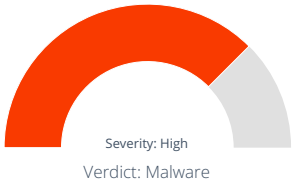
VALKYRIE COMODO

Summary

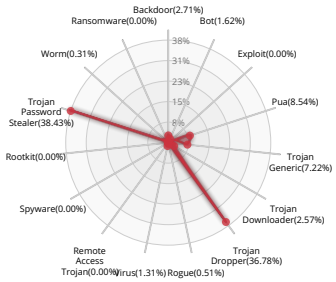
File Name: SecureBrowserSetup.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 4a361773655f41788ef53d1ee189c39673f421d8
MD5: afe7194c459fd4847b694f3abb4c2267

MALWARE
Valkyrie Final Verdict

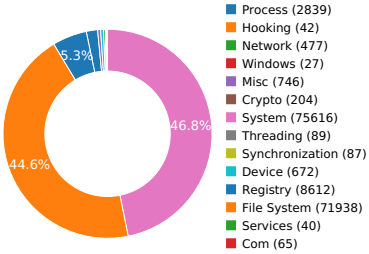
DETECTION SECTION



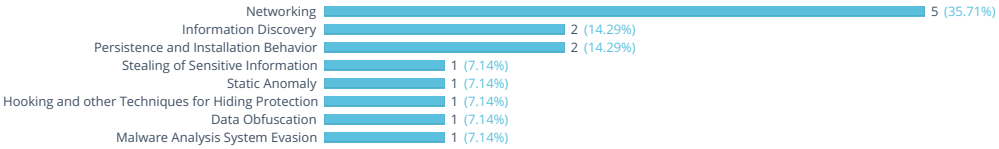
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes	Show sources
Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (4 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources
Network activity contains more than one unique useragent.	Show sources
A process sent information about the computer to a remote location.	Show sources

STEALING OF SENSITIVE INFORMATION

Steals private information from local Internet browsers	Show sources

STATIC ANOMALY

Anomalous binary characteristics	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

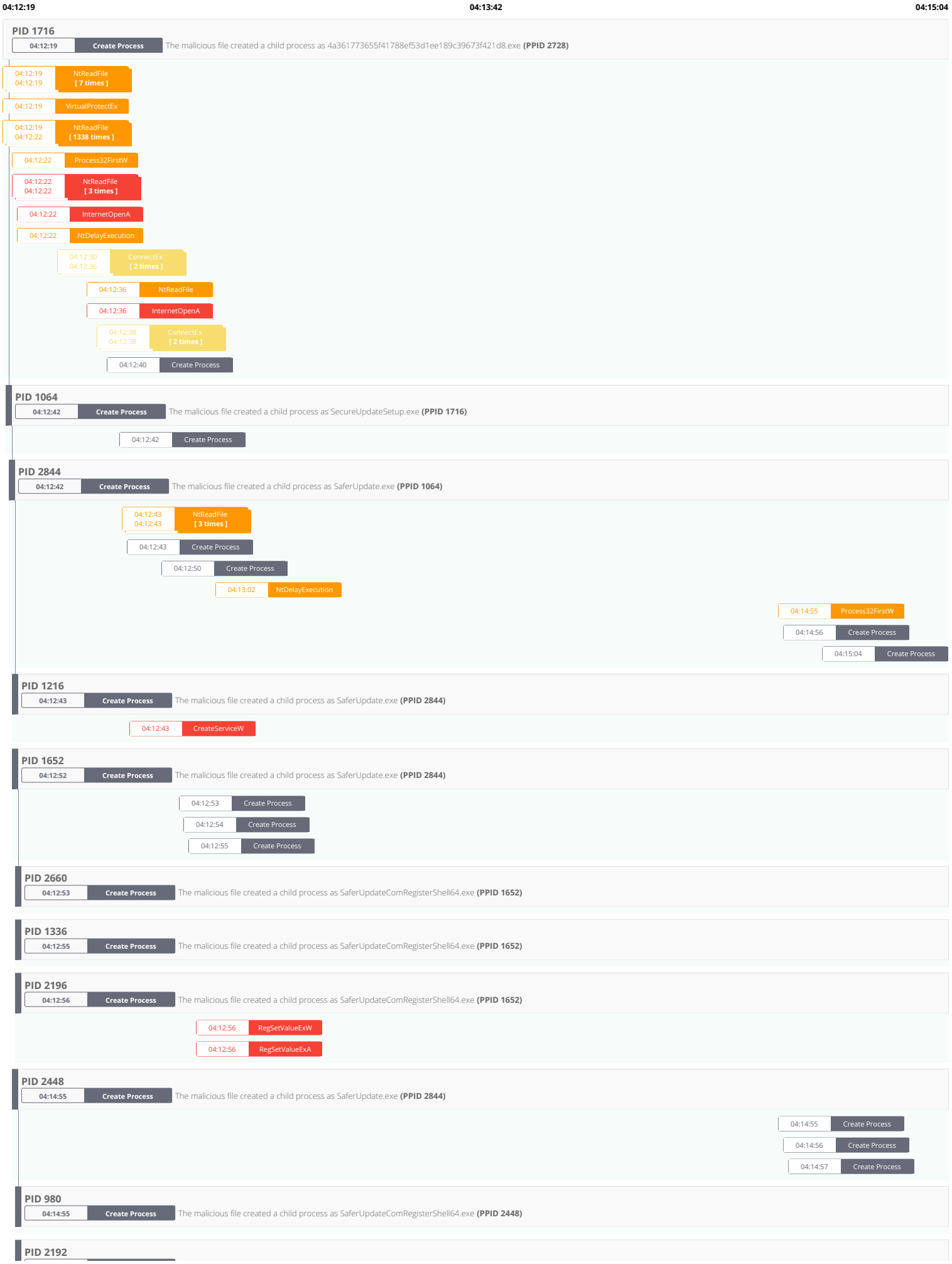
Installs itself for autorun at Windows startup	Show sources
Created a service that was not started	Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task.	Show sources

VALKYRIE COMODO

Behavior Graph



04:14:56 Create Process The malicious file created a child process as SaferUpdateComRegisterShell64.exe **(PPID 2448)**

PID 544

04:14:57 Create Process The malicious file created a child process as SaferUpdateComRegisterShell64.exe **(PPID 2448)**

PID 1360

04:15:02 Create Process The malicious file created a child process as SaferUpdate.exe **(PPID 2844)**

PID 1924

04:13:11 Create Process The malicious file created a child process as SaferUpdate.exe **(PPID 2844)**

04:13:13 04:13:13 NtReadFile **[8 times]**

04:13:13 ConnectEx

04:13:27 04:13:44 NtReadFile **[18 times]**

PID 2480

04:13:13 Create Process The malicious file created a child process as SaferUpdate.exe **(PPID 2844)**

PID 872

04:12:46 Create Process The malicious file created a child process as svchost.exe **(PPID 460)**

Behavior Summary

CREATED SERVICES

safer
saferm

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nsoA8D8.tmp
C:\Users\user\AppData\Local\Temp\4a361773655f41788ef53d1ee189c39673f421d8.exe
C:\Users\user\AppData\Local\Temp\nsyA917.tmp
C:\Users\user\AppData\Local\Temp\nsoA928.tmp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\StdUtils.dll
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsJSON.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\DataReaderNSIS.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini*.*
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default*.*
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\inetc.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\secure-browser-installer-tracking-response.tmp
C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\ras*.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\en-US\WINHTTP.dll.mui
C:\Users\user\AppData\LocalLow
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0F1583FFF42FFF476A09801ACB69213F_D4C83E2943267C1763EC8ED5C0DDE848
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0F1583FFF42FFF476A09801ACB69213F_D4C83E2943267C1763EC8ED5C0DDE848
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\secure-browser-installer-tracking-response.tmp*.*
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\modern-wizard.bmp
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsDialogs.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\InetBgDL.dll
C:\Windows\System32\UXTHEME.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\4a361773655f41788ef53d1ee189c39673f421d8.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\Linker.dll
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6E5336CDD9652A36A93E734B280625C5
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\DE624068503F3B953A6EC67A0654E15F_81E07CC400DF4DB0ECA725A050D525AB
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\DE624068503F3B953A6EC67A0654E15F_81E07CC400DF4DB0ECA725A050D525AB
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6E5336CDD9652A36A93E734B280625C5

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsProcess.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\SecureUpdateSetup.exe
C:\Program Files (x86)\Safer Technologies\Secure Browser\Application\secure.exe
C:\Program Files (x86)
C:\Program Files (x86)\GUMFAA1.tmp
C:\Program Files (x86)\GUTFAB2.tmp
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdate.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferCrashHandler.exe
C:\Program Files (x86)\GUMFAA1.tmp\goopdate.dll
C:\Program Files (x86)\GUMFAA1.tmp\npSaferUpdate3.dll
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateHelper.msi
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateBroker.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateOnDemand.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateComRegisterShell64.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateWebPlugin.exe
C:\Program Files (x86)\GUMFAA1.tmp\psmachine.dll
C:\Program Files (x86)\GUMFAA1.tmp\psmachine_64.dll
C:\Program Files (x86)\GUMFAA1.tmp\psuser.dll
C:\Program Files (x86)\GUMFAA1.tmp\psuser_64.dll
C:\Program Files (x86)\GUMFAA1.tmp\SaferCrashHandler64.exe
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_am.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ar.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_bg.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_bn.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ca.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_cs.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_da.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_de.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_el.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductName
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice\ProgId
HKEY_CURRENT_USER\Software\Classes\FirefoxURL\shell\open\command\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoProxyDetectType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASMANCS\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASMANCS\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASMANCS\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASMANCS\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASMANCS\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4a361773655f41788ef53d1ee189c39673f421d8_RASMANCS\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\WinHttpSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\EnableInetUnknownAuth
HKEY_CURRENT_USER\Software\Safer Technologies\user_date
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugFlags
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Domain
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\PendingFileRenameOperations
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\safer_task_name_c

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\nsyA917.tmp
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\StdUtils.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsJSON.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\DataReaderNSIS.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\inetc.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\secure-browser-installer-tracking-response.tmp
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0F1583FFF42FFF476A09801ACB69213F_D4C83E2943267C1763EC8ED5C0DDE848
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0F1583FFF42FFF476A09801ACB69213F_D4C83E2943267C1763EC8ED5C0DDE848
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\modern-wizard.bmp
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsDialogs.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\InetBgDL.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\Linker.dll
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\DE624068503F3B953A6EC67A0654E15F_81E07CC400DF4DB0ECA725A050D525AB
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\DE624068503F3B953A6EC67A0654E15F_81E07CC400DF4DB0ECA725A050D525AB
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6E5336CDD9652A36A93E734B280625C5
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6E5336CDD9652A36A93E734B280625C5
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsProcess.dll
C:\Users\user\AppData\Local\Temp\nsoA928.tmp\SecureUpdateSetup.exe
C:\Program Files (x86)\GUTFAB2.tmp
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdate.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferCrashHandler.exe
C:\Program Files (x86)\GUMFAA1.tmp\goopdate.dll
C:\Program Files (x86)\GUMFAA1.tmp\npSaferUpdate3.dll
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateHelper.msi
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateBroker.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateOnDemand.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateComRegisterShell64.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateWebPlugin.exe
C:\Program Files (x86)\GUMFAA1.tmp\psmachine.dll
C:\Program Files (x86)\GUMFAA1.tmp\psmachine_64.dll
C:\Program Files (x86)\GUMFAA1.tmp\psuser.dll
C:\Program Files (x86)\GUMFAA1.tmp\psuser_64.dll
C:\Program Files (x86)\GUMFAA1.tmp\SaferCrashHandler64.exe
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_am.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ar.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_bg.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_bn.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ca.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_cs.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_da.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_de.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_el.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_en.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_en-GB.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_es.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_es-419.dll

C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_et.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_fa.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_fi.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_fil.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_fr.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_gu.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_hi.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_hr.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_hu.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_id.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_is.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_it.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_iw.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ja.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_kn.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ko.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_lt.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_lv.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ml.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_mr.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ms.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_nl.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_no.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_pl.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_pt-BR.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_pt-PT.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ro.dll

RESOLVED APIS

version.dll.GetFileVersionInfoA
shfolder.dll.SHGetFolderPathA
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
kernel32.dll.GetUserDefaultUILanguage
shell32.dll.#680
stdutils.dll.GetParameter
system.dll.Call
kernel32.dll.CreateMutexA
nsjson.dll.Set
nsjson.dll.Get
kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
datareadernsis.dll.ReadTag
ole32.dll.CoCreateGuid
user32.dll.CharLowerA
kernel32.dll.GetCurrentProcess
kernel32.dll.IsWow64Process
kernel32.dll.GetProcessId

kernel32.dll.CreateToolhelp32Snapshot
system.dll.Alloc
kernel32.dll.Process32First
kernel32.dll.Process32Next
system.dll.Free
kernel32.dll.OpenProcess
psapi.dll.GetModuleFileNameExA
stdutils.dll.GetRealOsName
stdutils.dll.GetRealOsVersion
stdutils.dll.GetRealOsBuildNo
kernel32.dll.GetLocaleInfoA
kernel32.dll.GetLocalTime
kernel32.dll.GetSystemTime
inetc.dll.get
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
uxtheme.dll.EnableThemeDialogTexture
uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeInt
wininet.dll.FtpCommandA
rasapi32.dll.RasConnectionNotificationW
sechost.dll.NotifyServiceStatusChangeA
ole32.dll.CoInitializeEx
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
ole32.dll.CoCreateInstance
ole32.dll.CoTaskMemAlloc
oleaut32.dll.#8
oleaut32.dll.#9
oleaut32.dll.DllGetClassObject
oleaut32.dll.DllCanUnloadNow
advapi32.dll.RegOpenKeyW
ole32.dll.CoTaskMemFree
ole32.dll.StringFromIID
iphlpapi.dll.GetAdaptersAddresses
dhcpcsvc.dll.DhcpRequestParams
oleaut32.dll.#2
oleaut32.dll.#6
shlwapi.dll.UrlGetPartW
winhttp.dll.WinHttpOpen
winhttp.dll.WinHttpSetTimeouts
winhttp.dll.WinHttpSetOption
winhttp.dll.WinHttpCrackUrl
shlwapi.dll.StrCmpNW
cryptbase.dll.SystemFunction001
cryptbase.dll.SystemFunction002
cryptbase.dll.SystemFunction003
cryptbase.dll.SystemFunction004
cryptbase.dll.SystemFunction005
cryptbase.dll.SystemFunction028
cryptbase.dll.SystemFunction029
cryptbase.dll.SystemFunction034

VALKYRIE COMODO

DELETED FILES

C:\Users\user\AppData\Local\Temp\nsoA8D8.tmp
C:\Users\user\AppData\Local\Temp\nsoA928.tmp
C:\Program Files (x86)\GUMFAA1.tmp
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdate.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferCrashHandler.exe
C:\Program Files (x86)\GUMFAA1.tmp\goopdate.dll
C:\Program Files (x86)\GUMFAA1.tmp\npSaferUpdate3.dll
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateHelper.msi
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateBroker.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateOnDemand.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateComRegisterShell64.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateWebPlugin.exe
C:\Program Files (x86)\GUMFAA1.tmp\psmachine.dll
C:\Program Files (x86)\GUMFAA1.tmp\psmachine_64.dll
C:\Program Files (x86)\GUMFAA1.tmp\psuser.dll
C:\Program Files (x86)\GUMFAA1.tmp\psuser_64.dll
C:\Program Files (x86)\GUMFAA1.tmp\SaferCrashHandler64.exe
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_am.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ar.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_bg.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_bn.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ca.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_cs.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_da.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_de.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_el.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_en.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_en-GB.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_es.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_es-419.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_et.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_fa.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_fi.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_fil.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_fr.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_gu.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_hi.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_hr.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_hu.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_id.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_is.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_it.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_iw.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ja.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_kn.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ko.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_lt.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_lv.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ml.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_mr.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ms.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_nl.dll

C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_no.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_pl.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_pt-BR.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_pt-PT.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ro.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ru.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_sk.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_sl.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_sr.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_sv.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_sw.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ta.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_te.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_th.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_tr.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_uk.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ur.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_vi.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_zh-CN.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_zh-TW.dll
C:\Program Files (x86)\GUTFAB2.tmp
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateSetup.exe
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\SaferUpdate.exe
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdate.dll

DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\mi
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ui
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\LastChecked
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\LastCodeRedCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}\UpdateAvailableCount
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}\UpdateAvailableSince
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\uid
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\old-uid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content Type\application/x-vnd.update.securebrowser.com.oneclickctrl.9\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content Type\application/x-vnd.update.securebrowser.com.update3webcontrol.3\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SaferUpdate.exe\DisableExceptionChainValidation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\UninstallCmdLine
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\IsMSIHelperRegistered
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\LastOSVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\RetryAfter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\SaferUpdateTaskMachineCore.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\SaferUpdateTaskMachineCore.job.fp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\SaferUpdateTaskMachineUA.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\SaferUpdateTaskMachineUA.job.fp
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\eulaaccepted
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{EE8476B7-7A63-460D-87FD-90BD169D2749}\InprocHandler32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{0AD8F5F5-68AF-44CA-94AF-61BEA9D435BF}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{30E8E9BA-54F0-4034-9D07-2B30474A0444}\LocalizedString

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{30E8E9BA-54F0-4034-9D07-2B30474A0444}\Elevation\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{30E8E9BA-54F0-4034-9D07-2B30474A0444}\Elevation\IconReference
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D4B36AD2-6840-4724-A773-14B679DC254A}\LocalizedString
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D4B36AD2-6840-4724-A773-14B679DC254A}\Elevation\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D4B36AD2-6840-4724-A773-14B679DC254A}\Elevation\IconReference
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{A5595323-81CC-44F5-ABE6-BF31B2B1BC19}\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{A5595323-81CC-44F5-ABE6-BF31B2B1BC19}\Policy
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{244E8A46-C0DB-414D-B9B4-935B394ACAED}\LocalizedString
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{244E8A46-C0DB-414D-B9B4-935B394ACAED}\Elevation\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{244E8A46-C0DB-414D-B9B4-935B394ACAED}\Elevation\IconReference
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A67F6625-D938-4825-91DF-68E3E1D1FAF0}\LocalizedString
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A67F6625-D938-4825-91DF-68E3E1D1FAF0}\Elevation\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A67F6625-D938-4825-91DF-68E3E1D1FAF0}\Elevation\IconReference
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{423CF489-F1A6-4358-A236-384033B55804}\LocalizedString
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{423CF489-F1A6-4358-A236-384033B55804}\Elevation\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{423CF489-F1A6-4358-A236-384033B55804}\Elevation\IconReference
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{EE8476B7-7A63-460D-87FD-90BD169D2749}\InprocHandler32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0AD8F5F5-68AF-44CA-94AF-61BEA9D435BF}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{C3AB7A34-75F2-4D4B-90FD-EEE151AEA971}\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\SaferUpdate.exe\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{14A60BDB-4098-4D00-A481-5D1C5402D099}\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{49610592-C002-410C-BFC3-B1E65105646D}\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{FA795BC7-74B5-4F0B-B68D-CA5CF3E37618}\AppID

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Secure Browser
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductName
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice\ProgId
HKEY_CLASSES_ROOT\FirefoxURL\shell\open\command
HKEY_CURRENT_USER\Software\Classes\FirefoxURL\shell\open\command\(Default)
HKEY_CURRENT_USER\Software\Safer Technologies
HKEY_CURRENT_USER\Software\Safer Technologies\user_id
HKEY_LOCAL_MACHINE\Software\Safer Technologies
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocHandler32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocHandler
HKEY_LOCAL_MACHINE\Software\Microsoft\OleAut
HKEY_CURRENT_USER\Software\Classes\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoProxyDetectType
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\nsoA928.tmp\SecureUpdateSetup.exe" /silent /install bundlename=Secure%20Browser&appguid={428169FE-8EF9-F2FE-C5FC-6E50B2CD33B3}&appname=Secure%20Browser&needsadmin=true&ap=mv:50.0.2661.205&lang=en&brand=3132_def-3132-atl-atr-bbc-bim-dbc-dim-hbl-lfb-mys
"C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdate.exe" /silent /install bundlename=Secure%20Browser&appguid={428169FE-8EF9-F2FE-C5FC-6E50B2CD33B3}&appname=Secure%20Browser&needsadmin=true&ap=mv:50.0.2661.205&lang=en&brand=3132_def-3132-atl-atr-bbc-bim-dbc-dim-hbl-lfb-mys

"C:\Program Files (x86)\Safer Technologies\Update\SaferUpdate.exe" /regsvc

"C:\Program Files (x86)\Safer Technologies\Update\SaferUpdate.exe" /regserver

C:\Program Files (x86)\Safer Technologies\Update\SaferUpdate.exe /ping
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48cmVxdWVzdCBwcm90b2NvbD0iMy4wIiB2ZXJzaW9uPSIxLjMuMTI5LjciIHNoZWxsX3ZlcnNpb249IjEuMy4xMjkuNyIgaXNtYWNoaW5lPSIxIiBzZXNzaW9uaWQ9IntEQzRBRjBDNy01N0RGLTQ2NDM
PGh3IHBoeXNtZW1vcnk9IjMiIHNzZT0iMSIgc3NlMj0iMSIgc3NlMz0iMSIgc3NzZTM9IjEiIHNzZTQxPSIwIiBzc2U0Mj0iMCIgYXZ4PSIwIi8-
PG9zIHBsYXRmb3JtPSJ3aW4iIHZlcnNpb249IjYuMSIgc3A9IlNlcnZpY2UgUGFjayAxIiBhcmNoPSJ4NjQiLz48YXBwIGFwcGlkPSJ7NDMwRkQ0RDAtQjcyOS00RjYxLUFBMzQtOTE1MjY0ODE3OTlEfSIgdmVyc2lvbj0iIiBuZXh0dmVyc2lvbj0iMS4zLjEyOS43IiBsYW5nPSJlb
PC9hcHA-PC9yZXF1ZXN0Pg

C:\Program Files (x86)\Safer Technologies\Update\SaferUpdate.exe /handoff "bundlename=Secure%20Browser&appguid={428169FE-8EF9-F2FE-C5FC-6E50B2CD33B3}&appname=Secure%20Browser&needsadmin=true&ap=mv:50.0.2661.205&lang=en&brand=3132_def-3132-atl-atr-bbc-bim-dbc-dim-hbl-lfb-mys" /installsource otherinstallcmd /sessionid "{DC4AF0C7-57DF-4643-BC72-01D7EBC7D43D}" /silent

"C:\Program Files (x86)\Safer Technologies\Update\SaferUpdate.exe" /unregserver

"C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdate.exe" /unregsvc

"C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\SaferUpdateComRegisterShell64.exe"

"C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\SaferUpdateComRegisterShell64.exe" /unregister

READ FILES

\Device\KsecDD

C:\Users\user\AppData\Local\Temp\nsoA8D8.tmp

C:\Users\user\AppData\Local\Temp\4a361773655f41788ef53d1ee189c39673f421d8.exe

C:\Users\user\AppData\Local\Temp\nsyA917.tmp

C:\Users\user\AppData\Local\Temp\nsoA928.tmp

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\StdUtils.dll

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\System.dll

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsJSON.dll

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\DataReaderNSIS.dll

C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\inetc.dll

C:\Windows\System32\en-US\WINHTTP.dll.mui

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0F1583FFF42FFF476A09801ACB69213F_D4C83E2943267C1763EC8ED5C0DDE848

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0F1583FFF42FFF476A09801ACB69213F_D4C83E2943267C1763EC8ED5C0DDE848

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\secure-browser-installer-tracking-response.tmp

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsDialogs.dll

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\modern-wizard.bmp

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\InetBgDL.dll

C:\Windows\System32\UXTHEME.dll.Config

C:\Windows\System32\uxtheme.dll

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\Linker.dll

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6E5336CDD9652A36A93E734B280625C5

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\DE624068503F3B953A6EC67A0654E15F_81E07CC400DF4DB0ECA725A050D525AB

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\DE624068503F3B953A6EC67A0654E15F_81E07CC400DF4DB0ECA725A050D525AB

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6E5336CDD9652A36A93E734B280625C5

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\nsProcess.dll

C:\Program Files (x86)\GUMFAA1.tmp

C:\Program Files (x86)\GUTFAB2.tmp

C:\Users\user\AppData\Local\Temp\nsoA928.tmp\SecureUpdateSetup.exe

C:\Windows\Globalization\Sorting\sortdefault.nls

C:\Program Files (x86)\GUMFAA1.tmp\goopdate.dll

C:\Windows\System32\IPHLPAPI.DLL

C:\Windows\System32\winnsi.dll

C:\Windows\System32\netapi32.dll

C:\Windows\System32\netutils.dll

C:\Windows\System32\srvcli.dll

C:\Windows\System32\rasapi32.dll

C:\Windows\System32\rasman.dll

C:\Windows\System32\version.dll
C:\Windows\System32\userenv.dll
C:\Windows\System32\profapi.dll
C:\Windows\System32\wtsapi32.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\System32\msi.dll
C:\Windows\System32\msimg32.dll
\??\PIPE\wkssvc
C:\Program Files (x86)\Safer Technologies\CrashReports
\??\pipe\SaferCrashServices\S-1-5-21-2298303332-66077612-2598613238-1000
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_en.dll
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdate.exe
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\SaferUpdate.exe
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdate.dll
C:\Program Files (x86)\GUMFAA1.tmp\SaferCrashHandler.exe
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\SaferCrashHandler.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferCrashHandler64.exe
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\SaferCrashHandler64.exe
C:\Program Files (x86)\GUMFAA1.tmp\SaferUpdateComRegisterShell64.exe
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\SaferUpdateComRegisterShell64.exe
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_am.dll
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdateres_am.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ar.dll
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdateres_ar.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_bg.dll
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdateres_bg.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_bn.dll
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdateres_bn.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_ca.dll
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdateres_ca.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_cs.dll
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdateres_cs.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_da.dll
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdateres_da.dll
C:\Program Files (x86)\GUMFAA1.tmp\goopdateres_de.dll
C:\Program Files (x86)\Safer Technologies\Update\1.3.129.7\goopdateres_de.dll

MUTEXES

secure-browser-50.0.2661.205_installer_mutex
IESQMMUTEX_0_208
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\Safer{D19BAF17-7C87-467E-8D63-6C4B1C836373}
Global\Safer{A9A86B93-B54E-4570-BE89-42418507707B}
Global\MSILOG_f6fbb9701d3f48eGOL.09826ISM_pmeT_lacoL_ataDppA_resu_sresU_:C
Global_MSIExecute

MODIFIED REGISTRY KEYS

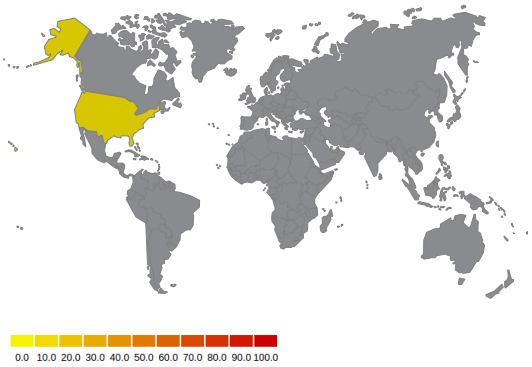
HKEY_CURRENT_USER\Software\Safer Technologies
HKEY_CURRENT_USER\Software\Safer Technologies\user_id
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Safer Technologies\user_date
HKEY_LOCAL_MACHINE\Software\Safer Technologies\
HKEY_LOCAL_MACHINE\Software\Safer Technologies\Update\
HKEY_LOCAL_MACHINE\Software\Safer Technologies\Update\ClientState\
HKEY_LOCAL_MACHINE\Software\Safer Technologies\Update\Clients\
HKEY_LOCAL_MACHINE\Software\Safer Technologies\Update\Clients\{430FD4D0-B729-4F61-AA34-91526481799D}
HKEY_LOCAL_MACHINE\Software\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}
HKEY_LOCAL_MACHINE\Software\Safer Technologies\Update\ClientStateMedium\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\UninstallCmdLine
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\Clients\{430FD4D0-B729-4F61-AA34-91526481799D}\pv
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\Clients\{430FD4D0-B729-4F61-AA34-91526481799D}\name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}\pv
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SaferUpdate.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SaferUpdate.exe\DisableExceptionChainValidation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\IsMSIHelperRegistered
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\LastOSVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\version
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Safer.OneClickCtrl.9
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Safer.OneClickCtrl.9\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Safer.OneClickCtrl.9\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Safer.OneClickCtrl.9\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\ProgID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\ProgID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\Implemented Categories
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\Implemented Categories\{59FB2056-D625-48D0-A944-1A85B5AB2640}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4424021B-831C-4F50-A74F-1AF30ADA650C}\Implemented Categories\{59FB2056-D625-48D0-A944-1A85B5AB2640}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content Type\application/x-vnd.update.securebrowser.com.oneclickctrl.9
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content Type\application/x-vnd.update.securebrowser.com.oneclickctrl.9\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Safer.Update3WebControl.3
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Safer.Update3WebControl.3\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Safer.Update3WebControl.3\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Safer.Update3WebControl.3\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\ProgID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\ProgID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\Implemented Categories

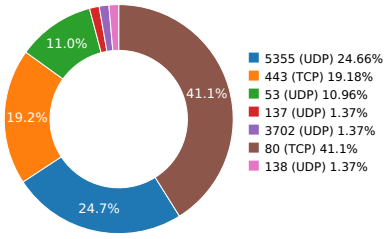
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\Implemented Categories\{59FB2056-D625-48D0-A944-1A85B5AB2640}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{62593C70-ACF0-44CC-8716-990919D46A85}\Implemented Categories\{59FB2056-D625-48D0-A944-1A85B5AB2640}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content Type\application/x-vnd.update.securebrowser.com.update3webcontrol.3
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content Type\application/x-vnd.update.securebrowser.com.update3webcontrol.3\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}\brand
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}\InstallTime
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}\DayOfInstall
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}\DayOfLastActivity
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Safer Technologies\Update\ClientState\{430FD4D0-B729-4F61-AA34-91526481799D}\DayOfLastRollCall
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{C3AB7A34-75F2-4D4B-90FD-EEE151AEA971}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{C3AB7A34-75F2-4D4B-90FD-EEE151AEA971}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\SaferUpdate.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\SaferUpdate.exe\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{C3AB7A34-75F2-4D4B-90FD-EEE151AEA971}\LocalService
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{C3AB7A34-75F2-4D4B-90FD-EEE151AEA971}\ServiceParameters
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SaferUpdate.Update3COMClassService.1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SaferUpdate.Update3COMClassService.1.0\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SaferUpdate.Update3COMClassService.1.0\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SaferUpdate.Update3COMClassService.1.0\CLSID\(Default)

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.18.21.226	United States	13335	Cloudflare, Inc.	Malware Process
crl.microsoft.com	23.67.251.99	United States	20940	Akamai Technologies, Inc.	OS Process
ctldl.windowsupdate.com	23.67.251.96	United States	20940	Akamai Technologies, Inc.	OS Process
gp.symcd.com	23.35.171.27	United States	20940	Akamai Technologies, Inc.	Malware Process
update.securebrowser.com	54.172.8.74	United States	14618	Amazon Technologies Inc.	Malware Process
crl.globalsign.net	104.18.20.226	United States	13335	Cloudflare, Inc.	Malware Process
gp.symcb.com	72.21.91.29	United States	15133	MCI Communications Services, Inc. d/b/a Verizo..	Malware Process
g2.symcb.com	23.50.75.27	United States	3257	Akamai Technologies, Inc.	Malware Process
installer.securebrowser.com	54.172.8.74	United States	14618	Amazon Technologies Inc.	Malware Process

VALKYRIE COMODO

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	17.8116970062
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?42517b9f220bf520 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?42517b9f220bf520						
g2.symcb.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	23.1835768223
Path: /MEQwQjBAMD4wPDAJBgUrDgMCGgUABBSxtDkXkBa3l3lQEfFgudSiPNvt7gQUAPkqw0GRtsnCuD5V8sCXEROgByACAwI6cQ%3D%3D **URI:** http://g2.symcb.com/MEQwQjBAMD4wPDAJBgUrDgMCGgUABBSxtDkXkBa3l3lQEfFgudSiPNvt7gQUAPkqw0GRtsnCuD5V8sCXEROgByACAwI6cQ%3D%3D						
gp.symcb.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	25.8646228313
Path: /gp.crl **URI:** http://gp.symcb.com/gp.crl						
gp.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	25.8668467999
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRH4mIoBb%2Bhjdi7K%2FE2J4ZS9L%2FZgAQUl8InUJ7CyewMiDLIfK3ipgFP2m8CEF9%2F3iBjBpfCaXcXqCUlYAI%3D **URI:** http://gp.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRH4mIoBb%2Bhjdi7K%2FE2J4ZS9L%2FZgAQUl8InUJ7CyewMiDLIfK3ipgFP2m8CEF9%2F3iBjBpfCaXcXqCUlYAI%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	65.566298008
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	65.6035349369
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	65.897993803
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	66.4179048538
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						
update.securebrowser.com	80	POST	1.1	Google Update/1.3.129.7;winhttp	1	69.6486508846
Path: /service/update2 **URI:** http://update.securebrowser.com/service/update2						
update.securebrowser.com	80	POST	1.1	Google Update/1.3.129.7;winhttp	1	72.6810259819
Path: /service/update2 **URI:** http://update.securebrowser.com/service/update2						
update.securebrowser.com	80	POST	1.1	Google Update/1.3.129.7;winhttp	1	82.9299409389
Path: /service/update2 **URI:** http://update.securebrowser.com/service/update2						
update.securebrowser.com	80	POST	1.1	Google Update/1.3.129.7;winhttp	1	85.657148838
Path: /service/update2 **URI:** http://update.securebrowser.com/service/update2						
update.securebrowser.com	80	POST	1.1	Google Update/1.3.129.7;winhttp	1	114.299767971
Path: /service/update2 **URI:** http://update.securebrowser.com/service/update2						
update.securebrowser.com	80	POST	1.1	Google Update/1.3.129.7;winhttp	1	117.098057985
Path: /service/update2 **URI:** http://update.securebrowser.com/service/update2						
update.securebrowser.com	80	POST	1.1	Google Update/1.3.129.7;winhttp	1	157.420171976
Path: /service/update2 **URI:** http://update.securebrowser.com/service/update2						
update.securebrowser.com	80	POST	1.1	Google Update/1.3.129.7;winhttp	1	160.237128973
Path: /service/update2 **URI:** http://update.securebrowser.com/service/update2						

DNS QUERIES

Request	Type
installer.securebrowser.com	A
Answers - 54.172.8.74 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - a1621.g.akamai.net (CNAME) - 23.67.251.96 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
g2.symcb.com	A
Answers - ocsp-ds.ws.symantec.com.edgekey.net (CNAME) - e8218.dscb1.akamaiedge.net (CNAME) - 23.50.75.27 (A)	
gp.symcb.com	A
Answers - crl-symcprod.digicert.com (CNAME) - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
gp.symcd.com	A
update.securebrowser.com	A
crl.microsoft.com	A
Answers - 23.67.251.99 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.18.21.226 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.18.20.226 (A)	

VALKYRIE COMODO

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
12.2081639767	Sandbox	54.172.8.74	443
17.8116970062	Sandbox	23.67.251.96	80
23.1835768223	Sandbox	23.50.75.27	80
23.2787950039	Sandbox	54.172.8.74	443
23.5065598488	Sandbox	54.172.8.74	443
25.8646228313	Sandbox	72.21.91.29	80
25.8668467999	Sandbox	23.50.75.27	80
27.2698528767	Sandbox	54.172.8.74	443
52.1065587997	Sandbox	54.172.8.74	443
54.8306109905	Sandbox	54.172.8.74	443
55.8851439953	Sandbox	54.172.8.74	443
65.566298008	Sandbox	23.67.251.99	80
66.3887329102	Sandbox	54.172.8.74	443
66.4179048538	Sandbox	104.18.21.226	80
68.2396478653	Sandbox	54.172.8.74	443
69.3236789703	Sandbox	54.172.8.74	443
69.6486508846	Sandbox	54.172.8.74	80
72.6810259819	Sandbox	54.172.8.74	80
82.9299409389	Sandbox	54.172.8.74	80
85.657148838	Sandbox	54.172.8.74	80
111.441561937	Sandbox	54.172.8.74	443
114.23285985	Sandbox	54.172.8.74	443
114.299767971	Sandbox	54.172.8.74	80
117.098057985	Sandbox	54.172.8.74	80
157.420171976	Sandbox	54.172.8.74	80
160.237128973	Sandbox	54.172.8.74	80
190.138350964	Sandbox	54.172.8.74	443
195.763925791	Sandbox	54.172.8.74	443

VALKYRIE COMODO

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.01841878891	Sandbox	224.0.0.252	5355
3.02184486389	Sandbox	224.0.0.252	5355
3.02958297729	Sandbox	239.255.255.250	3702
3.07947897911	Sandbox	192.168.56.255	137
5.57993292809	Sandbox	224.0.0.252	5355
9.09432291985	Sandbox	192.168.56.255	138
9.57830190659	Sandbox	224.0.0.252	5355
12.1488609314	Sandbox	8.8.4.4	53
12.5883009434	Sandbox	224.0.0.252	5355
15.181746006	Sandbox	224.0.0.252	5355
17.7388498783	Sandbox	8.8.4.4	53
17.9774599075	Sandbox	224.0.0.252	5355
20.5482769012	Sandbox	224.0.0.252	5355
23.1110479832	Sandbox	8.8.4.4	53
23.2364377975	Sandbox	224.0.0.252	5355
23.2470118999	Sandbox	224.0.0.252	5355
25.8178567886	Sandbox	8.8.4.4	53
25.8181939125	Sandbox	8.8.4.4	53
51.5700550079	Sandbox	8.8.4.4	53
53.2810709476	Sandbox	224.0.0.252	5355
65.4506537914	Sandbox	8.8.4.4	53
65.595140934	Sandbox	224.0.0.252	5355
66.3737568855	Sandbox	8.8.4.4	53
66.5369389057	Sandbox	224.0.0.252	5355
69.9206619263	Sandbox	224.0.0.252	5355
83.0652458668	Sandbox	224.0.0.252	5355
111.610507965	Sandbox	224.0.0.252	5355
114.421365976	Sandbox	224.0.0.252	5355
157.577675819	Sandbox	224.0.0.252	5355

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Windows\Tasks\SaferUpdateTaskMachineCore.Job	**Type :** VAX-order 68k Blit mpx/mux executable **MD5 :** aed73736ea9f2f7765d6e3532b14f9dd **SHA-1 :** 273ae3aaebdb92bcee43b420178d21210f8ff5b7 **SHA-256 :** 9784e3c36a35a089031a5298878772b6c579079fbe2ebec536d7fde67b186bf3 **SHA-512 :** 89117cfbc69e9059a212484a284303b69ba04abdd20a6525087fd96db8e125b1a297 **Size :** 0.906 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferUpdateWebPlugin.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 252f868cae6415cd3f209145c11b6eaa **SHA-1 :** e54efdeb00456fff378564cb095aa6bfdef388d5 **SHA-256 :** 23d97015790b650397a3cb9345b65b180dcdb7fb6c3701c6982830fbe8224350 **SHA-512 :** 15f8ae0db004abc06c7b04970b02eb557e33e1475fb012e1f9c2bfa6dd5225a454136 **Size :** 87.968 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ms.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 404f7a5517a0527750f344e2ea143445 **SHA-1 :** e65799d6e97cd56d485a5fc9548df267e8f575e2 **SHA-256 :** 4eb132cfca8fe953849e84746264e13a95b8cc1564fa806a9df10b1e3e9fb11f **SHA-512 :** 3c24a1dda292994a3bbac3893d40b41c2b7e701c598a20f380b7bf94789d3ed0f4a76 **Size :** 38.304 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_it.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4855f60a5f9eb0e458a2d02607fe43f8 **SHA-1 :** e95637acd1f95013ca55f749d501f6b9faa0b99f **SHA-256 :** 094ea79279655126e2e617deddefdcb0e90f4271084e022926c471977ef6f30a **SHA-512 :** 9311e614a0945ffc4871780528cb8af9b7cde63ab89938eb2a215411b6cf1913ff2848f **Size :** 40.352 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_zh-CN.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** fdcf28fe424c00abf2e0f2f06ad5eca5 **SHA-1 :** f7157e075751808a2c69d2bf58675279d9be4893 **SHA-256 :** 3ec5b78a92f17cd37e4727eabcc61b96400d733f4159e5a1057f599710dd879b **SHA-512 :** 611754fe56c9f278d15f6dcda19024693f675ddb9c809246cc73a0e15627915be92df9 **Size :** 32.672 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_hi.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 8eb9a58fae2576f5bb22c2a8f84a7720 **SHA-1 :** 0fd51e278d70c413ef224a66c62da6e13b24b744 **SHA-256 :** 41837bd98ba4524d023a5028b8fef0b8ac1e5f8b1058bd985ef71b4adb0cca83 **SHA-512 :** 93eaeb8472d9e4de994b229991b39f852de3c588c06f8953b6933bd9b621ba5629f7e **Size :** 38.816 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferUpdateSetup.Exe **C:\Program Files (X86)\GUMFAA1.Tmp\SaferUpdateSetup.Exe** **C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\SecureUpdateSetup.Exe**	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** cbd8800d68c19e033145d6038f257389 **SHA-1 :** 30aa0c20deaea87062b86c0d1ceb82bc78f4e11d **SHA-256 :** 8f58b5af83fdcf9f3ddae4af7e3d6814eb637acd25ba0688e251f00c53f89bf2 **SHA-512 :** 33e14cec7b0935e2255a58e8b77f568a82915fbe162f71c4f2ed4f63d356df163492aa1 **Size :** 924.848 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0F1583FFF42FFF476A09801ACB69213F_D4C83E2943267C1763EC8ED5C0DDE848	**Type :** data **MD5 :** 68b73be444f891311e29c92652bfc8b9 **SHA-1 :** 1d252954e5dc08175953f4305c1a838dbe62108d **SHA-256 :** cc603dedb4bb0b11072e5bdb34db0081aed18e6b0c5d476cdb067e2f0b5d18e4 **SHA-512 :** 2f25873a26d1c45e3e9bc5591701eb33fbf9c5a76a2a3847b0729a397814c8de6cbf56 **Size :** 1.378 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\StdUtils.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386, for MS Windows **MD5 :** eae3ad27a38d80364f9469f22459ef3f **SHA-1 :** 6fd0eaf0765e275048957ef08940e013e6aa7043 **SHA-256 :** 44f2b6eef0532eac20c5d308fb64130a1dc010b617cfd0f532a6cdec2d5d81ba **SHA-512 :** f7cdcb8d4c31c3a5f3f57fc5a0c97402fa28335372c96e1c1bae6834db26204ef5ee657f **Size :** 95.744 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferUpdateComRegisterShell64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 9aba4de7e7e95c1c2553fd8946f5b939 **SHA-1 :** fff1b7285310ec98bd8264f7a0dc0c40bc07c67c **SHA-256 :** a0086ab3beb05c2a22fe1d7ff6dfda4507438ef28d3b64e7c6a35abf9387159f **SHA-512 :** 56b3d36b426843a01dbe225c1a2755d2fb21d11f554d9bcd24b8f8067d60b168e3ddf **Size :** 130.464 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ur.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 95435dcb0c4e76775b2fd4e4a53e7d7b **SHA-1 :** 5fff41f3d08c1a3722e20371446bb559685ff84d **SHA-256 :** 2b4e5d36579babdc60b44bf7b4a7b553babbb32f07f8674615cc1df90832de27 **SHA-512 :** 7afd45acb1b30bcdc1be028f3f46ee0181e80a7cbc788ec69d8449a9126e33a32832e1 **Size :** 38.816 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferUpdateOnDemand.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 6202ca9dcce0c261f2ebdd275d44eff1 **SHA-1 :** fd869b4fdd0f17a0ff24dff9e36cb61ff48d2cb5 **SHA-256 :** 29d9649953d6480920e40060ea9a3ed99fc68e002960ddb55abffca14e8af3c1 **SHA-512 :** c65277b40394fdbf217424f56567a2dff4f9e9e5ee250a8f84a0483bd441a2261a7ee4c **Size :** 87.968 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c396f72ffe42fd1b781c24cba **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872e06fb79f4af4f35d020ed0add9d8d1l **Size :** 6.509 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_lv.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** e4dc1518b58641890dfa842aef9e23a3 **SHA-1 :** ab385995605092ad47ca3955e346b86929909d9e **SHA-256 :** 5a31b630475a83b1dc12e215cb1fc69d9f4cf3f57738a04f34606d3af14f719f **SHA-512 :** e518405a59fd8264dac56152a378882f9b8661735edbdf52701271cfae2489715ccd31 **Size :** 39.84 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_pl.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f7bc7c2059fc6d4b10fc435472fcbfcb **SHA-1 :** 35798ae97945d3cd47a171a66b005e1f0ed2cff6 **SHA-256 :** 8bca551d4755c12c6d4886d297f2157ee8a736674f600d36de105bb4873ec0a1 **SHA-512 :** 38d5b965f779d3d77d7632144a4316d8367415e24da424b4e26e6b6d9ed406f695a8 **Size :** 39.328 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_gu.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f15b78dbc16caab7989f918688b80b92 **SHA-1 :** 0238b9e66cd360a984bb3eae04473739aaffd144 **SHA-256 :** 9cb5775f666ba6060f212ab24689e48b6906c15b9ed102c11dd42074c2c07f82 **SHA-512 :** b7ac094c8f32f75f7bf8d2edefe93abef55798e4a1442ec14b3bbc044697d7d67997a4 **Size :** 40.352 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Psmachine_64.Dll	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 3dc2a254ed8031f0236bc21b9322de72 **SHA-1 :** c2555da60181d88d16f090c86ac4b3150ecd72f0 **SHA-256 :** 642a5eb2afd66839f8c19be16cdc3ff6741342a38d2a7f7878ed0d9815c10918 **SHA-512 :** 4c1032150ead281e28be352fd1059d4b5ae6f524bebb1006131fee9fd1455a227c2ef7 **Size :** 214.944 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\NsProcess.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** faa7f034b38e729a983965c04cc70fc1 **SHA-1 :** df8bda55b498976ea47d25d8a77539b049dab55e **SHA-256 :** 579a034ff5ab9b732a318b1636c2902840f604e8e664f5b93c07a99253b3c9cf **SHA-512 :** 7868f9b437fcf829ad993ff57995f58836ad578458994361c72ae1bf1dfb74022f9f9e94 **Size :** 4.608 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_fil.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b6390c657552fc13eeb2970344d6bbb4 **SHA-1 :** 789a49ee944abb0342fa50441c493a6f033fefc0 **SHA-256 :** 0dd457fe0a7678ce75d7674bcdf76c83d8fe7d2847c58a60a3fd9b835a0957de **SHA-512 :** 14af9adbb65184f33e6a53097c208686e9aa5b6fbcd5d8679bc62fb1217c4296842075 **Size :** 39.84 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferCrashHandler64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** 6e4f35484f0714b15eb5dc6883a30c31 **SHA-1 :** 91ea590b29d0d468a0664a4a881018cba159b022 **SHA-256 :** cb93d440a69d74da645a14034f49aeb88ddec2bb3c6cac19e737084797a3c30a **SHA-512 :** 16910c1c80ddfd39c7601ee2a5897aa69a382c24f79873e7bcf478cec23582ba35e891 **Size :** 307.104 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\DE624068503F3B953A6EC67A0654E15F_81E07CC400DF4DB0ECA725A050D525AB	**Type :** data **MD5 :** 0e1333741c590ae72b510edf3584653f **SHA-1 :** e30c10f50237838333397e6d1fbbfaea0ac18db4d **SHA-256 :** e5972091ea6bd98ce66ef3b770aa2d2a1cffbe959bdd054584fccc42b2f38116 **SHA-512 :** 5d5eb4ff935448409c55de608f200345795b2941309b6137068116430597e92f76b2f6 **Size :** 0.402 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ru.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 818484e7ad48b6d81b5bd259ccba286b **SHA-1 :** 0189ba7d1637642ba2e7fedfc81c1a8c2dc5b07a **SHA-256 :** d5324b3dba0ca8a45cd4d6b638b14915e5bbc4fe03b3439527ae41dfe5fb9659 **SHA-512 :** 6d328c108c69b26ee59fd84d4d63da4b3b30743773da55b1f4734ce7461842c46c576 **Size :** 38.304 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_id.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 704eb0c09ce9e9b8d8f1f42a789fcc0a **SHA-1 :** aadfb35eff9cd9048261c81d4b38991b08fbe298 **SHA-256 :** 5aee276f05ace6d55626258416c33248cd8d4c4df3517bff6a1a39248107b2af **SHA-512 :** 64608a580e01dc7d3cc891433646d34db5e946d3befe74c4d8d99d6c678edd9e4085 **Size :** 38.304 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_pt-PT.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** cbbd04227f459e9b98d238240ba630f1 **SHA-1 :** 5203f1b705103bfa7ab68a692ef2c747ebe572af **SHA-256 :** 86b2f28a1f6b5f438fdd17d4b94797869aab7ac94c92ac61d3d99894d5d8bafd **SHA-512 :** e46533973fd345196217137e65d3d45ea7c72e04af5fd1c2b04535d495c792aa50609 **Size :** 39.328 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferUpdateHelper.Msi	**Type :** Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Title: Installation Database, Subject: Safer Update Helper, Author: Safer Technologies, Inc., Keywords: Installer, Comments: Copyright 2013-2014 Safer Technologies, Inc. All rights reserved., Template: Intel;1033, Revision Number: {5AF0D38A-A4A1-45D1-99B0-919A0A154EBE}, Create Time/Date: Tue Mar 1 10:16:20 2016, Last Saved Time/Date: Tue Mar 1 10:16:20 2016, Number of Pages: 300, Number of Words: 0, Name of Creating Application: Windows Installer XML Toolset (3.8.1128.0), Security: 2 **MD5 :** fd2aedacf6f5c5bfd95d778b2fb07445 **SHA-1 :** 1d4679d81cfc55683257d3aa6b42e92bab78e850 **SHA-256 :** 74f1c87a6d128a6537ada9853c80de7204c6dbfc233c9947ed05cce9b67c801c **SHA-512 :** cde20996032edc710ffbf9a2a00e3aa76de52e63e5e56ef1adb980e96075f70d2bec4a **Size :** 40.96 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_uk.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 766adfd5857e8de52aa487b0165cd3ee **SHA-1 :** 4e57fc6feba01e8ba24baf6213dd792810991fba **SHA-256 :** bc15188ac87be8dc259932752acd553ca2ae2c057692e2df944f21c6b4d1d707 **SHA-512 :** ee521e0a80d25fc8c74a0cbe72e7c7864a90d8bb68b16ddf095b7658eaefff0b3b502c **Size :** 38.816 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ja.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c3d1935bb1f6d11bc5250a3bb0475c4f **SHA-1 :** ca5f96bf2d69220b76278b5015fc21217bc7752a **SHA-256 :** 62e5ca25ca57c1917c11eba541e42d7110bf1bd2ede3753dfde5496fc2fa5a01 **SHA-512 :** b6a6522f1a70200ba9939b7bd083c6b4109efee30fa9b1d68fe09195f2e291f400959e **Size :** 35.232 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_bg.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** d55137b96b79b2483d30669e70ed14c9 **SHA-1 :** 627fd3cc07e0de141cbcc0924cb2dba4cf069c9f **SHA-256 :** 5e6183cf532a8ab7b67682d2b88aecaf8a42ba49683e648ad8a707b54705fc9a **SHA-512 :** f0ae938c06f487a75bdbd72deb27648120946beade577e51d5d13866358c9e9c06fdc **Size :** 39.84 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_fr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 57e3152957704638c62113b46692a6c4 **SHA-1 :** 9a71503676bee5370123ebb2ecb880046f110d80 **SHA-256 :** ac6cea0a0080cafde7fdae92ccb59eddace7f3b9bc0f97a80037b25080eff7cb **SHA-512 :** 30148692fff6bd3d7370e6960275f8cb5bf7cfd1fb7262045cf73c43b859c0c293bcaf79 **Size :** 40.352 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferUpdateBroker.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 413528faf72d46bcb4c580b1eb4c6d5d **SHA-1 :** cfb6a80624260867a7b2dc1c41636a2498ab6a32 **SHA-256 :** ecd24d40c6c285f4537ac450efd3284ee0ad34ef9e249bad29e32265efb7a8fd **SHA-512 :** 710179633a0efdf2d77913f53e2b016bc605833756bcc2c911d6f1d20abdb9b7e3decc **Size :** 87.968 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\System.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4d3b19a81bd51f8ce44b93643a4e3a99 **SHA-1 :** 35f8b00e85577b014080df98bd2c378351d9b3e9 **SHA-256 :** fda0018ab182ac6025d2fc9a2efcce3745d1da21ce5141859f8286cf319a52ce **SHA-512 :** b2ba9c961c0e1617f802990587a9000979ab5cc493ae2f8ca852eb43eeaf24916b0b29 **Size :** 11.264 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ar.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 15df9d463c8ff12dbd8166f9401ae67f **SHA-1 :** 45ee529dd1f309d093eba45b8b478791aa4116a6 **SHA-256 :** aff8d7d70bd43cd65b9d97390860a5c5e4ad8014ff21bf00261120bfe9494dc9 **SHA-512 :** 108476b3d4dd9462958320107467849 72ecb0c73b40935b4fb7ecfbbe819ed031bb14 **Size :** 36.768 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_am.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b649535a23837ea8ec8055eb611ffbd8 **SHA-1 :** 62a29db54e00ba6b0bb08a2fa432ba8525b9fd32 **SHA-256 :** d85273e47af7473c3a54fa203cc296f37363252673d56e01d51cbe0f61649830 **SHA-512 :** 9f2dcadab63b402e1f231ae8c81056e5dcf24a51df6e7d7859679d4b14eeaee1a6d272 **Size :** 37.792 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_en-GB.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 89963ef1b0d626625ada73911fd1a59d **SHA-1 :** 0550360444298724 1018ea7ee74c432aa7562dbb **SHA-256 :** f26f58e9aeabb05dfdb0cb3a62c728136802bd987c239fc89f3f96cbb0776031 **SHA-512 :** 815789febab2b759173dc3d4018ace19da8fb1280e925acd5bf265f89d896d16a1969(**Size :** 38.304 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_sw.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f504fa089bfb167b4d99b0fc3ca9678b **SHA-1 :** 4e5b477b282b2cf26ea28d40dfc41e8bc899d2f1 **SHA-256 :** 82812cb1511153c13f0b63c0d2e5bc1ef2ea05933296b48b696076fed5a12ea8 **SHA-512 :** f64de15e3feed03fac1d93840bd440375c5e78e4633ca2ba56ff10d82999b2c7b32193 **Size :** 40.352 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\DataReaderNSIS.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 37ae60c9d44e46cae9bb7db3d7494069 **SHA-1 :** 1c322c718b4f569fee679734f6c370fd6a51a5d8 **SHA-256 :** 17052b6594fa8830f54f62556fd804f0274904c1abd398fe80ed49c62d68ca9a **SHA-512 :** 25482528c7dcdcc86da88ac7f8cc75f2edca5f5431a800e0e561c8c4e453f50d201aa5e **Size :** 49.152 Kilobytes.
C:\Windows\Sysnative\Tasks\SaferUpdateTaskMachineUA	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 386d1c9100e8c3e227ad2b57d8aef995 **SHA-1 :** f42931f33560bf6e8380df00baa1b6a05df430c1 **SHA-256 :** 2f28b36a5b3a7a010eee1ebbebc89daf7ca0ca7534bcfc286406000127c48912 **SHA-512 :** 04efb3cfd2c4a76d9ea1eea32803dd547aa0b3263311178d857a2e43d2c7ca9724937 **Size :** 3.906 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdate.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 7fee8cefdd1cd0f72c044f10807c0608 **SHA-1 :** d5bce60f1818a2b212474935bc639c2086971fdf **SHA-256 :** 8572057c6628615828d145c3b586aeaba70713b1f1454bf68677483b4bb67ed2 **SHA-512 :** 288c45660171b2251d16225512bc4323555c3f5ef42ba900f8cf3a07ddd81d7f868e5a **Size :** 1682.336 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_hu.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 1f7206734a053889ad51edf599360f2e **SHA-1 :** 1f01b54c0b4489d7a7cd2dd6d1e98727102df55a **SHA-256 :** b91cec4964d5b1fb2f2f795ab777abed47a0cee04ab204b578b8722f680c0df2 **SHA-512 :** be141b9d08b63dbe2020a31ffdd1cc0a9f8308e331aca903178caa2419b110d00562c4 **Size :** 39.328 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Psuser_64.Dll	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 379af609d16fc59b5588356d2c077f56 **SHA-1 :** bb31da7e60299c7923df96664d416ae5fc750447 **SHA-256 :** f677e90c70cbf0b6cb6ac435d81153bbacb3abebe97c0001dd8b94d4a1716139 **SHA-512 :** c00085df8c76a700bb50fde03248449aa310d27ed13626fac1fb1f3208a0b84e0fc525e **Size :** 214.944 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_nl.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 99d44850a985babe95b9115a83d31790 **SHA-1 :** 356154a815b995daa0e07e194f7ec82f60034a83 **SHA-256 :** ec34561b2ebd88109945be2a558201c1c16f322f746f1c2a2a2acbfee5fed0df **SHA-512 :** b512eeda5b92db94f4168404fbb0e9451deefe3f033c74a667fdb1be86a52de1a3c89e **Size :** 39.84 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_sr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b2df183ece6c3e418eeb57527d0d1d19 **SHA-1 :** c0410e829166ec696e3ce97eb26124482d76f3fc **SHA-256 :** 8429d08830ee6aa6c45e866a52130e72e6c7f0762ca650812076020458e324cf **SHA-512 :** f098fbe339dc1c2b46ebfe6583f32330f24e1b96c939f15d71ca76c0952f697910be460 **Size :** 38.816 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\NsDialogs.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 137b32c8564ff1648fc0a9f939384c47 **SHA-1 :** 44e48979c3ae5ba65923d3fb229518b5957f685b **SHA-256 :** 89b99998b83155254aeb6e90713cb6118e0c72e71e51853af01bc218bd9e1e11 **SHA-512 :** 19b62d6413cdc1d4d28be75367325a7aa283ed801ca9450bd19187f75b745ffa43854 **Size :** 9.728 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6E5336CDD9652A36A93E734B280625C5	**Type :** data **MD5 :** ee1217065e6478f0b3f1c8afae5d467b **SHA-1 :** fa760e62546b432388d885ff24748c79bdcac2e9 **SHA-256 :** 4f020985a2cf70f1b165df23adf7c0da292a47c6a1157c6c067900b606d154d2 **SHA-512 :** 7706a76568ef2685c429098619e4a5a3877d24f14f137b3fb58219e3547d45daa2ce21 **Size :** 646.875 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\Inetc.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** d7a3fa6a6c738b4a3c40d5602af20b08 **SHA-1 :** 34fc75d97f640609cb6cadb001da2cb2c0b3538a **SHA-256 :** 67eff17c53a78c8ec9a28f392b9bb93df3e74f96f6ecd87a333a482c36546b3e **SHA-512 :** 75cf123448567806be5f852ebf70f398da881e89994b82442a1f4bc6799894e799f979f **Size :** 22.016 Kilobytes.
C:\Program Files (X86)\GUTFAB2.Tmp	**Type :** POSIX tar archive **MD5 :** 10732ed1957e7101ba8506fcf1de1269 **SHA-1 :** 2d2465bc5629aed97a12fb0def0d723e07bf7786 **SHA-256 :** 12883d0ae4fa7c896fb630701ac6b97f8951142670b07764b5ff7fe129288cf7 **SHA-512 :** 0c7a2fe1a238193cbfecd9fa02282736fb7df1f09ba24795c17bec450c60aabd3bb7f1f1 **Size :** 6379.52 Kilobytes.
C:\Windows\Sysnative\Tasks\SaferUpdateTaskMachineCore	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 6411f7da9075d12d63b42ef6c88277f4 **SHA-1 :** bcaf187d8d7829764d352de3424ce445256af480 **SHA-256 :** 4c6af86a4a7b503421402aad3cb25d4905c1a3097aed094d5d5060e359610d2f **SHA-512 :** d63835e1b95e112c725fc4c93cec6678c110252f057f911b5dc8e74c6d1163577cc5f6c **Size :** 3.654 Kilobytes.
C:\Windows\Tasks\SaferUpdateTaskMachineUA.Job	**Type :** VAX-order 68k Blit mpx/mux executable **MD5 :** ce7e6a08fab8196858cc6274c14753ac **SHA-1 :** 9501d780856a0aabe7488502bd1c280cf48a0890 **SHA-256 :** cdac2f5daa85b5565f9032f1ce16636b786f733926d1bc05c46e1b9d527abc15 **SHA-512 :** 1d70d93a9c93afb88084889ea6d59e4b388e4ae632133c13780ba8cdcc8e21b4773af **Size :** 0.91 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_es.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 68d473cb10a9a95ad5f0b40d05c93742 **SHA-1 :** 212c91c8c53a04c10197edefa6219a770f8868f2 **SHA-256 :** f3cc32c233f0fd70c022fbd5d9343a92e284b72a5f628f2b7ccb9a977760d358 **SHA-512 :** 32cd694fed50730dc2bb807b416592aa03885080dc05c1dcbe4839e3eb636f5a0b681 **Size :** 40.864 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_cs.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 1504cf73dd36adb98900d3a6762e3f84 **SHA-1 :** 45de9cb195f3a5a9dc7acee3d1b2459a97e5bd9c **SHA-256 :** 9926654dc771f2d9a8aa6a8f43e6566e0e369b739e09be5dbee71a81b775b5f2 **SHA-512 :** c34cdde8a0f75eb8075383aab01ef706c0812bb4850ea78558c5299e13cc98db0bf943 **Size :** 38.816 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_de.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c82716d3a592ebe8271d2d05a6a508e3 **SHA-1 :** 9fba335bd2a6cb7fbfa0976f5dd5124f25ebb997 **SHA-256 :** 133ece3ebf9d0cb9960d9942d264f20f34665b0276dd815793f92f5d032b187d **SHA-512 :** bbfc3eb7249c29b3746953cb9bb58ee0d0faeac1502a2b23bf1d5d1088095f91719457 **Size :** 40.864 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_te.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 0dabc5047e617b0b4e0519423d6ad164 **SHA-1 :** 32ee4220c2e88a3493bc944e8952c7d2d6990312 **SHA-256 :** 164d7218cb5e99c080dafb7e55cc80fd78420ef52e8c1482c1c9053bda2a821f **SHA-512 :** f4bd35844736e87c7fcb08385d203d9f054187fd1eb60addfbe0687bb654b32375bb4 **Size :** 40.352 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Windows\Appcompat\Programs\RecentFileCache.Bcf	**Type :** data **MD5 :** 986d533ad49f79dc2b1b524d7fb6535f **SHA-1 :** e7786b3f3a21a8b75c337c193312561e80789998 **SHA-256 :** fcbe788ea3d2da5f14c85fbdad32e2ac3b87a8614db0d7a51007d9dff1a1e847 **SHA-512 :** e38dd6a98a5d6a9c3577d4cf9b6181d7e2c0d356bcd449a7d3439aa9adf7656bf11ab **Size :** 5.878 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_tr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** bd10efaa98d86fe68da1c9d3cc56513a **SHA-1 :** 06b6ca6df34d2aea5e6bd26a850b522ae21ed44a **SHA-256 :** c1e1159e4fdcf43cc9796ec64fe86e34719d008f1c880e97eebba2d748a19416 **SHA-512 :** 515d235d302b98a256fd864e7d76d14edb939a5d70398991f0b83a9795e15b58760f **Size :** 38.816 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\Secure-Browser-Installer-Tracking-Response.Tmp	**Type :** ASCII text, with no line terminators **MD5 :** e0aa021e21dddbd6d8cecec71e9cf564 **SHA-1 :** 9ce3bd4224c8c1780db56b4125ecf3f24bf748b7 **SHA-256 :** 565339bc4d33d72817b583024112eb7f5cdf3e5eef0252d6ec1b9c9a94e12bb3 **SHA-512 :** 900110c951560eff857b440e89cc29f529416e0e3b3d7f0ad51651bfdbd8025b91768c **Size :** 0.002 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_bn.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 24d257dc4a52d206fac90696cac004db **SHA-1 :** 8586f9a3cc855323bf5bcc5a47c050b00b7131ed **SHA-256 :** b81e5e736c572e2d09cd9e2b44ecdbc9a50e6835249f96e8d8f5ba3843659a47 **SHA-512 :** 070d78b4eb77ae882052cad503759ef8c3a3933e72686e2e4d6c37a91322e7844df3f **Size :** 39.84 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_vi.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 7e89872ce4e85b1fc6b48186f7bc8c6f **SHA-1 :** d12d6afbddaf7ebaef1b4c04bf18f9a5eed96866 **SHA-256 :** 7cdc8e703404f48556a460064dac4b1d8b98cdd88f96cda13907b8634b26c0c6 **SHA-512 :** 865dff3f2c65395199f7ecbee6394dcae19af804569eb77e00245c8811b801168c275a5 **Size :** 38.304 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_sl.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 70bae6650663f4297783671553f2f36c **SHA-1 :** 7f6326e1067c38bc8f73f1eca44f1a1b3bd43c36 **SHA-256 :** a361f17eda550a3af69f76fb0de5cbd46f1e54caeaba19843abf8f8181d177a4 **SHA-512 :** 26ada81f3011fc34b0f799e9bff848e79a653be708714f51692ae5d3f132d75b8f27214 **Size :** 39.328 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferCrashHandler.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** ce0c4d94fcb651f1f19c10bbb739a675 **SHA-1 :** 74ceebaaa01fd634c7af8fe4e3f17e782fb0e8ce **SHA-256 :** 15a0dafededfea95f3753ec9a711c1c86da19f616f43c9ffb44395ce5a37dfc8 **SHA-512 :** 419b0ab6e188566e15d5746e8662c1a7bb1e43ca27e8b24ec08163382118d851d33e **Size :** 245.664 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 5051f9fe18e61f15219d8f2db20202f2 **SHA-1 :** 2037486c112923e9d66621d5fc2fd6b287357099 **SHA-256 :** a4c8266c6ae4a09cfbe2018e64d2dc34f1ef96401efa5055e628924bd1e3dfdc **SHA-512 :** a6160f91787cef49ad2039cea3c0b083bd34199a68401fbbc67e1ff61050ea8d9715ab **Size :** 0.342 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\NsJSON.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 588ddeca425c424e21d07ca0c6bc3278 **SHA-1 :** 47dd590721965e13c0a25f334d54955d28e49746 **SHA-256 :** b8a48391a7cf1a04ac2928c9089d76375bcb9a773db67388219558ee4872e902 **SHA-512 :** 2b7ce0ed11d135c9dda748bca2baf5888a9aad0bde550772a4c671ace60a3a7784431 **Size :** 12.8 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_es-419.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 7793a6b0283e51f901102bdd7c5a6f23 **SHA-1 :** 5170483b6c2ac7cc2f9650c53daf3eb4cd0a3a0c **SHA-256 :** 511289523d2d50d01c129b80125836a155886b484ca7a13563453a50e135235c **SHA-512 :** 409391679ec637d3482ed00648caf345adb0aa3f0d616d5fc3f76100db2948b08a22b6 **Size :** 39.328 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Psuser.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 88184ce03ff7992a1cd5b16f54016520 **SHA-1 :** a68f8ebc47c881bb996975ce482c1793ff667441 **SHA-256 :** 88e3e3f5b63158392391d677fd883e49bc9d33903c610db42b03f933014af72a **SHA-512 :** 867b8aafd01d63fbf097834189486141e4774dcb850dac3f506c60e36ad07d3e5aa7f4 **Size :** 184.736 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_iw.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** eeb2aa721db5a310cda4b88bc69edc59 **SHA-1 :** 83b9beff8ec943c1ac8ffb26593841072ca2984f **SHA-256 :** 198d325e6a25bf9b31de162bfa333885726db7e9dadca462db130237254bfd05 **SHA-512 :** c9a1be462810e2e580c11f50a6698523195c45bed2ed3d746bc8b8ca1dab732633f10 **Size :** 36.256 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\SaferUpdate.Exe **C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\SaferUpdate.Exe**	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 2f4a3c81b7bca3ea8b85ad11b13bc44a **SHA-1 :** 3cecea0460aa6468a4cf103ab28046ff592b4265 **SHA-256 :** aadc1c78d53bced66bf371b84f24816d65b9a99ba39fff13e82bc1ac52dda31b **SHA-512 :** 2b3cb34f09ad56a76e935c83ca256a638b60e98dd94430ab88d496723fe8679dbf983 **Size :** 150.432 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_no.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b02a233862eac71ff7547ceac25c9477 **SHA-1 :** c79eb84c3a64b95f7547ee85e4f8bb201e7d4efd **SHA-256 :** 759aae4056f6631b23b1de09c7c61367cf6bfe86a682dd9bd070f870bdf357f6 **SHA-512 :** 8b66b3cea70e3bc8ba377088104bd4215df9560fc1005b477d10af1119452a1a1cd47 **Size :** 38.816 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_en.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 9e142c9529341f431052686c32d42fff **SHA-1 :** eb673ec5b271d2f6f89ccd8b62695f2a1c842ca8 **SHA-256 :** 52a3e773c70577d0c55742a89b411e657ebfba9f904e941c1555ae6d69548f4d **SHA-512 :** d238eea27174e99be5fc6c681f5b35387fca495a051e34b37430de637a819b8a540fbc **Size :** 37.792 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ta.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** a939f5e1148ef48cfa8a2e708fbf5767 **SHA-1 :** d5d8cbef27d6119e530968902b4c1ae7b8271846 **SHA-256 :** 3331aa20f0256a5e7301dc34e0ebe89b83f6b883e3e0b131c13be6bd9f560ca4 **SHA-512 :** 6acfe8c3715abe505ad42909b6f26e9c629356bd4bc6b52729aacdee41c15d088a4a2 **Size :** 40.864 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_th.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** e03a09bbba8017abd9939c9da37097fe **SHA-1 :** e82e32c89b299f9ca8a847af7830ac425479100e **SHA-256 :** b3dba95a058ebdbc328684f85e62139ebcc8ab6cbb8b0e976a2be692f5a1b3bd **SHA-512 :** 853376339cb3c1960b13ef9bb4add3c34d4159a4e2f7118040f01e928d8840e510bce **Size :** 37.792 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ml.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 3fa54c8b4fafbf887d2fe4d0a612cc82 **SHA-1 :** 01e4ceeaecd028157725fa7a08714b3ec17e67c7 **SHA-256 :** 05d6760be292258348d854279d3c3ad614b80daa2408db75bb1f304a9e62182f **SHA-512 :** 9c875ccabdf6e6e3864b69239d38c1dea819d18a00059f668e7e5c335510b6f632ce47 **Size :** 41.888 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_el.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 0659c74967bb6a994350f69b1f7ac445 **SHA-1 :** f434e21f17ea927a9e82e12a233b2fb57f7db9e7 **SHA-256 :** 1470affea411c0dc68e32fad0fb2813dba1a75d0ba194c9be5282cd0ecfcdd1e **SHA-512 :** e5ffba4b8a812c3830ec584e40da1a27f980607278ca51e061bc6bb7ca70907a8e3285 **Size :** 40.352 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ro.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f9eff614618cfdafd65c2f84c3fb65c2 **SHA-1 :** 2acefbd81f985d7a0eddbeb978af39c89fc37b5b **SHA-256 :** ba17a886191dd220aeee20f0b920aff65bdf48b8482816efe461738751ebe3a3 **SHA-512 :** 05c80d7e227b06114c4647f40a55f71c6a4cd5d8537898960549f186212f5b80cd08f64 **Size :** 39.328 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6E5336CDD9652A36A93E734B280625C5	**Type :** data **MD5 :** ed7d1dc0921d98559974f2bffea89ea7 **SHA-1 :** 72b77fd1666a4745f7c122a2b69687395f9065b4 **SHA-256 :** 527689e5ee0f4fea928b2a734ed8be05abd362c0656bea7fa351e828a367c6a5 **SHA-512 :** 0e5a0fc1b95535eba11a945b31e716869848e835667ba1486f00a55dd87e4ff936614 **Size :** 0.196 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_da.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 8742de5d2f04b69a180070e40451cdb8 **SHA-1 :** a792c5fefb8880d5917e9a02ce89e1c7cc344ba1 **SHA-256 :** 276773de4e20c1ef049eb5b727833ef7507ca683b522a6f7b5706341ee7029db **SHA-512 :** 025e18b4e79cf5680d4f5b393d49f2b4ca4a73f9fa1cc21eb4d52d5bb9b3baa2b2b4cc **Size :** 38.816 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\Linker.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 14b655f0567e2d13459a4c77b2641ad8 **SHA-1 :** 16f073c74680f4ef8b6b477e86b75d8f136824c2 **SHA-256 :** d5684110f61200ac1142648f06a4df3ee30acf38b96538496c33cac69942c4cc **SHA-512 :** f64ab83cbb87986d0356a7b9f0ebd0314d1341aecb6be627861b6a35df80d765cf851 **Size :** 8.192 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0F1583FFF42FFF476A09801ACB69213F_D4C83E2943267C1763EC8ED5C0DDE848	**Type :** data **MD5 :** b0340a4e665bbc8298a815df3fb14253 **SHA-1 :** 87f2abc9182827ef36bd6514511b3c7495a035ff **SHA-256 :** bc85cbe5009270b3c5d6779f2c470da06f855b9b6776bba522529be86e2e8cbc **SHA-512 :** 557a9f3b21bbbb2e54de6fff92aad87ff52072a90c2c6471cac00ca7a02b3fbfa0d335b **Size :** 0.358 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ko.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 9ee9eee2f917af09ac820b72e542b9e8 **SHA-1 :** 25b708ea4ccc7968bf38eb91d3face5644e119f7 **SHA-256 :** 4a1cd7215332ec2519edcf63c0cc448dab8864bead0c8cd48f74a5a173817a6f **SHA-512 :** ca24b0e0f33cd0f849433abfc023aa0249d9e060763e20f72227f2528b2873654110b9 **Size :** 34.72 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_is.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 9a86501515a7bdba4504dcfb2added82 **SHA-1 :** d671d650a6bee032525e508c4ebf823a2177cb02 **SHA-256 :** 2da7d1e07cbebbaf0d43ce08dd7eeaccd7c955b636848502a9b18db2eccf7e45 **SHA-512 :** 9936562f2dc1e282200cc629dc5688babb99eeadf93000be486a9d29555de17b70d69 **Size :** 38.816 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_fa.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 261b1c340ff13886989c66402dea5874 **SHA-1 :** ce9c0266df7efced4f70e2b7d4d6813fa45ccddd **SHA-256 :** 84162d23408988345d6b375444cd534eb83af76da414ed257c581f30c7a52df6 **SHA-512 :** 4ff5a06490ff9ec71a1d719b70df5ed80c5fb16bb4d1b13fb0fbf0107a037a897a5d5ab **Size :** 37.792 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\Modern-Wizard.Bmp	**Type :** PC bitmap, Windows 3.x format, 164 x 314 x 24 **MD5 :** 84d7d87ea6c519f48b02207ec95e9d51 **SHA-1 :** 87d62cdab00023af0f757d111050d145c3901bb2 **SHA-256 :** 8b48a0cb2498191e97ced45191f488d84349221f16d2f183422d65c99f963b53 **SHA-512 :** 08e4f3680694320dbc6a0aa8f90644ee9d6dcff3defc49101c3889e2db5c8f78fb1ebad **Size :** 154.544 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_pt-BR.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 2953bc351af8d1ada3785f454eb232a7 **SHA-1 :** d3e4f2632d4b9d7f598c4b7e8e5021852b4b53c9 **SHA-256 :** d536e6b72ef94de3a28befd50be514226bc4a78f1e8a1eea75753543b063b3e4 **SHA-512 :** 559c6f166e1a14b3e42bfadb940483b8b24c193881a885e554c4956e70039b162dc7b **Size :** 38.816 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsoA928.Tmp\InetBgDL.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 2404df50b598353f13d0638156e32698 **SHA-1 :** b11899ef2c0538ec745e01e5be94956e28e5df83 **SHA-256 :** 3a0e4473e41c0f328dfd20aa1f1e42b713a2835a79d9fbd2240a49ddb7be0c53 **SHA-512 :** 1de7903a786cd2494fa576ebb2c08c69d4227bb66d6fcfbd71c733c1e71d2da9ed8b1 **Size :** 4.608 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Psmachine.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 6c4b7f1df73e1c0314cd79e2a1df0d46 **SHA-1 :** 2f5ce62f1a796bc3bba7f517399af159a883ab29 **SHA-256 :** 27d4ae43581b4a6d536fd75c706459abdad3a84811401dc39fe1b75f1d0817d9 **SHA-512 :** b8031f980746e15de44f6c940ccd7430beb19e39bed609a03059a0b81cb4315e1499c **Size :** 184.736 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_sv.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 749624e7d76de8c8eca2b879b9969ec4 **SHA-1 :** 2db18545cd8305ab6b86235b5480b0f3a92f44ff **SHA-256 :** aeb9a2d4c0d188ca554e17a24e26812fe6b430731d4576b93de9b799e5e44fab **SHA-512 :** bec7bffca02b29aab53bf8889e5861a0cadaadcfd407828b918e0206b61ee05c22151f **Size :** 38.816 Kilobytes.
C:\Users\User\AppData\Local\Temp\MSI62890.LOG	**Type :** Little-endian UTF-16 Unicode text, with CRLF, CR line terminators **MD5 :** fd9bc51d5797b44daea178e797408878 **SHA-1 :** 5ec745f30a879ffef42b5ed64445214dd4a4cfde **SHA-256 :** 37967aef6c0421fe5cd5aa5e05f1c890bfd9ad9a09c2dff68566f63521892b32 **SHA-512 :** 0e1531a3939a700ef9507c85c4b0f6df09f0beb1c16d12cb234de64c1194c8e3012af0b **Size :** 5.74 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_hr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** eaeb7a2bbf8617f9863631da8b7c8bb3 **SHA-1 :** 8773af608e90af102f410f919435c12ccd2bcc3d **SHA-256 :** 8c8fa8db1a40b8824cb64a87865c90ff78292998400c5da4a00788240ed8072d **SHA-512 :** 20e4aca6bb4f1f1bcc06f588e2a8321853fbf3772d4237639c7c31fef86c9bc8421d995a **Size :** 39.328 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_lt.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ed2ca7f2a60a6a1734d4fa95b82fb17e **SHA-1 :** 49ed03932002725714f78dd6c9ef4239d391478b **SHA-256 :** 79b581944ed3f47017f39fa1a6f7f8b805280a7eebde0f5b3f7341a098a29519 **SHA-512 :** 159cd50e8a382518413218c19c137366d9ba34bc96717cae613fc61789779bc9ffb0f15 **Size :** 38.304 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_fi.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 82526682e53e40c788dba7a72482cd2e **SHA-1 :** 1846dc7aba2cdfa9b20d0afbdc9e7f8aa4a4cee8 **SHA-256 :** 106d3006e47ee955e8079db6708c8d4ddf89d6e7e179ef3551dc4cd693ed60ab **SHA-512 :** 68eeea926b35eb6240f74e4a9df0abdb1936e103b2d43ab4e95838a0888684c165ae5 **Size :** 38.816 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\NpSaferUpdate3.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 3dc0d95ef7470128f08ec07f5e0ff195 **SHA-1 :** 216a7741dd080c76094dcb6fc670c6a6c047de9c **SHA-256 :** f4a02b2d084927bd01a63f685fed20498dde5e1414d3cb5eb109c74be24311b6 **SHA-512 :** 05c103abaa5298d5553f14a052e7274424b6bc0a7d3626c4e9fcbcc42076c307b002a2 **Size :** 582.048 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_kn.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 2d1958896b4b0270d09b5671456fd87c **SHA-1 :** 26e5920d3f342d8bfc8769723d0a4af78ca8540e **SHA-256 :** bf05674a1bb27308599b8825ab89737cf665713fced162934b46f0971ee6148f **SHA-512 :** 4ac82171221ff732328da2584e578e07d6ef5f15969405a6c5ddf14dc71eeba75cefdfcb **Size :** 40.352 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_sk.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 7d053c8e7aa8aca684d9b11c47ae3706 **SHA-1 :** fe6fe1787673ace694f58bc762797488edf4fc78 **SHA-256 :** 900ec66005d4a1fcfde280c7fa69752ff6dd23d44bc6350860c7cf8d07886d64 **SHA-512 :** 954be57672004e67ccc5bf7c4cf978c8ab6a7b1b3a4662d8b2deaaf63079d4496acb27 **Size :** 38.816 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\DE624068503F3B953A6EC67A0654E15F_81E07CC400DF4DB0ECA725A050D525AB	**Type :** data **MD5 :** a5593d52ecb3828fd9b09e953f7fb9ef **SHA-1 :** fbc3bc338a7ba61f8d3a5ea68eee2af07e86ca04 **SHA-256 :** 2b14f82c3ab8c824507debbb0c17b26373816072c67e8d01fd59b9143a858a5e **SHA-512 :** c2fc0feb241e5dc4d502c3bcff3cfe43f49cb1e589540c6dbec4bdd8bb6287f93c384e38 **Size :** 1.415 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_et.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ec2d782a435d7a785cb5b17d2dc49a75 **SHA-1 :** 4c27a9c36517c9b8e8050f4c96b3651d2d625360 **SHA-256 :** f30418203bdb14e4b0d8d8d331782e41ec4eb55a799878dd8b71938e485c72ed **SHA-512 :** 4586d584a3ff0cd0e211dbe60d63c349e9d3e3d7d7b651a39d9f2dbe962f3f8c8c9074 **Size :** 38.304 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_ca.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 681acea6f89197e9e1dc19aa4a7daa43 **SHA-1 :** 659ea583c86a78f5348b66df1d00335301d5cdf3 **SHA-256 :** 5550cd84758ac93f0c077294a1f9aebf6931a08695f04a0e104851f8a8835707 **SHA-512 :** 758624ab1e90061683c45ffd1e68a8c65030a7d875a4f46f2f238a25d01f5c86499b072 **Size :** 39.84 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_zh-TW.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 89a630430590204a3bb83ab22db7d80d **SHA-1 :** 4fe931ca8cce3bbc66b746aa0207f242217811f8 **SHA-256 :** b94f23dc0b6f024776bce22f4c46dcc658ff07ef84f308dc328669347566ebef **SHA-512 :** fbc779a349939a9180b7ff03a528df178c66cb229b5a55f5615fa92b8bee45acab70dca **Size :** 33.184 Kilobytes.
C:\Program Files (X86)\Safer Technologies\Update\1.3.129.7\Goopdateres_mr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 48931e934ab225fe88eb5686903a6c8a **SHA-1 :** 6c1a2ad77ea5706cb044a7a2e6349a9333dc977f **SHA-256 :** 6d682c7d8066cf921634278e548a3c3a40eee6beabec97c04ca774e46bb77982 **SHA-512 :** 332fdb5c1d9f3899cb60647d830a5c5da6ec85a478208a5d359bfe02e7af664043a55b **Size :** 39.84 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	SecureBrowserSetup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	4a361773655f41788ef53d1ee189c39673f421d8
MD5:	afe7194c459fd4847b694f3abb4c2267
First Seen Date:	2016-10-12 05:34:30.520055 (5 years ago)
Number Of Clients Seen:	1
Last Analysis Date:	2016-10-12 05:34:30.520055 (5 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	5
Compilation Time Stamp	0x567F8476 [Sun Dec 27 06:25:58 2015 UTC]
LegalCopyright	Safer Technologies LLC
BuildDate	20160604
BuildVersion	3.0.1.4783
BuildTime	214510
ProductName	Secure Browser
ProductVersion	50.0.2661.205
FileDescription	Secure Browser
FileVersion	50.0.2661.205
Translation	0x0409 0x04e4
Entry Point	0x40322b (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1160144
Sha256	7466b165bd41e60c518265d8a7e049fb36891fa23d857a71cda21675bfebe25b
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x5dc5	0x5e00	6.477897	-
.rdata	0x7000	0x1212	0x1400	4.927735	-
.data	0x9000	0x1a838	0x600	4.072001	-
.ndata	0x24000	0x46000	0x0	0.000000[SUSPICIOUS]	-
.rsrc	0x6a000	0xb390	0xb400	6.568018	-

PE Imports

- KERNEL32.dll
  - Sleep
  - SetFileAttributesA
  - GetFileAttributesA
  - GetTickCount
  - GetFileSize
  - GetModuleFileNameA
  - ReadFile
  - CreateFileA
  - GetCurrentProcess
  - ExitProcess
  - SetEnvironmentVariableA
  - GetWindowsDirectoryA
  - GetTempPathA
  - GetCommandLineA
  - GetVersion
  - SetErrorMode
  - ExpandEnvironmentStringsA
  - CopyFileA
  - GetFullPathNameA
  - GlobalUnlock
  - GlobalLock
  - CreateThread
  - GetLastError
  - CreateDirectoryA
  - CreateProcessA
  - RemoveDirectoryA
  - GetTempFileNameA
  - WriteFile
  - lstrcpyA
  - MoveFileExA
  - lstrcatA
  - GetSystemDirectoryA
  - LoadLibraryA
  - GetProcAddress
  - lstrcmpiA
  - lstrcmpA
  - SetCurrentDirectoryA
  - MoveFileA
  - CompareFileTime
  - GetShortPathNameA
  - SearchPathA
  - CloseHandle
  - SetFileTime
  - GetDiskFreeSpaceA
  - lstrlenA
  - lstrcpynA
  - GlobalFree
  - FindFirstFileA
  - FindNextFileA

    - DeleteFileA
    - SetFilePointer
    - GetPrivateProfileStringA
    - FindClose
    - MultiByteToWideChar
    - MulDiv
    - WritePrivateProfileStringA
    - FreeLibrary
    - LoadLibraryExA
    - GetModuleHandleA
    - GetExitCodeProcess
    - WaitForSingleObject
    - GlobalAlloc
- USER32.dll
    - GetSystemMenu
    - SetClassLongA
    - EnableMenuItem
    - IsWindowEnabled
    - SetWindowPos
    - GetSysColor
    - GetWindowLongA
    - SetCursor
    - LoadCursorA
    - CheckDlgButton
    - GetMessagePos
    - LoadBitmapA
    - CallWindowProcA
    - IsWindowVisible
    - CloseClipboard
    - SetClipboardData
    - EmptyClipboard
    - ScreenToClient
    - GetWindowRect
    - GetDlgItem
    - CreatePopupMenu
    - GetSystemMetrics
    - SetDlgItemTextA
    - GetDlgItemTextA
    - MessageBoxIndirectA
    - CharPrevA
    - DispatchMessageA
    - PeekMessageA
    - GetDC
    - ReleaseDC
    - EnableWindow
    - InvalidateRect
    - SendMessageA
    - DefWindowProcA
    - BeginPaint
    - GetClientRect
    - FillRect
    - EndDialog
    - RegisterClassA
    - SystemParametersInfoA
    - CreateWindowExA
    - GetClassInfoA
    - DialogBoxParamA
    - CharNextA
    - ExitWindowsEx
    - LoadImageA
    - CreateDialogParamA
    - SetTimer
    - SetWindowTextA
    - SetWindowLongA
    - SetForegroundWindow
    - ShowWindow
    - IsWindow
    - SendMessageTimeoutA
    - FindWindowExA
    - OpenClipboard
    - TrackPopupMenu
    - AppendMenuA
    - DrawTextA
    - EndPaint
    - DestroyWindow
    - wsprintfA
    - PostQuitMessage
- GDI32.dll
    - SelectObject
    - SetBkMode
    - CreateFontIndirectA
    - SetTextColor
    - DeleteObject
    - GetDeviceCaps
    - CreateBrushIndirect
    - SetBkColor
- SHELL32.dll
    - SHGetSpecialFolderLocation
    - SHGetPathFromIDListA
    - SHBrowseForFolderA
    - SHGetFileInfoA
    - ShellExecuteA
    - SHFileOperationA
- ADVAPI32.dll
    - RegDeleteKeyA
    - SetFileSecurityA
    - OpenProcessToken
    - LookupPrivilegeValueA
    - AdjustTokenPrivileges
    - RegOpenKeyExA
    - RegEnumValueA
    - RegDeleteValueA
    - RegCloseKey
    - RegCreateKeyExA
    - RegSetValueExA
    - RegQueryValueExA
    - RegEnumKeyA
- COMCTL32.dll
    - ImageList_AddMasked
    - None
    - ImageList_Destroy
    - ImageList_Create
- ole32.dll

- OleUninitialize
- OleInitialize
- CoTaskMemFree
- CoCreateInstance

PE Resources

- RT_BITMAP
- RT_ICON
- RT_DIALOG
- RT_GROUP_ICON
- RT_VERSION
- RT_MANIFEST

CERTIFICATE VALIDATION

- Success ✔

[+] Safer Technologies LLC	
Status	NoError ✔
Start Date	2016-05-04 00:00:00+00:00
End Date	2018-11-03 23:59:59+00:00
Sha256	c5cdb6bacd6663a96eeac9c04895d1ea578df59bae6913256971f6b06cd8b52d
Serial	522AD06C00D636D11A6494D34695FDCF
Subject Key Identifier	ec e2 ab 18 6a 76 15 79 eb 80 30 89 cb 56 69 47 76 77 58 8e
Issuer Name	VeriSign Class 3 Code Signing 2010 CA
Issuer Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Crl link	http://sf.symcb.com/sf.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

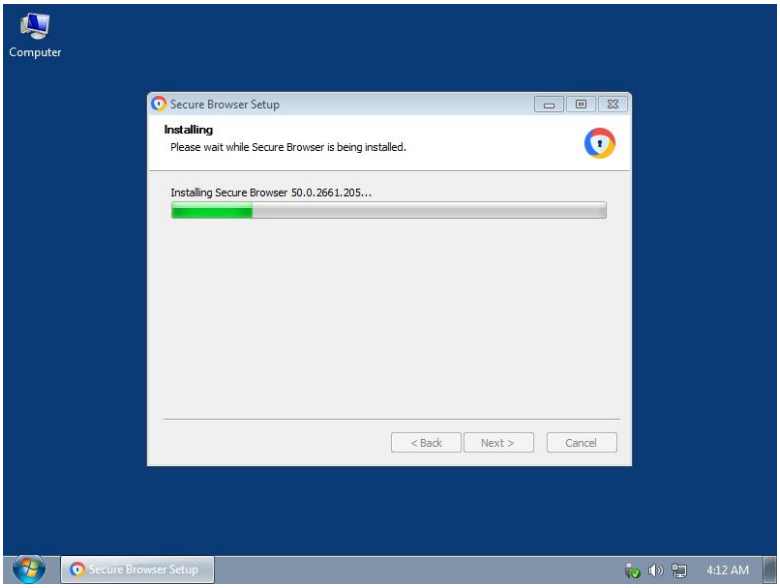
[+] VeriSign Class 3 Code Signing 2010 CA	
Status	NoError ✔
Start Date	2010-02-08 00:00:00+00:00
End Date	2020-02-07 23:59:59+00:00
Sha256	0f5cd6ebab15fa367e35893fad2bc49cd1a95449f58e7eb978d72bb0b100d764
Serial	5200E5AA2556FC1A86ED96C9D44B33C7
Subject Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Crl link	http://crl.verisign.com/pca3-g5.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

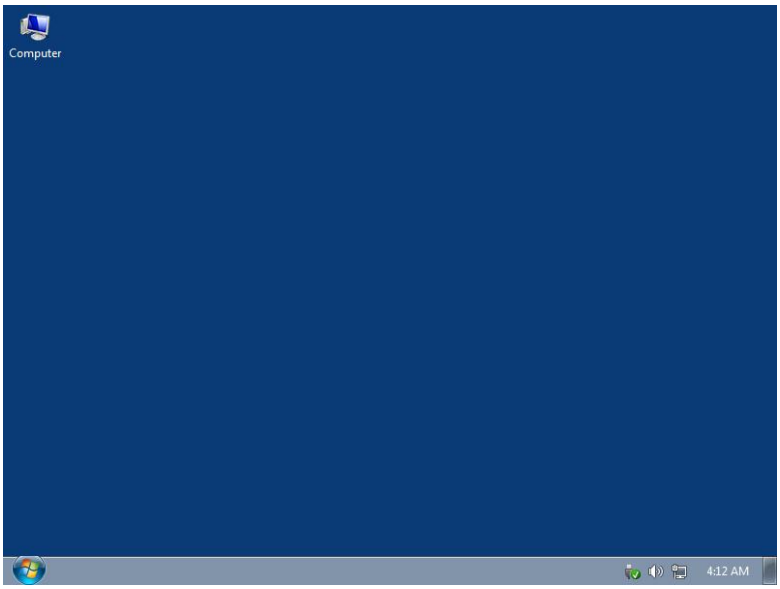
[+] VeriSign Class 3 Public Primary Certification Authority - G5	
Status	NoError ✔
Start Date	2006-11-08 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

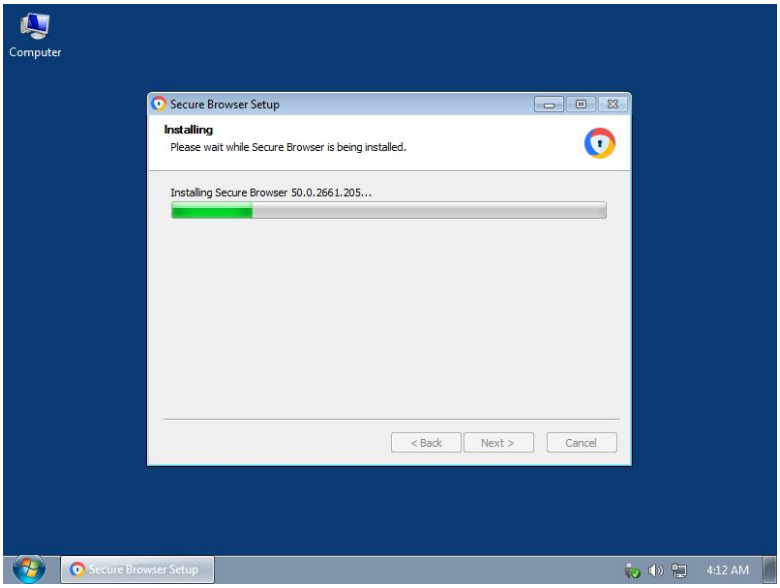
[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 00:00:00+00:00
End Date	2020-12-30 23:59:59+00:00
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

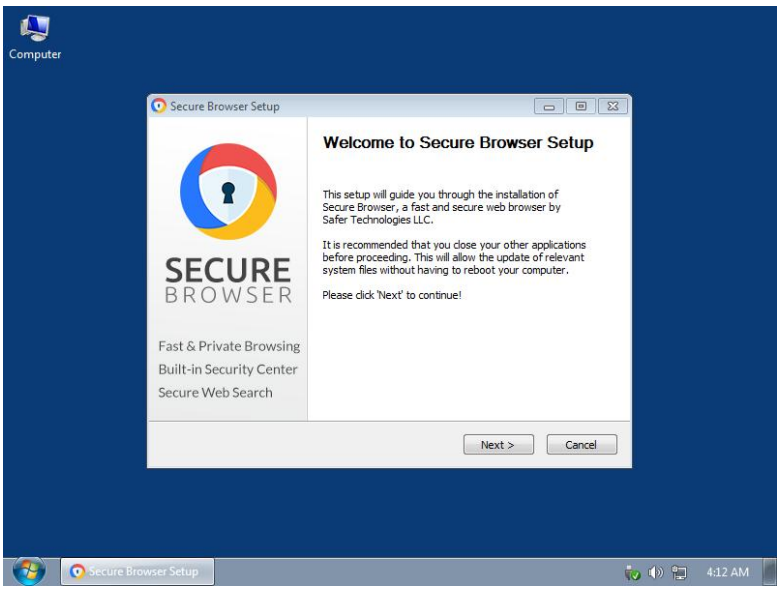
[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 00:00:00+00:00
End Date	2020-12-31 23:59:59+00:00
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	undefined
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

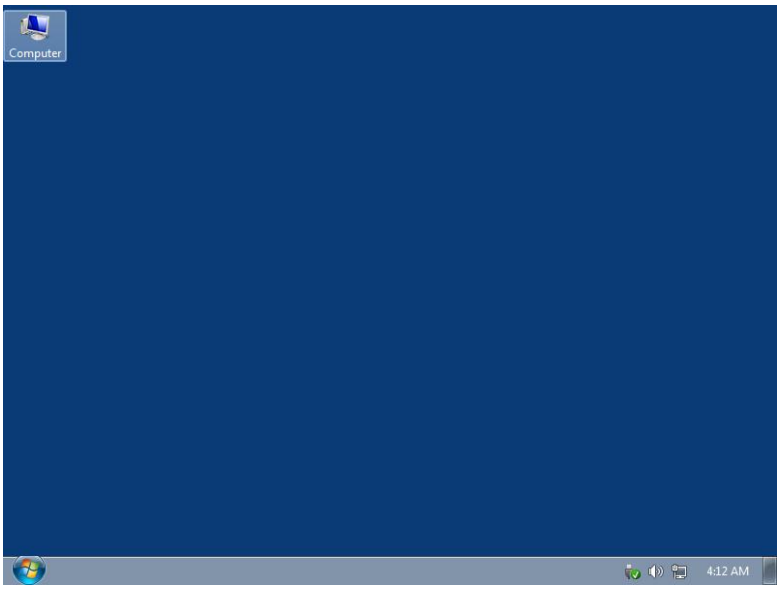
SCREENSHOTS



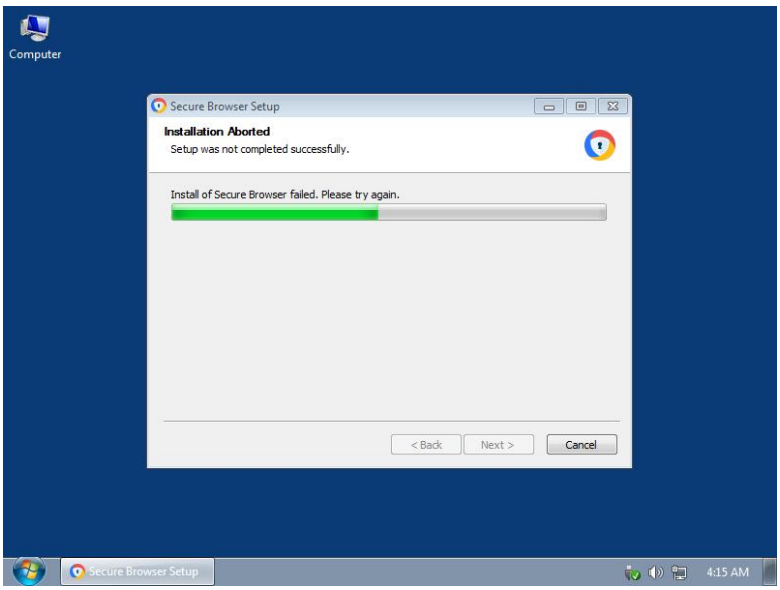

Computer
4:12 AM

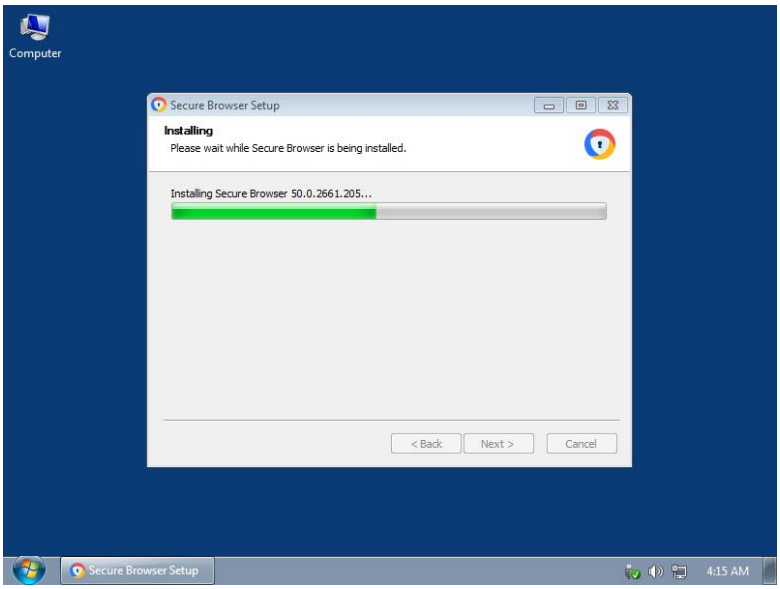

Computer
Secure Browser Setup
Installing
Please wait while Secure Browser is being installed.
Installing Secure Browser 50.0.2661.205...
< Back
Next >
Cancel
Secure Browser Setup
4:12 AM

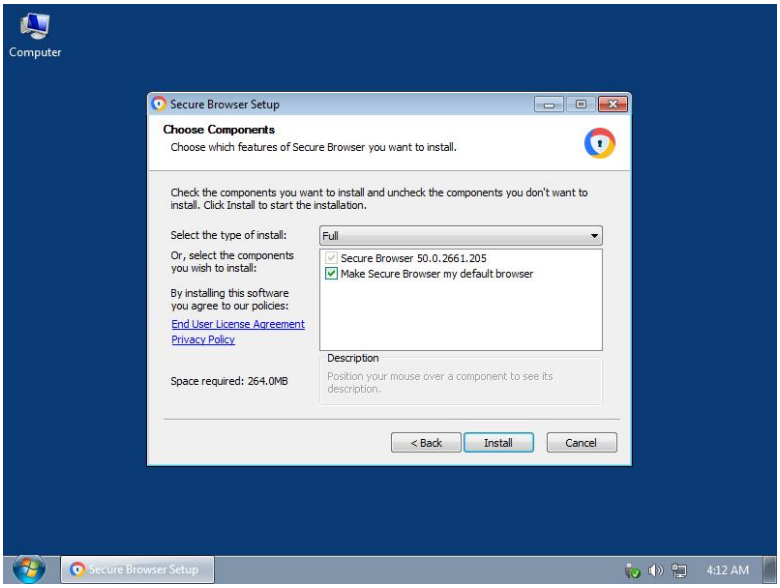

Computer
Secure Browser Setup
SECURE
BROWSER
Fast & Private Browsing
Built-in Security Center
Secure Web Search
Welcome to Secure Browser Setup
This setup will guide you through the installation of Secure Browser, a fast and secure web browser by Safer Technologies LLC.
It is recommended that you close your other applications before proceeding. This will allow the update of relevant system files without having to reboot your computer.
Please click 'Next' to continue!
Next >
Cancel
Secure Browser Setup
4:12 AM

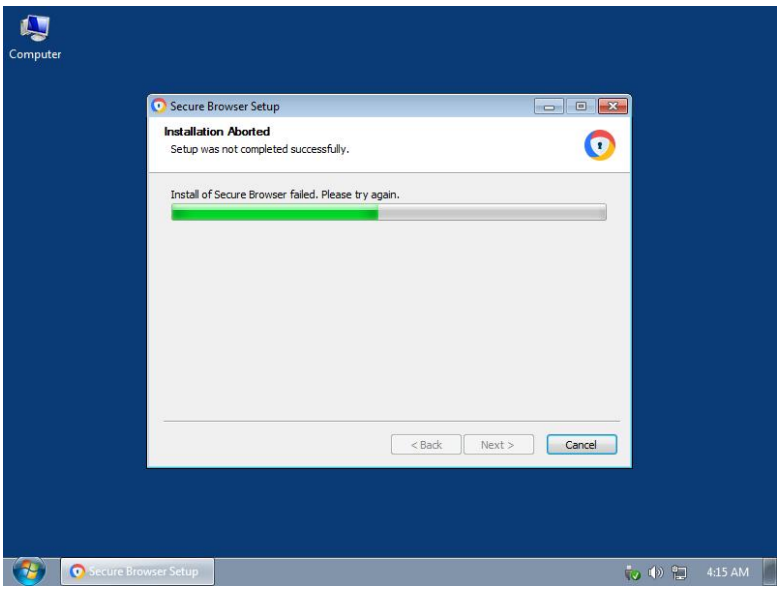

Computer
4:12 AM

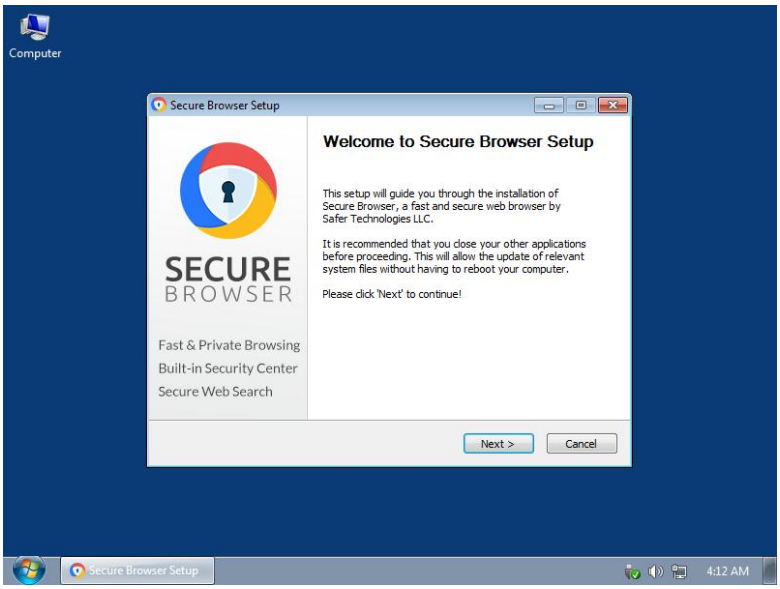

Computer
4:12 AM


Computer
Secure Browser Setup
Installation Aborted
Setup was not completed successfully.
Install of Secure Browser failed. Please try again.
< Back
Next >
Cancel
Secure Browser Setup
4:15 AM


Computer
Secure Browser Setup
Installing
Please wait while Secure Browser is being installed.
Installing Secure Browser 50.0.2661.205...
< Back
Next >
Cancel
Secure Browser Setup
4:15 AM


Computer
Secure Browser Setup
Choose Components
Choose which features of Secure Browser you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Install to start the installation.
Select the type of install:
Full
Or, select the components you wish to install:
Secure Browser 50.0.2661.205
Make Secure Browser my default browser
By installing this software you agree to our policies:
End User License Agreement
Privacy Policy
Description
Position your mouse over a component to see its description.
Space required: 264.0MB
< Back
Install
Cancel
Secure Browser Setup
4:12 AM


Computer
Secure Browser Setup
Installation Aborted
Setup was not completed successfully.
Install of Secure Browser failed. Please try again.
< Back
Next >
Cancel
Secure Browser Setup
4:15 AM


Computer
Secure Browser Setup
Welcome to Secure Browser Setup
This setup will guide you through the installation of Secure Browser, a fast and secure web browser by Safer Technologies LLC.
It is recommended that you close your other applications before proceeding. This will allow the update of relevant system files without having to reboot your computer.
Please click 'Next' to continue!
SECURE
BROWSER
Fast & Private Browsing
Built-in Security Center
Secure Web Search
Next >
Cancel
Secure Browser Setup
4:12 AM