MD5 :** 5062ce9faa704829e92f42e0196f33f9 **SHA-1 :** 4f5c6de00638b7ccf9e1427a709e7eb89501f15c **SHA-256 :** c6aa1ca55aa2aa0e15fff8f6c3a5c644f2bb176824 **SHA-512 :** 783fce9ced6851f29f5b930bbcde4fbb27eb9f4e2 **Size :** 1.236 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Index	**Type :** data **MD5 :** 5759064c3510519bddd7be7d28b0f97c **SHA-1 :** 876a2531dc24196c342fc1f6ed08d45dd8287c7c **SHA-256 :** 7fd86697e202fe0e78e80d40a3ca8b3af7a0d328 **SHA-512 :** b440311d385bedd08c1e069c05a22a210714806 **Size :** 1.564 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\4H89P7ZWCO\SecondL.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 72c5089576d10d0d6ab9d7518c72a8f2 **SHA-1 :** 8afca3e42d3cfa6af0dedd5c99262de4efc1b98c **SHA-256 :** 539fe97cbec2242284054f38b40d67aa9adebce5 **SHA-512 :** 835813484e19f2fe121c88cd3161721f45d5a768 **Size :** 7.168 Kilobytes.
C:\Program Files\2VCLXBBP8J\Cast.Config	**Type :** ASCII text, with CRLF line terminators **MD5 :** 55c3ef7d7a2552fc1405eba10e2731b4 **SHA-1 :** 079f85eee67b822c34092d052f90eb472f71b6e2 **SHA-256 :** b23be6853e2a8db3c482f0aded8516cc1cb3b60a **SHA-512 :** a1a42ff09c8a455f082551dda8d934cd2071500d **Size :** 0.037 Kilobytes.
C:\Users\User\AppData\Local\Temp\4H89P7ZWCO\SecondL.Exe.Config **C:\Users\User\AppData\Local\Temp\4H89P7ZWCO\OneTwo.Exe.Config** **C:\Users\User\AppData\Local\Temp\4H89P7ZWCO\Up.Exe.Config** **C:\Program Files\2VCLXBBP8J\2VCLXBBP8.Exe.Config** **C:\Program Files\2VCLXBBP8J\Uninstaller.Exe.Config**	**Type :** XML document text **MD5 :** a2ebf843442988ee2d667e9c7fc28ce1 **SHA-1 :** 7f24c475bb217c448090dce593abee8957b7b1d4 **SHA-256 :** 8a0d5d6c5ab131bab9c8a29a7bcc81d6470ec51 **SHA-512 :** 1b56db588131023f427e0476582e3381a818d96 **Size :** 1.81 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-PGN10.Tmp\Itdownload.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** d82a429efd885ca0f324dd92afb6b7b8 **SHA-1 :** 86bbdaa15e6fc5c7779ac69c84e53c43c9eb20ea **SHA-256 :** b258c4d7d2113dee2168ed7e35568c8e03341e2 **SHA-512 :** 5bf0c3b8fa5db63205a263c4fa5337188173248b **Size :** 205.312 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	None
File Type:	
SHA1:	44ee549bd481f02c6c0edc02da5fe6fe5af442f0
MD5:	250bf6b3516e0849ab35549372f622a8
First Seen Date:	2018-08-21 00:47:53.262477 (4 months ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-08-21 00:47:53.262477 (4 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	0
Debug Artifacts	[{u'Path': u'C:\\Users\\Wizzlabs\\Documents\\Elukton\\Elukton\\obj\\Release\\MacroMicro.pdb\x00', u'GUID': u'{993db8f5-5700-4f31-b894-62ba89ad3a70}', u'timestamp': u'2018-07-31 12:24:08'}]
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Number Of Sections	3
Trid	[[81.0, u'Generic CIL Executable (.NET, Mono, etc.)'], [7.2, u'Win32 Dynamic Link Library (generic)'], [4.9, u'Win32 Executable (generic)'], [2.2, u'OS/2 Executable (generic)'], [2.2, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x5B6054E8 [Tue Jul 31 12:24:08 2018 UTC]
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 6378
Assembly Version	0.5.2.2
InternalName	MacroMicro.exe
FileVersion	0.0.2.5
CompanyName	BG8
LegalTrademarks	
Comments	BG
ProductName	BG
ProductVersion	0.0.2.5
FileDescription	
OriginalFilename	MacroMicro.exe
Entry Point	0x40d962 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	242176
Ssdeep	
Sha256	35d9f4e3091cd87ade7842b87569531fe0381e582ee7f9623178153cc9894374
Exifinfo	[]
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0xb970	0xba00	6.22606572129	724b92d2a2349fb7facaa13947f8d995
.rsrc	0xe000	0x2f234	0x2f400	4.7740758669	6d5590f02dc64f083705086ebc341a2c
.reloc	0x3e000	0xc	0x200	0.0815394123432	82f8c53d9cf996b39a00741b48506085

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 57856, u'sha256': u'f5157ab852e8a7a5896b060175a3f728d9a1941f0e0ac204608a99c6be57556b', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 26812}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 84684, u'sha256': u'2b3c98cd70d973e5c20b5b76be0f9911a6d31df6d925db03200fd343c6cff5b5', u'type': u'dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0', u'size': 67624}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 152324, u'sha256': u'2d7580b8acc471fde88738117ef461cbdf50546d89ad039e7e39be9538d5eca2', u'type': u'data', u'size': 38056}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 190396, u'sha256': u'23969152addc2eed5b3a2e2c9cb10b29e462967bf0bb6f1e3b528f8ae7ec2148', u'type': u'data', u'size': 21640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 212052, u'sha256': u'4adee163931cfedb94a94f0e4a3a3362b49635e2cb81f92ac0ac5c2dbb9ed0e5', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 12648447, next used block 4294902528', u'size': 16936}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 229004, u'sha256': u'0bb4c270c5ac5f790c381131832ce7bafda81f08a74e9a3cd0d0bcecfc5af764', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 238660, u'sha256': u'cd0c36b80bc23ad6d48bfafb1294704e91495caa42676040161511e587912787', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 242940, u'sha256': u'd3245c19c2ee1d46edaf3508840f774eeb32bf1242e889ef08f706a6e14885f6', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 245396, u'sha256': u'fa5edead672f9724f52a9e1f152c5afe37495f35f32b060a8206efa9bfa07307', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 246540, u'sha256': u'6cdda0ae2c406383536535df01e40871d7ba15b85db35dd09155ae6f876ea37e', u'type': u'MS Windows icon resource - 9 icons, 256x256', u'size': 132}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 246688, u'sha256': u'5c0eadfb950e865c5f5078cd3064e1285528385d99cd7bdc3e3037f8db9ecdb7', u'type': u'data', u'size': 784}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 247488, u'sha256': u'8b7d33b2f2ac9e8461a6390fc340499216b49ef6ca4dc7b9fea97fbe13820dd8', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 2927}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS