Summary

File Name: ITParadiseSetup.exe

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

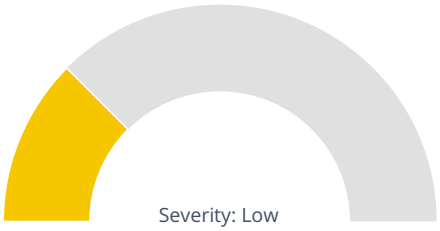
SHA1: 90bed29242832e3d7380e92e7481a73517b81328

MD5: 8440bcebd3cd7291c73c31039e46d1ed

PUA

Valkyrie Final Verdict

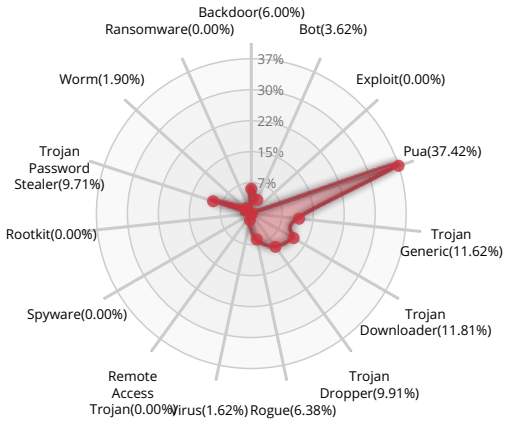
DETECTION SECTION



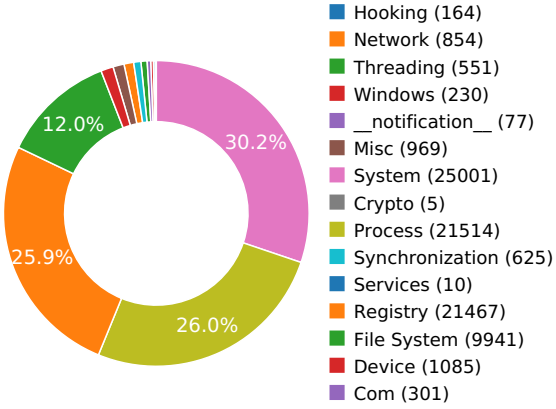
Severity: Low

Verdict: PUA

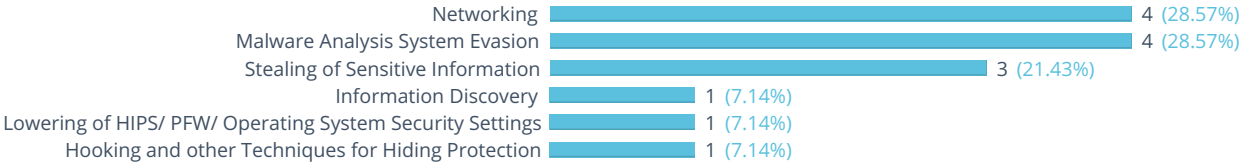
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (6 unique times)	Show sources
Starts servers listening on 127.0.0.1:0	
Performs some HTTP requests	Show sources
A process sent information about the computer to a remote location.	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

STEALING OF SENSITIVE INFORMATION

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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Checks the system manufacturer, likely for anti-virtualization	Show sources
Detects VirtualBox through the presence of a registry key	Show sources
Tries to unhook or modify Windows functions monitored by Cuckoo	Show sources
Attempts to repeatedly call a single API many times in order to delay analysis time	Show sources

Behavior Graph

01:49:34 **01:51:56** **01:54:18**

PID 2940

01:49:34 | Create Process | The malicious file created a child process as 90bed29242832e3d7380e92e7481a73517b81328.exe **(PPID 1380)**

- 01:49:34 / 01:49:34 — NtReadFile **[3 times]**
- 01:49:34 — Create Process

PID 2140

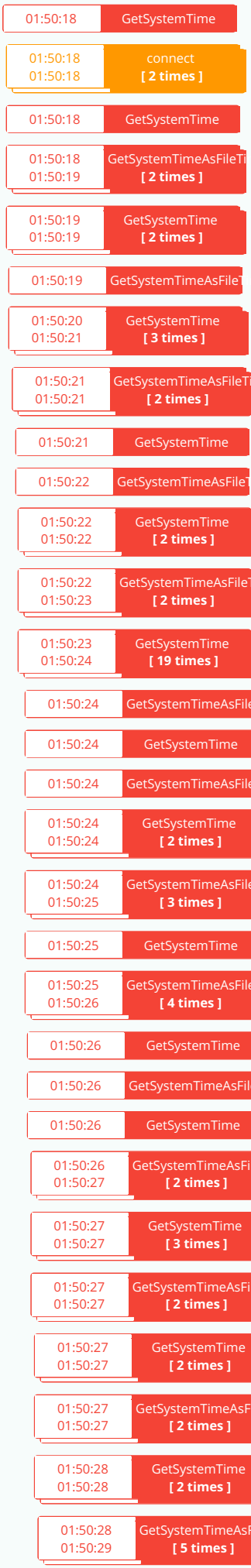
01:49:35 | Create Process | The malicious file created a child process as 90bed29242832e3d7380e92e7481a73517b81328.exe **(PPID 2940)**

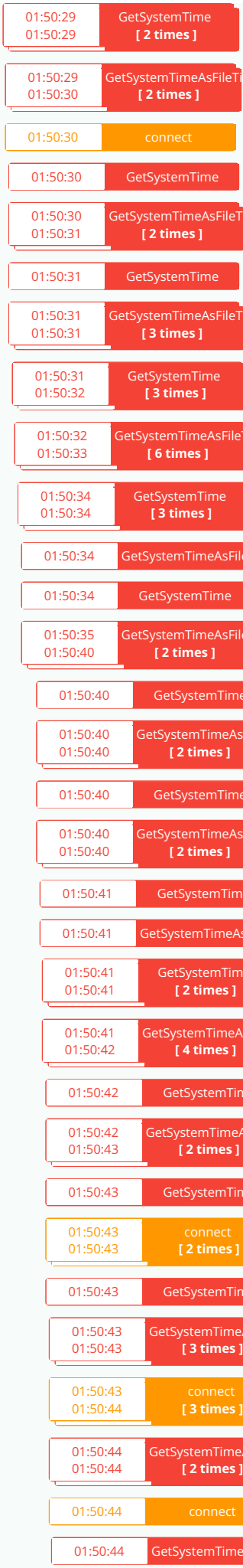
- 01:49:35 / 01:49:35 — NtReadFile **[4 times]**
- 01:49:35 — VirtualProtectEx
- 01:49:35 / 01:49:35 — NtReadFile **[2 times]**
- 01:49:48 / 01:49:56 — ConnectEx **[2 times]**
- 01:49:56 / 01:49:58 — NtReadFile **[10 times]**
- 01:49:58 / 01:49:58 — RegQueryValueExA **[2 times]**
- 01:49:58 / 01:49:59 — NtReadFile **[6 times]**
- 01:49:59 / 01:49:59 — RegQueryValueExA **[73 times]**
- 01:49:59 — RegOpenKeyExA
- 01:49:59 / 01:49:59 — RegQueryValueExA **[16 times]**
- 01:50:00 / 01:50:01 — NtReadFile **[6 times]**

PID 1200

01:50:07 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

- 01:50:08 — connect
- 01:50:08 — __anomaly__
- 01:50:09 — GetSystemTime
- 01:50:09 / 01:50:12 — GetSystemTimeAsFileTi **[15 times]**
- 01:50:12 — GetSystemTime
- 01:50:12 / 01:50:14 — GetSystemTimeAsFileTi **[7 times]**
- 01:50:15 — GetSystemTime
- 01:50:16 / 01:50:16 — GetSystemTimeAsFileTi **[4 times]**
- 01:50:16 / 01:50:17 — GetSystemTime **[4 times]**
- 01:50:18 / 01:50:18 — GetSystemTimeAsFileTi **[2 times]**


01:50:18 GetSystemTime
01:50:18 01:50:18 connect [2 times]
01:50:18 GetSystemTime
01:50:18 01:50:19 GetSystemTimeAsFileTime [2 times]
01:50:19 01:50:19 GetSystemTime [2 times]
01:50:19 GetSystemTimeAsFileTime
01:50:20 01:50:21 GetSystemTime [3 times]
01:50:21 01:50:21 GetSystemTimeAsFileTime [2 times]
01:50:21 GetSystemTime
01:50:22 GetSystemTimeAsFileTime
01:50:22 01:50:22 GetSystemTime [2 times]
01:50:22 01:50:23 GetSystemTimeAsFileTime [2 times]
01:50:23 01:50:24 GetSystemTime [19 times]
01:50:24 GetSystemTimeAsFileTime
01:50:24 GetSystemTime
01:50:24 GetSystemTimeAsFileTime
01:50:24 01:50:24 GetSystemTime [2 times]
01:50:24 01:50:25 GetSystemTimeAsFileTime [3 times]
01:50:25 GetSystemTime
01:50:25 01:50:26 GetSystemTimeAsFileTime [4 times]
01:50:26 GetSystemTime
01:50:26 GetSystemTimeAsFileTime
01:50:26 GetSystemTime
01:50:26 01:50:27 GetSystemTimeAsFileTime [2 times]
01:50:27 01:50:27 GetSystemTime [3 times]
01:50:27 01:50:27 GetSystemTimeAsFileTime [2 times]
01:50:27 01:50:27 GetSystemTime [2 times]
01:50:27 01:50:27 GetSystemTimeAsFileTime [2 times]
01:50:28 01:50:28 GetSystemTime [2 times]
01:50:28 01:50:29 GetSystemTimeAsFileTime [5 times]


01:50:29 01:50:29 GetSystemTime [2 times]
01:50:29 01:50:30 GetSystemTimeAsFileTi [2 times]
01:50:30 connect
01:50:30 GetSystemTime
01:50:30 01:50:31 GetSystemTimeAsFileTi [2 times]
01:50:31 GetSystemTime
01:50:31 01:50:31 GetSystemTimeAsFileTi [3 times]
01:50:31 01:50:32 GetSystemTime [3 times]
01:50:32 01:50:33 GetSystemTimeAsFileTi [6 times]
01:50:34 01:50:34 GetSystemTime [3 times]
01:50:34 GetSystemTimeAsFileTi
01:50:34 GetSystemTime
01:50:35 01:50:40 GetSystemTimeAsFileTi [2 times]
01:50:40 GetSystemTime
01:50:40 01:50:40 GetSystemTimeAsFileTi [2 times]
01:50:40 GetSystemTime
01:50:40 01:50:40 GetSystemTimeAsFileTi [2 times]
01:50:41 GetSystemTime
01:50:41 GetSystemTimeAsFileTi
01:50:41 01:50:41 GetSystemTime [2 times]
01:50:41 01:50:42 GetSystemTimeAsFileTi [4 times]
01:50:42 GetSystemTime
01:50:42 01:50:43 GetSystemTimeAsFileTi [2 times]
01:50:43 GetSystemTime
01:50:43 01:50:43 connect [2 times]
01:50:43 GetSystemTime
01:50:43 01:50:43 GetSystemTimeAsFileTi [3 times]
01:50:43 01:50:44 connect [3 times]
01:50:44 01:50:44 GetSystemTimeAsFileTi [2 times]
01:50:44 connect
01:50:44 GetSystemTimeAsFileTi

01:50:44 connect

01:50:45 GetSystemTimeAsFileTi
01:50:45 [4 times]

PID 1216

01:50:11 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:50:12 __anomaly__

PID 1332

01:50:18 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

PID 1136

01:50:22 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:50:23 __anomaly__

PID 1152

01:50:26 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:50:27 __anomaly__

PID 1632

01:50:32 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:50:33 __anomaly__

PID 1540

01:50:36 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:50:37 __anomaly__

PID 1752

01:50:41 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:50:42 __anomaly__

PID 2780

01:50:55 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:50:56 __anomaly__

PID 2992

01:50:58 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:50:59 __anomaly__

PID 2980

01:51:01 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:02 __anomaly__

PID 2712

01:51:04 Create Process The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:04 __anomaly__

PID 2088

01:51:06 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:07 __anomaly__

PID 2480

01:51:09 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:10 __anomaly__

PID 1640

01:51:11 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:12 __anomaly__

PID 1392

01:51:15 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:16 __anomaly__

PID 2004

01:51:17 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

PID 1744

01:51:21 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:23 __anomaly__

PID 1000

01:51:27 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:29 __anomaly__

PID 2984

01:51:32 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:34 __anomaly__

PID 2252

01:51:36 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:39 __anomaly__

PID 1528

01:51:41 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:44 __anomaly__

PID 196

01:51:46 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:48 __anomaly__

PID 2448

01:51:53 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:51:56 __anomaly__

PID 3028

01:51:59 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:52:02 __anomaly__

PID 1576

01:52:07 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:52:09 __anomaly__

PID 2528

01:52:14 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:52:17 __anomaly__

PID 1196

01:52:21 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:52:23 __anomaly__

PID 1964

01:52:29 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:52:32 __anomaly__

PID 1116

01:52:38 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:52:41 __anomaly__

PID 2452

01:52:47 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:52:50 __anomaly__

PID 2824

01:53:04 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:53:08 __anomaly__

PID 2972

01:53:16 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:53:18 __anomaly__

PID 2968

01:53:23 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:53:25 __anomaly__

PID 2192

01:53:30 **Create Process** The malicious file created a child process as firefox.exe **(PPID 2140)**

01:53:32 __anomaly__

PID 1932

01:53:37 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:53:39 | __anomaly__

PID 1464

01:53:43 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:53:45 | __anomaly__

PID 2008

01:53:52 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:53:53 | __anomaly__

PID 1816

01:53:59 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:54:01 | __anomaly__

PID 2616

01:54:04 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

01:54:07 | __anomaly__

PID 960

01:54:13 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

PID 932

01:54:18 | Create Process | The malicious file created a child process as firefox.exe **(PPID 2140)**

PID 584

01:50:39 | Create Process | The malicious file created a child process as svchost.exe **(PPID 460)**

PID 2076

01:50:48 | Create Process | The malicious file created a child process as svchost.exe **(PPID 460)**

01:50:54 | RegOpenKeyExW

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nsk29C0.tmp
C:\Users\user\AppData\Local\Temp\90bed29242832e3d7380e92e7481a73517b81328.exe
C:\Users\user\AppData\Local\Temp\nsl2C31.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Banner.dll
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\nsr2D8B.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\inetc.dll
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\6BADA8974A10C4BD62CC921D13E43B18_2BD85C712A72CD147177B036ACBEE38C
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_2BD85C712A72CD147177B036ACBEE38C
C:\Users\user\AppData\Local\Temp\1.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuA.dll

C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuX.dll
C:\Users\user\AppData\Local\Temp\21.txt
C:\Users\user\AppData\Local\Temp\33.txt
C:\Users\user\AppData\Local\Temp\nsc82EF.tmp
C:\Users\user\AppData\Local\Temp\2.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Dialogs.dll
C:\Windows\System32\drivers*.*
\??\VBoxMiniRdrDN
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\1.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\registry.dll
C:\Users\user\AppData\Local\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuZ.dll
C:\Users\user\AppData\Local\Temp\nsb891A.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\2.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\md5dll.dll
C:\Users\user\AppData\Roaming_Setup_NUCDZ\.exe
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\100.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\101.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Image.bmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\LCLogo.bmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\accept.ico
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\decline.ico
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\BrowserSafer.ico
C:\Users\user\AppData\Local\Temp\Image.bmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\nsDialogs.dll
C:\Program Files (x86)\Mozilla Firefox\mozglue.dll
C:\Program Files (x86)\Mozilla Firefox\VERSION.dll
C:\Windows\System32\version.dll
C:\Program Files (x86)\Mozilla Firefox\msvcr120.dll
C:\Program Files (x86)\Mozilla Firefox\msvcp120.dll
C:\Program Files (x86)\Mozilla Firefox\xul.dll
C:\Program Files (x86)\Mozilla Firefox\dependentlibs.list
C:\Program Files (x86)\Mozilla Firefox\nss3.dll
C:\Program Files (x86)\Mozilla Firefox\WINMM.dll

C:\Windows\System32\winmm.dll
C:\Program Files (x86)\Mozilla Firefox\WSOCK32.dll
C:\Windows\System32\wsock32.dll
C:\Program Files (x86)\Mozilla Firefox\sandboxbroker.dll
C:\Program Files (x86)\Mozilla Firefox\lgpllibs.dll
C:\Program Files (x86)\Mozilla Firefox\icuin56.dll
C:\Program Files (x86)\Mozilla Firefox\icuuc56.dll
C:\Program Files (x86)\Mozilla Firefox\icudt56.dll
C:\Program Files (x86)\Mozilla Firefox\NETAPI32.dll

READ REGISTRY KEYS

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\Microsoft\Rpc\Extensions\NdrOleExtDLL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\System.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\Banner.dll
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
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\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\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\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\inetc.dll
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\90bed29242832e3d7380e92e7481a73517b81328_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASAPI32\EnableConsoleTracing

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASMANCS\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASMANCS\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASMANCS\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASMANCS\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_RASMANCS\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\90bed29242832e3d7380e92e7481a73517b81328_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_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Banner.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\inetc.dll
C:\Users\user\AppData\Local\Temp\nsr2D8B.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\6BADA8974A10C4BD62CC921D13E43B18_2BD85C712A72CD147177B036ACBEE38C
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_2BD85C712A72CD147177B036ACBEE38C
C:\Users\user\AppData\Local\Temp\1.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuA.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuX.dll
C:\Users\user\AppData\Local\Temp\21.txt
C:\Users\user\AppData\Local\Temp\33.txt

C:\Users\user\AppData\Local\Temp\nsc82EF.tmp
C:\Users\user\AppData\Local\Temp\2.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Dialogs.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\1.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\registry.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuZ.dll
C:\Users\user\AppData\Local\Temp\nsb891A.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\2.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\md5dll.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\100.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\101.txt
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Image.bmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\LCLogo.bmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\accept.ico
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\decline.ico
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\BrowserSafer.ico
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\nsDialogs.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\parent.lock
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.tmp
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cert8.db
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\key3.db
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\doomed\18678
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\permissions.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\content-prefs.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs.js
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs-1.js
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-shm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps.json
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps-1.json
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\9BBE93EE66A24A6574E0B0B292F1184CC816B4A0
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\formhistory.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\SiteSecurityServiceState.txt
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-shm
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\B1BF484310B181937E88AFC02D2B2F23B1FBCC38
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\1A7DB7AFBC4999A68D319D571CBFD9F0A0E3523C
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\4A055E0BDA8A10AC24EB026B701A2ABD6000E397
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\mimeTypes.rdf
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR

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
ole32.dll.CoRevokeInitializeSpy
comctl32.dll.#388

ole32.dll.NdrOleInitializeExtension

ole32.dll.CoGetClassObject

ole32.dll.CoGetMarshalSizeMax

ole32.dll.CoMarshalInterface

ole32.dll.CoUnmarshalInterface

ole32.dll.StringFromIID

ole32.dll.CoGetPSClsid

ole32.dll.CoTaskMemAlloc

ole32.dll.CoTaskMemFree

ole32.dll.CoCreateInstance

ole32.dll.CoReleaseMarshalData

ole32.dll.DcomChannelSetHResult

oleaut32.dll.#500

advapi32.dll.UnregisterTraceGuids

comctl32.dll.#321

shell32.dll.#680

system.dll.Call

kernel32.dll.CreateMutexA

banner.dll.show

dwmapi.dll.DwmIsCompositionEnabled

comctl32.dll.RegisterClassNameW

uxtheme.dll.EnableThemeDialogTexture

ole32.dll.CoInitializeEx

ole32.dll.CoUninitialize

ole32.dll.CoRegisterInitializeSpy

gdi32.dll.GetLayout

gdi32.dll.GdiRealizationInfo

gdi32.dll.FontIsLinked

advapi32.dll.RegOpenKeyExW

advapi32.dll.RegQueryInfoKeyW

gdi32.dll.GetTextFaceAliasW

advapi32.dll.RegEnumValueW

advapi32.dll.RegCloseKey

advapi32.dll.RegQueryValueExW

gdi32.dll.GetFontAssocStatus

advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC
ole32.dll.CoCreateGuid
inetc.dll.get
uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeInt
wininet.dll.FtpCommandA
rasapi32.dll.RasConnectionNotificationW
sechost.dll.NotifyServiceStatusChangeA
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
oleaut32.dll.#8
oleaut32.dll.#9
oleaut32.dll.DllGetClassObject
oleaut32.dll.DllCanUnloadNow
advapi32.dll.RegOpenKeyW
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

DELETED FILES

C:\Users\user\AppData\Local\Temp\nsk29C0.tmp
C:\Users\user\AppData\Local\Temp\nsl2C31.tmp

C:\Users\user\AppData\Local\Temp\nsb2C90.tmp
C:\Users\user\AppData\Local\Temp\nsr2D8B.tmp
C:\Users\user\AppData\Local\Temp\nsc82EF.tmp
C:\Users\user\AppData\Local\Temp\nsb891A.tmp
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.log
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.tmp
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\doomed\18678
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs-1.js
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps-1.json
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index
C:\Users\user\AppData\Local\Temp\mozilla-temp-files
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\B1BF484310B181937E88AFC02D2B2F23B1FBCC38
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-wal
C:\Users\user\AppData\Local\Mozilla\updates\E7CF176E110C211B\update.test
C:\Program Files (x86)\Mozilla Firefox\update.test
C:\Program Files (x86)\update.test

DELETED REGISTRY KEYS

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

REGISTRY KEYS

HKEY_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\Rpc\Extensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\System.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\Banner.dll
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\90bed29242832e3d7380e92e7481a73517b81328.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Shell Dlg 2
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\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\inetc.dll
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)

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\90bed29242832e3d7380e92e7481a73517b81328.exe" /start=1 /path=
https://applicationloft.com/redirect.php?id=29

READ FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\nsk29C0.tmp
C:\Users\user\AppData\Local\Temp\90bed29242832e3d7380e92e7481a73517b81328.exe
C:\Users\user\AppData\Local\Temp\nsl2C31.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Banner.dll
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\nsr2D8B.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.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\6BADA8974A10C4BD62CC921D13E43B18_2BD85C712A72CD147177B036ACBEE38C
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_2BD85C712A72CD147177B036ACBEE38C
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuA.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuX.dll
C:\Users\user\AppData\Local\Temp\nsc82EF.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Dialogs.dll
\??\VBoxMiniRdrDN
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\registry.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\zuzuZ.dll
C:\Users\user\AppData\Local\Temp\nsb891A.tmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\md5dll.dll
C:\Users\user\AppData\Roaming_Setup_NUCDZ\.exe
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\Image.bmp
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\nsDialogs.dll
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\accept.ico
C:\Users\user\AppData\Local\Temp\nsb2C90.tmp\decline.ico
C:\Program Files (x86)\Mozilla Firefox\mozglue.dll

C:\Windows\System32\version.dll
C:\Program Files (x86)\Mozilla Firefox\msvcr120.dll
C:\Program Files (x86)\Mozilla Firefox\msvcp120.dll
C:\Program Files (x86)\Mozilla Firefox\dependentlibs.list
C:\Program Files (x86)\Mozilla Firefox\nss3.dll
C:\Windows\System32\winmm.dll
C:\Windows\System32\wsock32.dll
C:\Program Files (x86)\Mozilla Firefox\sandboxbroker.dll
C:\Program Files (x86)\Mozilla Firefox\lgpllibs.dll
C:\Program Files (x86)\Mozilla Firefox\xul.dll
C:\Program Files (x86)\Mozilla Firefox\icuin56.dll
C:\Program Files (x86)\Mozilla Firefox\icuuc56.dll
C:\Program Files (x86)\Mozilla Firefox\icudt56.dll
C:\Windows\System32\netapi32.dll
C:\Windows\System32\netutils.dll
C:\Windows\System32\srvcli.dll
C:\Windows\System32\msimg32.dll
C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\wtsapi32.dll
C:\Windows\System32\pdh.dll
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Crash Reports\InstallTime20160502172042
C:\Users\user\AppData\Local\Mozilla\updates\E7CF176E110C211B\updates\0\update.status
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\parent.lock

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\compatibility.ini
C:\Program Files (x86)\Mozilla Firefox\omni.ja
C:\Program Files (x86)\Mozilla Firefox\browser\omni.ja
C:\Windows\System32\tzres.dll
C:\Program Files (x86)\Mozilla Firefox\chrome.manifest
C:\Program Files (x86)\Mozilla Firefox\defaults\pref\channel-prefs.js
C:\Program Files (x86)\Mozilla Firefox\browser\chrome.manifest
C:\Program Files (x86)\Mozilla Firefox\browser\components\components.manifest
C:\Program Files (x86)\Mozilla Firefox\browser\components\browsercomps.dll
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\startupCache\startupCache.4.little
C:\Windows\System32\wship6.dll

MUTEXES

vortex_module
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
IESQMMUTEX_0_208
Local\FirefoxStartupMutex
Local\MSCTF.Asm.MutexDefault1
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
Local\WininetStartupMutex
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex
Global\MozillaUpdateMutex-AWkbzLFmEHPmIFtactC8kpT7UdM=

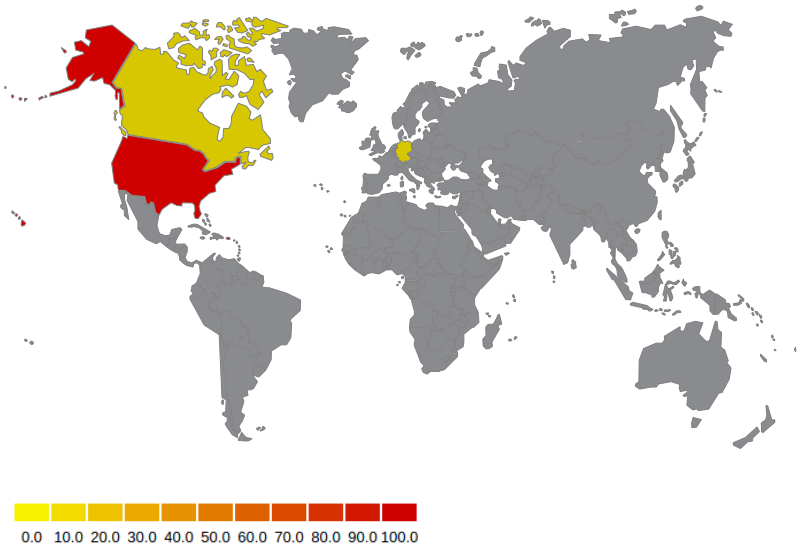
MODIFIED REGISTRY KEYS

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

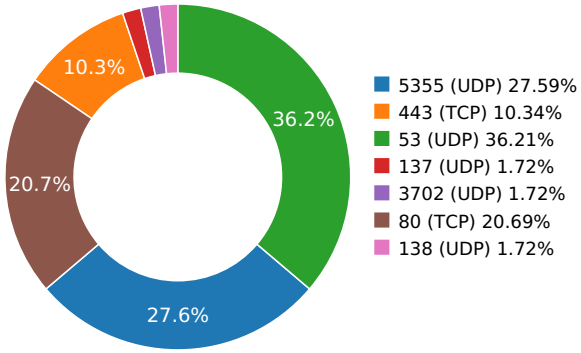
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider

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
	104.18.61.210	United States	13335	Cloudflare, Inc.	Malware Process
	104.28.17.56	United States	13335	Cloudflare, Inc.	Malware Process
	184.26.44.98	United States	20940	Akamai Technologies, Inc.	OS Process
	54.243.250.185	United States	14618	Amazon Technologies Inc.	Malware Process
	69.195.158.198	United States	19969	Joe's Datacenter, LLC	Malware Process
	192.241.99.194	Canada	55286	B2 Net Solutions Inc.	Malware Process
	69.195.158.197		19969	Joe's Datacenter, LLC	Malware Process
	178.255.83.1		35838		OS Process
	107.21.103.188		14618	Amazon.com, Inc.	Malware Process
	184.26.44.105		20940	Akamai Technologies, Inc.	Malware Process
	184.26.44.97		20940	Akamai Technologies, Inc.	OS Process
	178.255.83.1		35838		OS Process
	23.215.99.85		20940	Akamai Technologies, Inc.	OS Process
	94.130.73.107		24940		Malware Process
	72.21.91.29		15133	MCI Communications Services, Inc. ...	Malware Process
	104.28.16.56		13335	Cloudflare, Inc.	Malware Process
	85.10.210.166		24940		Malware Process
	184.26.44.105		20940	Akamai Technologies, Inc.	Malware Process
	104.18.60.210		13335	Cloudflare, Inc.	Malware Process

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	19.6296670437
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9a64d7e59c4e4d02 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9a64d7e59c4e4d02						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6...	1	27.399533987
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAYN1sHQZ5AbVHX8%2F8KeMTc%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAYN1sHQZ5AbVHX8%2F8KeMTc%3D						
stp-1014845532.us-east-1.elb.amazonaws.com	80	GET	1.1	NSIS_Inetc (Mozilla)	1	31.2993881702
Path: /p.gif?rs=i&h=&av=&aver=&osver=6.1&ossp=1&err=0&64=1&adm=1&quant=1360569703 **URI:** http://stp-1014845532.us-east-1.elb.amazonaws.com/p.gif?rs=i&h=&av=&aver=&osver=6.1&ossp=1&err=0&64=1&adm=1&quant=1360569703						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6...	1	68.0047609806
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	74.1735210419
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	79.597561121
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	86.1752231121
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
applicationloft.com	A
Answers - 104.18.61.210 (A) - 104.18.60.210 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 184.26.44.105 (A) - a1621.g.akamai.net (CNAME) - 184.26.44.97 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	

Request	Type
stp-1014845532.us-east-1.elb.amazonaws.com	A
Answers - 107.21.103.188 (A) - 54.243.250.185 (A)	
notification.adblockplus.org	A
Answers - 136.243.58.99 (A) - 78.46.39.215 (A) - 88.99.186.149 (A) - 144.76.20.58 (A) - 88.99.186.151 (A) - 88.99.186.150 (A) - easylist-downloads.adblockplus.org (CNAME) - 5.9.15.86 (A) - 144.76.219.20 (A) - 178.63.70.146 (A) - 94.130.73.107 (A) - 46.4.115.44 (A) - 94.130.73.103 (A)	
easylist-downloads.adblockplus.org	A
Answers - 176.9.146.200 (A) - 94.130.73.101 (A) - 176.9.116.83 (A) - 94.130.73.112 (A) - 176.9.127.15 (A) - 176.9.139.5 (A) - 94.130.73.106 (A) - 88.99.186.158 (A) - 144.76.137.234 (A)	
easylist-downloads.adblockplus.org	AAAA
Answers - 2a01:4f8:140:30e7::2 (AAAA) - 2a01:4f8:141:132c::2 (AAAA) - 2a01:4f8:192:7126::2 (AAAA) - 2a01:4f8:c0c:2d12::2 (AAAA)	
ocsp.comodoca.com	A
Answers - 178.255.83.1 (A)	
ocsp.usertrust.com	A
ocsp.comodoca.com	AAAA
Answers - 2a02:1788:2fd::b2ff:5301 (AAAA)	
ocsp.usertrust.com	AAAA
secure.informaction.com	A
Answers - 69.195.158.196 (A) - 69.195.158.198 (A) - 69.195.158.195 (A) - 69.195.158.197 (A) - 69.195.158.194 (A)	

Request	Type
secure.information.com	AAAA
crl.microsoft.com	A
Answers - 184.26.44.98 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
ocsp.int-x3.letsencrypt.org	A
Answers - a771.dscq.akamai.net (CNAME) - 184.26.44.103 (A) - ocsp.int-x3.letsencrypt.org.edgesuite.net (CNAME)	
a771.dscq.akamai.net	A
a771.dscq.akamai.net	AAAA
Answers - 2600:140a::48f6:2b38 (AAAA) - 2600:140a::48f6:2b2b (AAAA)	
crl.globalsign.net	A
Answers - 104.28.16.56 (A) - 104.28.17.56 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
10.8826069832	Sandbox	104.18.61.210	443
19.6296670437	Sandbox	184.26.44.105	80
27.399533987	Sandbox	72.21.91.29	80
27.6443769932	Sandbox	104.18.61.210	443
28.051156044	Sandbox	104.18.61.210	443
28.4417750835	Sandbox	104.18.61.210	443
31.2993881702	Sandbox	54.243.250.185	80
44.8992869854	Sandbox	5.9.15.86	443
56.14935112	Sandbox	69.195.158.198	443
68.0047609806	Sandbox	184.26.44.98	80
86.1752231121	Sandbox	104.28.17.56	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.1400270462	Sandbox	224.0.0.252	5355
3.17139315605	Sandbox	192.168.56.255	137
3.17231416702	Sandbox	224.0.0.252	5355
3.17777609825	Sandbox	239.255.255.250	3702
5.73581314087	Sandbox	224.0.0.252	5355
6.85425114632	Sandbox	192.168.56.255	138
8.00993013382	Sandbox	224.0.0.252	5355
10.8133120537	Sandbox	8.8.4.4	53
13.8684341908	Sandbox	224.0.0.252	5355
16.8072052002	Sandbox	224.0.0.252	5355
19.524408102	Sandbox	8.8.4.4	53
21.6655991077	Sandbox	224.0.0.252	5355
24.5722100735	Sandbox	224.0.0.252	5355
27.3536100388	Sandbox	8.8.4.4	53
31.2441170216	Sandbox	8.8.4.4	53
44.3145031929	Sandbox	8.8.4.4	53
44.6404030323	Sandbox	8.8.4.4	53
44.664317131	Sandbox	8.8.4.4	53
53.9238860607	Sandbox	8.8.4.4	53
53.9638631344	Sandbox	8.8.4.4	53
54.1275141239	Sandbox	8.8.4.4	53
54.1662931442	Sandbox	8.8.4.4	53
54.1665291786	Sandbox	8.8.4.4	53
54.1771211624	Sandbox	8.8.4.4	53
56.0805470943	Sandbox	8.8.4.4	53
56.1064400673	Sandbox	8.8.4.4	53
56.1317050457	Sandbox	8.8.4.4	53
62.2213420868	Sandbox	224.0.0.252	5355
65.0214681625	Sandbox	224.0.0.252	5355
67.8990960121	Sandbox	8.8.4.4	53
68.8296320438	Sandbox	8.8.4.4	53
68.8607289791	Sandbox	224.0.0.252	5355
68.9721951485	Sandbox	8.8.4.4	53
69.0568900108	Sandbox	8.8.4.4	53
71.4799070358	Sandbox	224.0.0.252	5355
74.2059230804	Sandbox	224.0.0.252	5355
76.9593970776	Sandbox	224.0.0.252	5355

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
79.9207391739	Sandbox	224.0.0.252	5355
83.4357681274	Sandbox	224.0.0.252	5355
86.1303670406	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Nsb891A.Tmp	**Type :** ASCII text **MD5 :** fb781e417cc981ff04d99b608b47dded **SHA-1 :** d4f447cbcb3d77e0e6cae07d5d9979a4d80ed3c8 **SHA-256 :** ff182e05770300c31b26d3df40d2c18a6b737c1d **SHA-512 :** e2713531d42e30e65638ec77ed56c8272ccdaf3a **Size :** 0.004 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\SiteSecurityServiceState.Txt	**Type :** ASCII text, with very long lines **MD5 :** c1825ea7e0da3dda742088ff409d838f **SHA-1 :** 782d531c00e02bbff434b90757ea8cee4fec7ec9 **SHA-256 :** 89e2f76ae1473406ce26e05e7eaaaba8c012dd7d **SHA-512 :** 5e1c917268dc1c3b1ee6fae4aa50ecaedc097a48 **Size :** 2.031 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsr2D8B.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** c301b37b105e83d8546e8e2590155920 **SHA-1 :** 7e40acc60cbfb228afec36fda02782b764d54ffc **SHA-256 :** affb37600428c55bf7eac14a1495a6601647960b3 **SHA-512 :** 401986cbe7baedc9bec3a836bd57b04c6a03d2b **Size :** 0.012 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\Accept.Ico	**Type :** MS Windows icon resource - 1 icon **MD5 :** c1f703873120bb852a901b6313bbad9c **SHA-1 :** 0a7aece67aae45706a570364da635ef8f0fa2a12 **SHA-256 :** 6f2a7202a5e4addb1d1bd6dc1704bd2ee14df22 **SHA-512 :** 784c648a5e2aa39f67e8cd8088059f31a62bfb15f **Size :** 7.517 Kilobytes.
C:\Users\User\AppData\Local\Temp\33.Txt	**Type :** ASCII text **MD5 :** b026324c6904b2a9cb4b88d6d61c81d1 **SHA-1 :** e5fa44f2b31c1fb553b6021e7360d07d5d91ff5e **SHA-256 :** 4355a46b19d348dc2f57c046f8ef63d4538ebb93 **SHA-512 :** 3abb6677af34ac57c0ca5828fd94f9d886c26ce59 **Size :** 0.002 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Storage\Permanent\Chrome\Idb\2918063365piupsah.Sqlite-Shm **C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Storage\Permanent\Moz-Safe-About+Home\Idb\818200132aebmoouht.Sqlite-Shm** **C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cookies.Sqlite-Shm**	**Type :** FoxPro FPT, blocks size 0, next free block index 417475840 **MD5 :** b7c14ec6110fa820ca6b65f5aec85911 **SHA-1 :** 608eeb7488042453c9ca40f7e1398fc1a270f3f4 **SHA-256 :** fd4c9fda9cd3f9ae7c962b0ddf37232294d55580e **SHA-512 :** d8d75760f29b1e27ac9430bc4f4ffcec39f1590be5 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\Registry.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 074c4e15702afffc703c87b0cb908d8d **SHA-1 :** 1cd91235dd43d9a651a27d4adeed1acbb51cf508 **SHA-256 :** a5951e09fa08899bf69f54056300a01b829fe454c **SHA-512 :** e63b8d82dbe7fa08c4417cb532e3a3338e458f9e **Size :** 30.72 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 5dadef7d3eb5bdd27c797712446af7b5 **SHA-1 :** 378d68d5b5d20b0ea8313f7bee28373c0fe1dce3 **SHA-256 :** 6f6ab60f78f5326b9fa4af75c969150aa6558e178 **SHA-512 :** b0502a25dc04c80ed5fa2100b2ae41e51eab3df3 **Size :** 0.34 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\Decline.Ico	**Type :** MS Windows icon resource - 1 icon **MD5 :** cd0b9e311c64a733c0f833733202291f **SHA-1 :** cf11f7bcd22029abd02c42e8c82ceaa2014ba865 **SHA-256 :** 447a3dd925c7c0c7409851fec40f21fae941bebcc **SHA-512 :** 38b99873ca041f5e5d02a3dab6be6faa2cee818f **Size :** 7.517 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\ZuzuX.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f95a8d78fb0053cd92f7c84bdc81b364 **SHA-1 :** 7838176962690a9bd953f3235d27eba5a2b1f8c2 **SHA-256 :** 0bae5c7a796b64f54193b877eab8566b5f8172d9 **SHA-512 :** 04746d37d2ee16872c5b5c8c3973003d3fd7a11b **Size :** 94.208 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Places.Sqlite	**Type :** SQLite 3.x database, user version 30 **MD5 :** 10006bf944b0f6794e00081599ee704c **SHA-1 :** 673372edb267448f645492cc5f67b315cfc451f4 **SHA-256 :** a43864fc9195a9a34ffea5f43c6101f7a591eb939(**SHA-512 :** fb168db35a2f660de021b8e3a1f9297ee5b11fc54 **Size :** 10485.76 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Prefs.Js	**Type :** UTF-8 Unicode text, with very long lines, with CRLF line terminators **MD5 :** d4c0da88c346cacf21326c3a03798fca **SHA-1 :** 4556249b1697cd99b183968dc4c38b2732ad81b4 **SHA-256 :** 755fad95675fadb725a7c9f976f42b7d6908775f8 **SHA-512 :** 35d728a3cb530cccec23f925f49e0ed1d0f9729a1 **Size :** 17.264 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\System.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 56a321bd011112ec5d8a32b2f6fd3231 **SHA-1 :** df20e3a35a1636de64df5290ae5e4e7572447f78 **SHA-256 :** bb6df93369b498eaa638b0bcdc4bb89f45e9b02c **SHA-512 :** 5354890cbc53ce51081a78c64ba9c4c8c4dc9e01 **Size :** 10.752 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\Image.Bmp	**Type :** PC bitmap, Windows 3.x format, 497 x 57 x 24 **MD5 :** 61e818d46cfe7a6c1ad90b3a02b98331 **SHA-1 :** 5611d6e10ddfaa2d8ef8f8015af7fd524794de61 **SHA-256 :** c82ff117c6325a2530a226c0c91109395c52e895c **SHA-512 :** 50fe09f3803d173ba06ef4d9377051dd2b57df57 **Size :** 85.098 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\Banner.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** a748a0a7a7eb56ad356cce710968a380 **SHA-1 :** a8cd1e978a4b481f410fc5205ca5a29cdb2c22e7 **SHA-256 :** 33409ceab861b0164a9ec3a0395934cade72e2ef **SHA-512 :** 05433019dc827399b00195461fcc58f287d53b34 **Size :** 4.096 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\101.Txt	**Type :** very short file (no magic) **MD5 :** c4ca4238a0b923820dcc509a6f75849b **SHA-1 :** 356a192b7913b04c54574d18c28d46e6395428ab **SHA-256 :** 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa2 **SHA-512 :** 4dff4ea340f0a823f15d3f4f01ab62eae0e5da579(**Size :** 0.001 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\LCLogo.Bmp	**Type :** PC bitmap, Windows 3.x format, 497 x 89 x 24 **MD5 :** 52c9f2dca89278be05cfc6eb704a4784 **SHA-1 :** 4e831880919ff82486908cc32f28ea74a3744ef0 **SHA-256 :** c653e53c33d85bf31de8b85c177a4ba341f0d91b **SHA-512 :** fc3ac366f10214084d8c5a5b1fc5d4ac905eb0399 **Size :** 132.842 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsc82EF.Tmp	**Type :** ASCII text **MD5 :** 0176ddafc8f0e88ab67ea8ed00060c7b **SHA-1 :** 8cf0b0dbd594e1e77d176c34608012953497a217 **SHA-256 :** 9bab0916810ecae3c0bb224ce1d1e413393821e **SHA-512 :** 140c3826fbdc5336846665f6633755cc704a025fb **Size :** 0.045 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Entries\1A7DB7AFBC4999A68D319D571CBFD9F0A0E3523C	**Type :** data **MD5 :** 9f1ec06f0a99cf348ba296b12a1ec0ff **SHA-1 :** 573165d219124cf00240ecfb3b84d33130f6dd40 **SHA-256 :** 182949d556b54922ea76b6bf1298b44dc0eb895 **SHA-512 :** 1a16e5928de483aeb621d9bd5ef1a0e1bece1d8 **Size :** 0.064 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Webapps\Webapps.Json	**Type :** ASCII text, with no line terminators **MD5 :** 99914b932bd37a50b983c5e7c90ae93b **SHA-1 :** bf21a9e8fbc5a3846fb05b4fa0859e0917b2202f **SHA-256 :** 44136fa355b3678a1146ad16f7e8649e94fb4fc21 **SHA-512 :** 27c74670adb75075fad058d5ceaf7b20c4e7786c **Size :** 0.002 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\Inetc.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** e541458cfe66ef95ffbea40eaaa07289 **SHA-1 :** caec1233f841ee72004231a3027b13cdeb13274c **SHA-256 :** 3bce87b66d9272c82421920c34b0216e12c57a4 **SHA-512 :** 0bf6313e4cb7bbdcfba828fb791540b630adc58c **Size :** 20.992 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\Dialogs.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 5793c42d934ee6965496b7275aa9fcf4 **SHA-1 :** 772c1eaf7378a61fe9a99982b4a14de79c19a7eb **SHA-256 :** 40af7d6b9ad40b937c1453d6b674ca895b6c47d **SHA-512 :** 796dba0a5e30d5ab70efd1ea3e7e0d48b373c07 **Size :** 82.432 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Index	**Type :** data **MD5 :** d0c8b9bf63fcdf68301b52fc554c4044 **SHA-1 :** 030caf7a3b1b72c11d6016d4b13d103252936c5c **SHA-256 :** 0964f33019fe5bff5730b817fb618b0a788e3d873 **SHA-512 :** 7a7f4e625b708ad0f2f8e9a9218ffe59c67c86c97c **Size :** 9.484 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\100.Txt	**Type :** GIF image data, version 89a, 1 x 1 **MD5 :** 57f187c7a868faeac558007a8eb6cb2e **SHA-1 :** 11ab10ab109fdb53d91d444ac781101f5a6360c6 **SHA-256 :** aa03dc59bdca72631d2301e4297cfa030bd31b9 **SHA-512 :** 3844065e1dd778a05e8cc39901fbf3191ded380d **Size :** 0.043 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Entries\B1BF484310B181937E88AFC02D2B2F23B1FBCC38	**Type :** data **MD5 :** a46360d2ff9e4136337f1a91fb60b6f4 **SHA-1 :** cacd04d95321abff22dce55768b73661b41ae6be **SHA-256 :** c424a6cdd98a3b5358ba42d58d1e4b6fefe4a264 **SHA-512 :** 51794eda6fdd22987459053bf263ec656d5972cf **Size :** 2.269 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\ZuzuA.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** feb2b09bc873208875818c184696f398 **SHA-1 :** e69e346114c5655559245326fb0eb1585ad0026c **SHA-256 :** 11cd5ae80a5882d253d55e60bb20f3b059f0cdba **SHA-512 :** c6a1734d003870d0963c8665b8a20efeca1ccee0 **Size :** 78.848 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Entries\9BBE93EE66A24A6574E0B0B292F1184CC816B4A0	**Type :** data **MD5 :** 7c67d581022356137af6375a2fc298b8 **SHA-1 :** 9b7648cef4d9db813735914b5bf3b80b7c63821d **SHA-256 :** da45bb6caa541ab5fd84eab45398e2e1f5e8f93f1 **SHA-512 :** 593df53cfd66b618a534ae319b0872731770bc9d **Size :** 0.265 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Places.Sqlite-Wal	**Type :** data **MD5 :** ba540645eb83d0d1f6fe23746a18a793 **SHA-1 :** 89073e233e968b358148c7722ca4bd6b68bb8571 **SHA-256 :** 8912981183afccdc2d953565995f096838c39423 **SHA-512 :** bc102ae901002237fcf26b7fb1bcd69895831055 **Size :** 32.824 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Index	**Type :** data **MD5 :** 5759064c3510519bddd7be7d28b0f97c **SHA-1 :** 876a2531dc24196c342fc1f6ed08d45dd8287c7c **SHA-256 :** 7fd86697e202fe0e78e80d40a3ca8b3af7a0d328 **SHA-512 :** b440311d385bedd08c1e069c05a22a210714806 **Size :** 1.564 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Places.Sqlite-Shm	**Type :** data **MD5 :** d7cb0ca4046846ed305fac5e9d4bd0e5 **SHA-1 :** 7dfb750a667bf9f533093068d10c64cff4b65355 **SHA-256 :** e7580f4fd78cd775d59894185708c337af4e9770 **SHA-512 :** e8c545836521f529b9eb3057be5a3ace20530df7 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_2BD85C712A72CD147177B036ACBEE38C	**Type :** data **MD5 :** 72cdf75c9ebba63bbef87f8e56364115 **SHA-1 :** cbc2583da1b3c5dd6849138a24dc45e19155505f **SHA-256 :** aa91114401c2612ec95236ce8648949745a7ccf4 **SHA-512 :** ae4b837653817d1a5d947e9280ab7d7b5fe62ca **Size :** 0.438 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\ZuzuZ.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** dfab2504ccbb1cf76bec6a9b9e96412d **SHA-1 :** 1bff48d8759df9dc2bf03d7f81ad477a8bc758d5 **SHA-256 :** b5fab2ab80317bd7b7f79d0ba418ea5b8f668db9 **SHA-512 :** b25d3ea1b95de7a0d93d7d00fcab391625b3f57c **Size :** 106.496 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\1.Txt **C:\Users\User\AppData\Local\Temp\21.Txt** **C:\Users\User\AppData\Local\Temp\2.Txt** **C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\1.Txt** **C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\2.Txt**	**Type :** ASCII text, with CRLF line terminators **MD5 :** a5ea0ad9260b1550a14cc58d2c39b03d **SHA-1 :** f0aedf295071ed34ab8c6a7692223d22b6a19841 **SHA-256 :** f1b2f662800122bed0ff255693df89c4487fbdcf45 **SHA-512 :** 7c735c613ece191801114785c1ee26a0485cbf1e **Size :** 0.003 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_2BD85C712A72CD147177B036ACBEE38C	**Type :** data **MD5 :** 714f8f2b92bf8c26756aa7606d04dad7 **SHA-1 :** e758e5dc4c1a5c184083040e2114d1be76855644 **SHA-256 :** c0ae28d01d88302c0247c138bc21a70e5bb5977(**SHA-512 :** 0da294bf3de46522524c2745bb3d79610bb54d4 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6564 bytes, 1 file **MD5 :** 16e8e953c65d610c3bfc595240f3f5b7 **SHA-1 :** 231a802e6ff1fae42f2b12561fff2767d473210b **SHA-256 :** 048846ed8ed185a26394adeb3f63274d1029bbd **SHA-512 :** 8cf223f68cd118be6bef746d4ccef2bc293e7e0f44 **Size :** 6.564 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Entries\4A055E0BDA8A10AC24EB026B701A2ABD6000E397	**Type :** data **MD5 :** fa3915cbca54b6f25c42a01205e9273f **SHA-1 :** de8e0df3626eb9d3e8b5dd856e961d269f0f67da **SHA-256 :** 363933f2e5994f483e1409162b555c60aa4dfcc5c **SHA-512 :** e60e72dfd3864a46e21d2d281095b9a0ea6d936 **Size :** 0.106 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\BrowserSafer.Ico	**Type :** MS Windows icon resource - 1 icon **MD5 :** 45b463e558b8039f6ef16a5a0ce6c227 **SHA-1 :** ecb32d3fb8698c84573d09bf82599d80fdaa1b23 **SHA-256 :** 0c627acc71f114815033668a026be66342011b1c **SHA-512 :** d2b5d19e4bfbc3db1926fe2f73e7df2ae4b2f5db1 **Size :** 4.286 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\NsDialogs.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f832e4279c8ff9029b94027803e10e1b **SHA-1 :** 134ff09f9c70999da35e73f57b70522dc817e681 **SHA-256 :** 4cd17f660560934a001fc8e6fdcea50383b78ca12 **SHA-512 :** bf92b61aa267e3935f0ea7f47d8d96f09f016e648 **Size :** 9.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsb2C90.Tmp\Md5dll.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 0745ff646f5af1f1cdd784c06f40fce9 **SHA-1 :** bf7eba06020d7154ce4e35f696bec6e6c966287f **SHA-256 :** fbed2f1160469f42ce97c33ad558201b2b43e302(**SHA-512 :** 8d31627c719e788b5d0f5f34d4cb175989eaa35a **Size :** 6.656 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cert8.Db	**Type :** Berkeley DB 1.85 (Hash, version 2, native byte-order) **MD5 :** 7965d09542e2ab093fcc707451c6f5b5 **SHA-1 :** 33c551cfcbfd5a75ab4a3518e30503d520973c81 **SHA-256 :** 78173b57c2269495264db6b96c3397dca31bca7(**SHA-512 :** 22b02e96ac16cac9fd8eeca2caf0ddf0736d3e6b3 **Size :** 163.84 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	ITParadiseSetup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	90bed29242832e3d7380e92e7481a73517b81328
MD5:	8440bcebd3cd7291c73c31039e46d1ed
First Seen Date:	2017-07-30 08:09:43.149183 (about a year ago)
Number Of Clients Seen:	1
Last Analysis Date:	2017-07-30 08:09:43.149183 (about a year 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
File Type Enum	6
Number Of Sections	5
Compilation Time Stamp	0x56FF3A6D [Sat Apr 2 03:20:13 2016 UTC]
Entry Point	0x40312a (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	417120
Sha256	68e5806f66288d40e077f68eccd0b5e3d721fa61e0a66cca199f07a657df353a
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x5e66	0x6000	6.44065573436	d22b359417726295d1d61eaac63c3d95
.rdata	0x7000	0x12a2	0x1400	5.0583287871	68295528d67e59e0536c9d80519cbe96
.data	0x9000	0x25d18	0x600	4.18773476617	82232fd09381275af53acb18fd24a88b
.ndata	0x2f000	0x34000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x63000	0x42e8	0x4400	4.15549974929	7f044a3e27d53464c1ea2cf31fa79378

CERTIFICATE VALIDATION

- Success ✔

[+] App Science Corporation	
Status	NoError ✔
Start Date	2017-05-01 00:00:00+00:00
End Date	2018-05-01 23:59:59+00:00
Sha256	b8b0c4a7d5e49b3cfd4cf4dfac16ef1fdd62c21dbdf3e06f3ecf69b428fed71a
Serial	79157880A2B969AE0C2271E7D7442075
Subject Key Identifier	15 d5 d8 93 da 22 4d 81 1b 20 6d 33 de 00 b0 f1 5e 95 5b 09
Issuer Name	thawte SHA256 Code Signing CA
Issuer Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Crl link	http://tl.symcb.com/tl.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

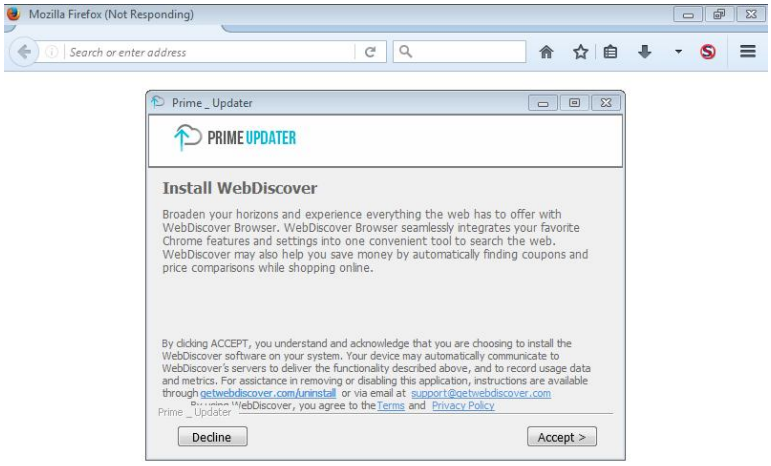
[+] thawte SHA256 Code Signing CA	
Status	NoError ✔
Start Date	2013-12-10 00:00:00+00:00
End Date	2023-12-09 23:59:59+00:00
Sha256	d542ad03871f39ed7a47a057892a67f6d76b973134a8a129d2ba1ace821de2e4
Serial	71A0B73695DDB1AFC23B2B9A18EE54CB
Subject Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Crl link	http://t1.symcb.com/ThawtePCA.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)

[+] thawte Primary Root CA	
Status	NoError ✔
Start Date	2006-11-17 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d6a37f73bd37d7adacb96997064639215d4806b63a4ccee5416e3da8d68a3b1f
Serial	344ED55720D5EDEC49F42FCE37DB2B6D
Subject Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Issuer Name	thawte Primary Root CA
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


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >

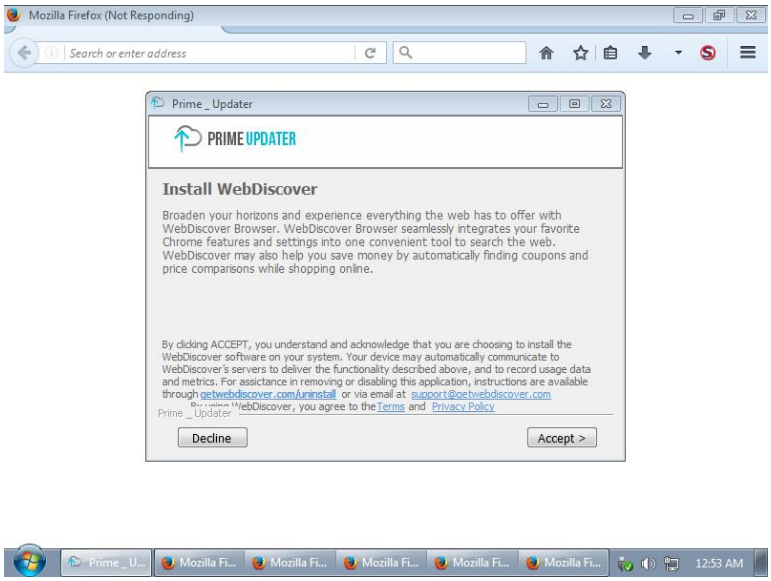

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:53 AM


Mozilla Firefox (Not Responding)
Search or enter address

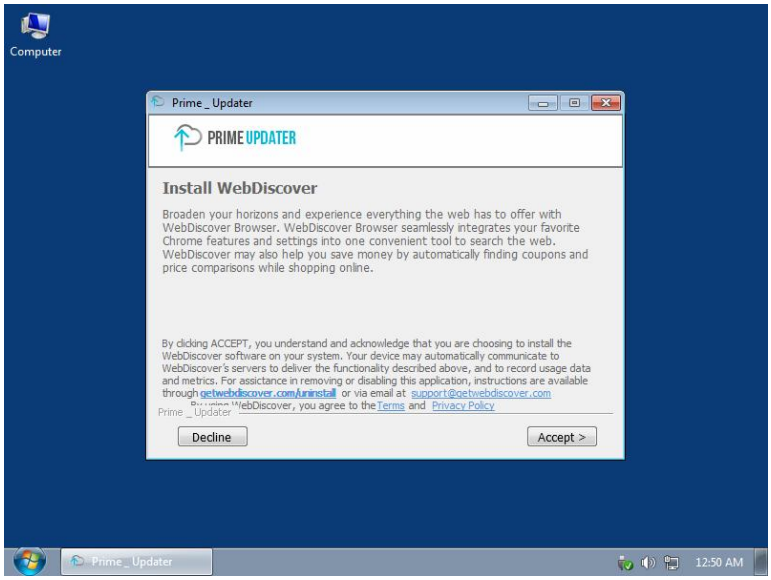

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:51 AM


Mozilla Firefox (Not Responding)
Search or enter address


Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:53 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:53 AM

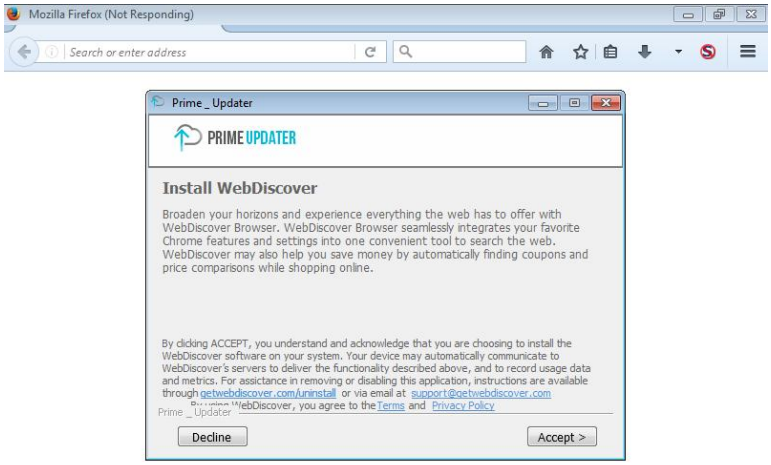

Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
Prime _ Updater
12:50 AM


Mozilla Firefox (Not Responding)
Search or enter address

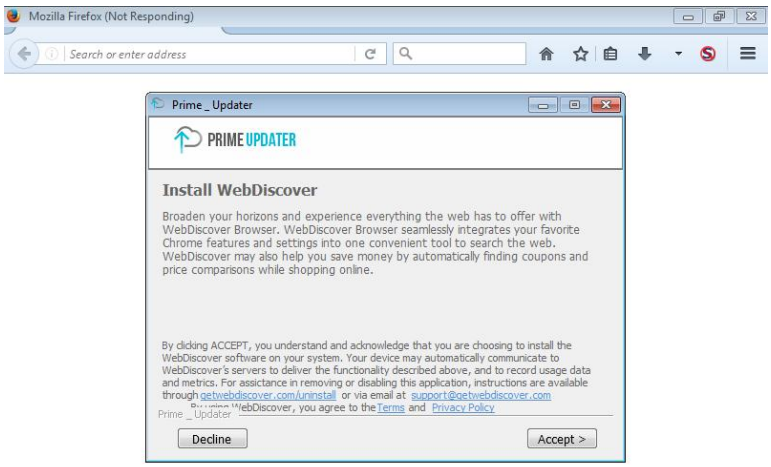

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:53 AM


Mozilla Firefox (Not Responding)
Search or enter address

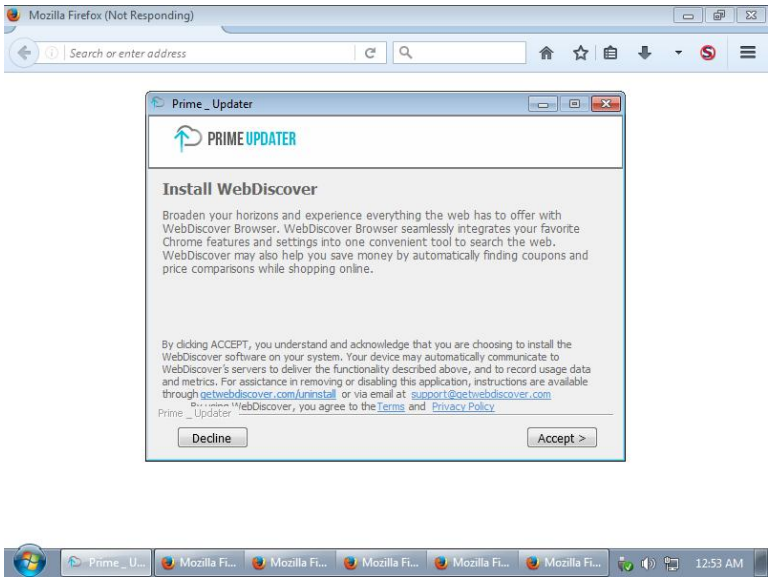

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:52 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >


Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:51 AM

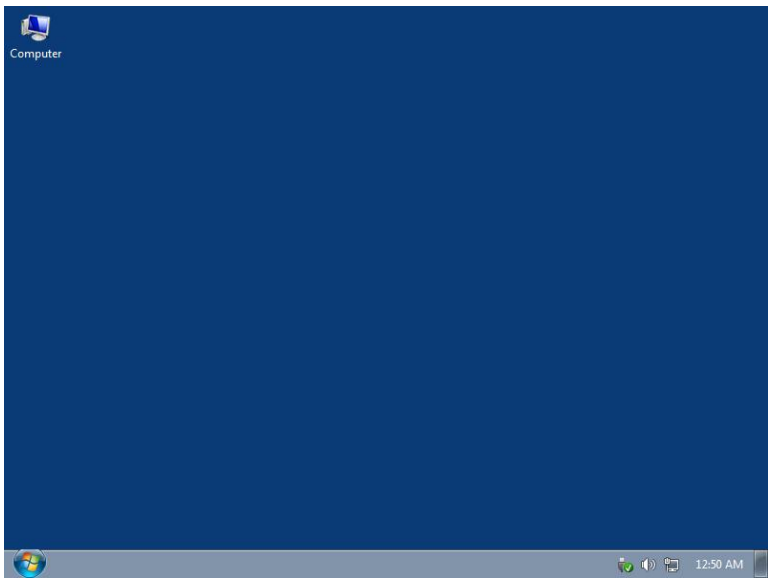

Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >

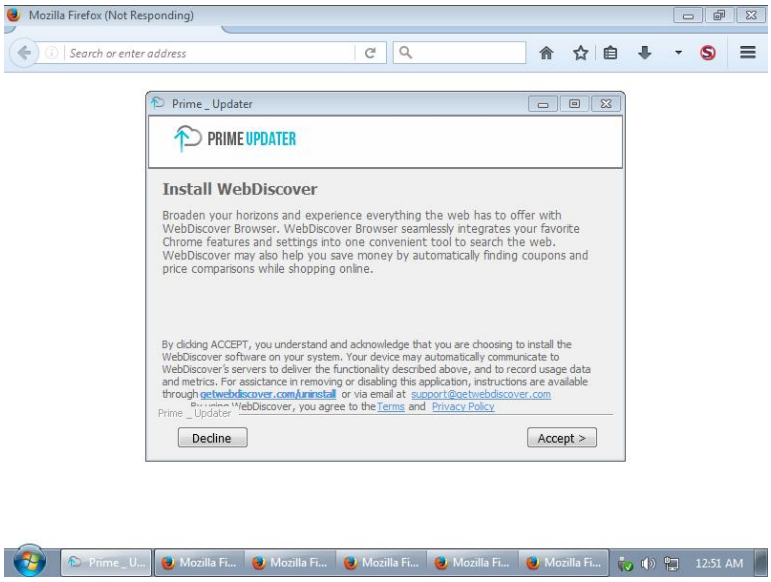

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:51 AM

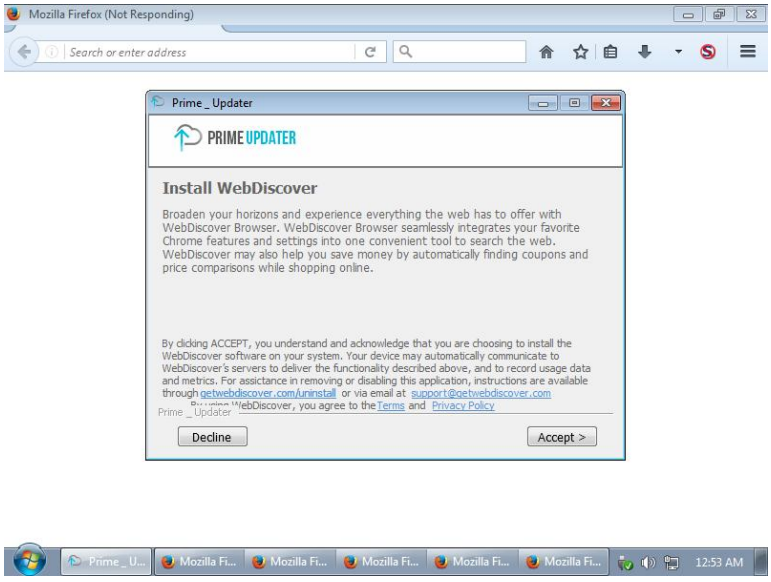

Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >
Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:53 AM


New Tab
Search or enter address


Prime _ Updater
Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
12:50 AM

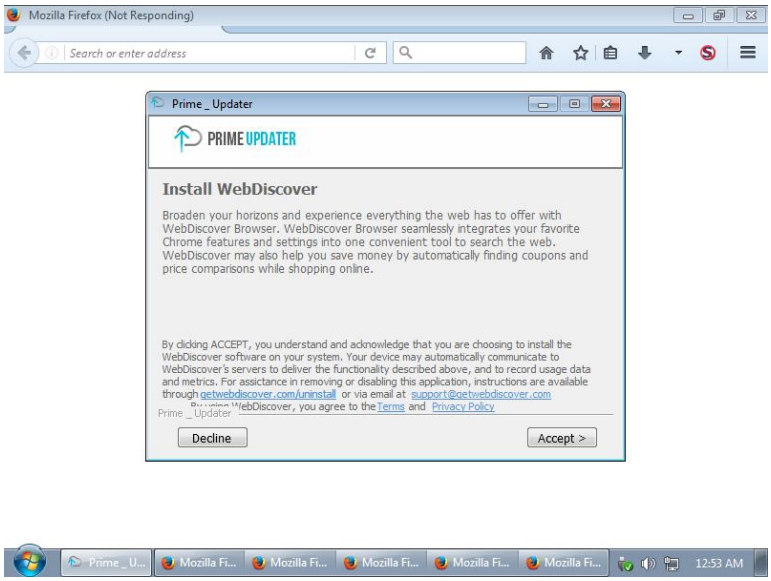

Computer
12:50 AM

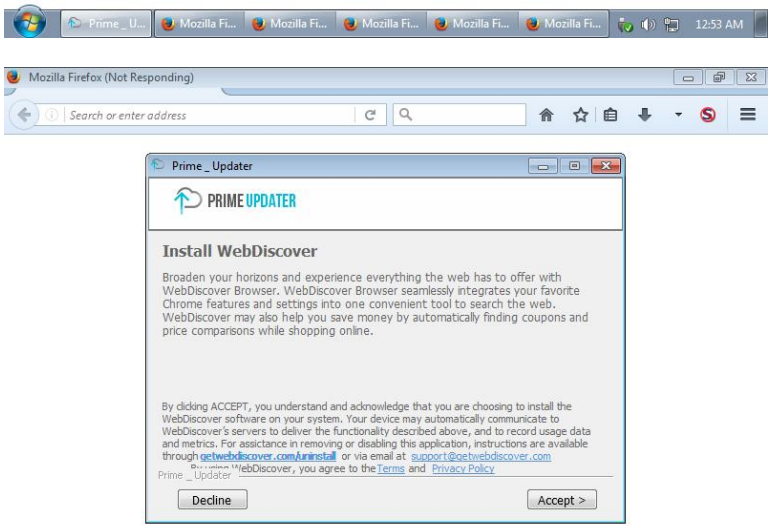

Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >
Prime _ U...
Mozilla Fi...
12:51 AM

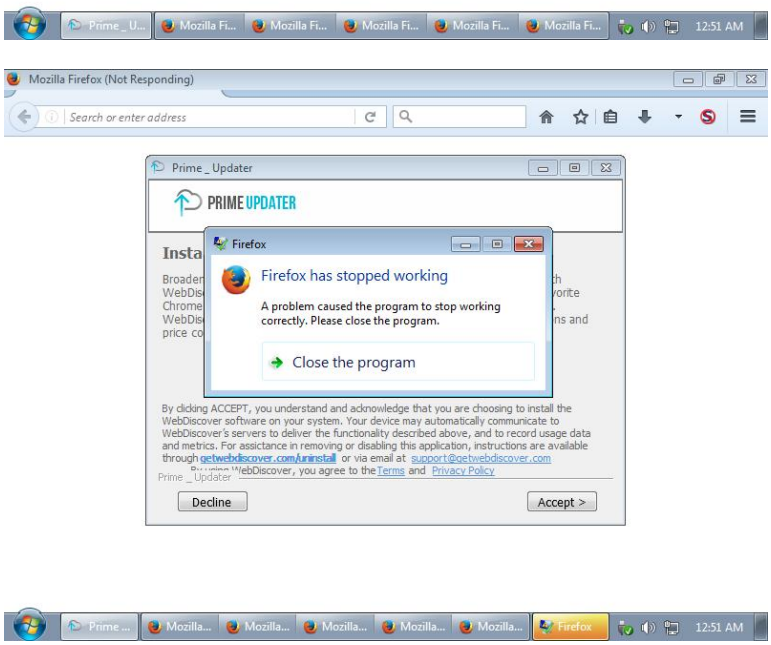

Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >
Prime _ U...
Mozilla Fi...
12:53 AM

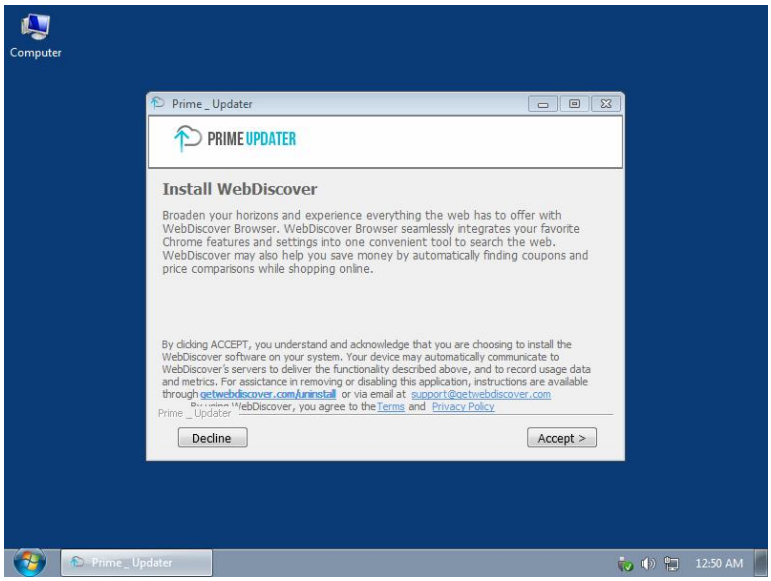

New Tab
Search or enter address

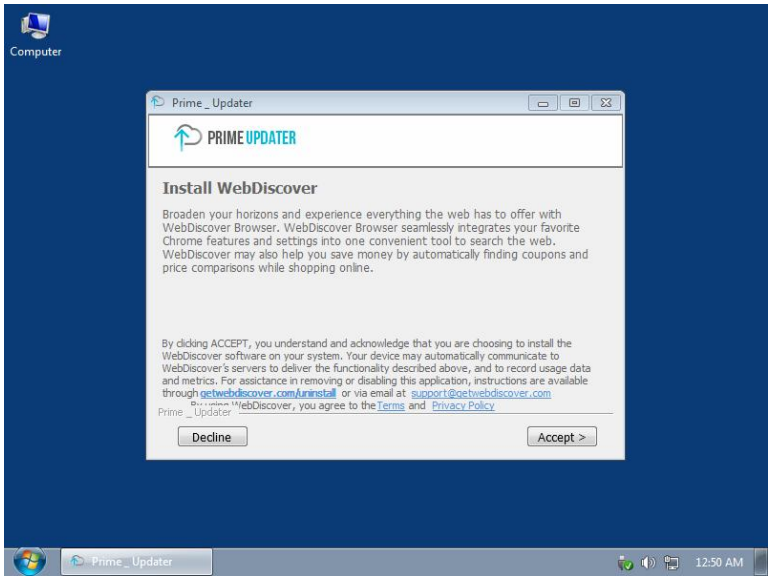

Prime _ Updater
Mozilla Firefox
12:50 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >

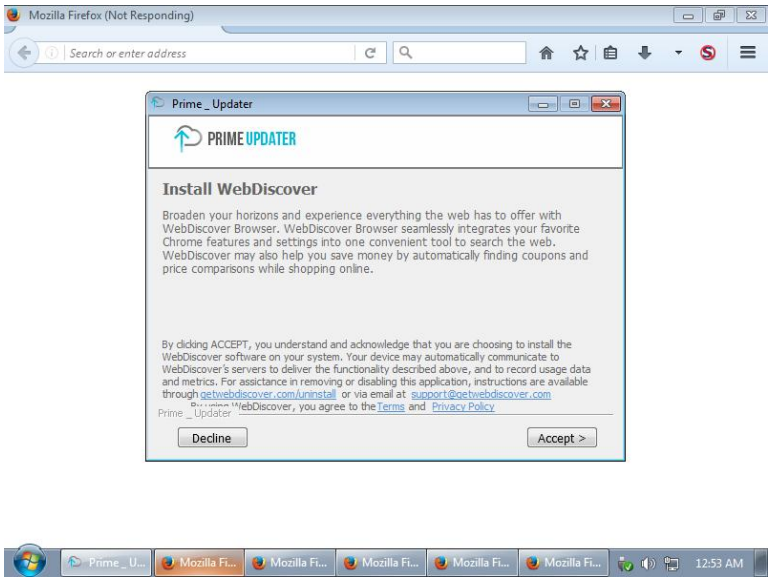

Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Firefox
Firefox has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >

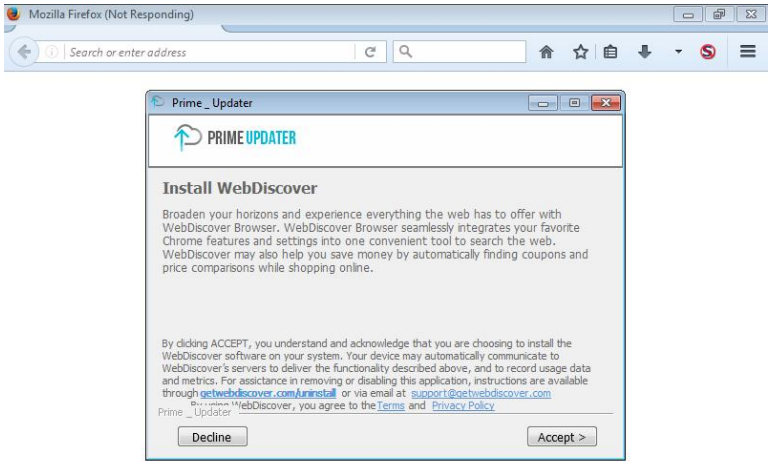

Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
Prime _ Updater
12:50 AM

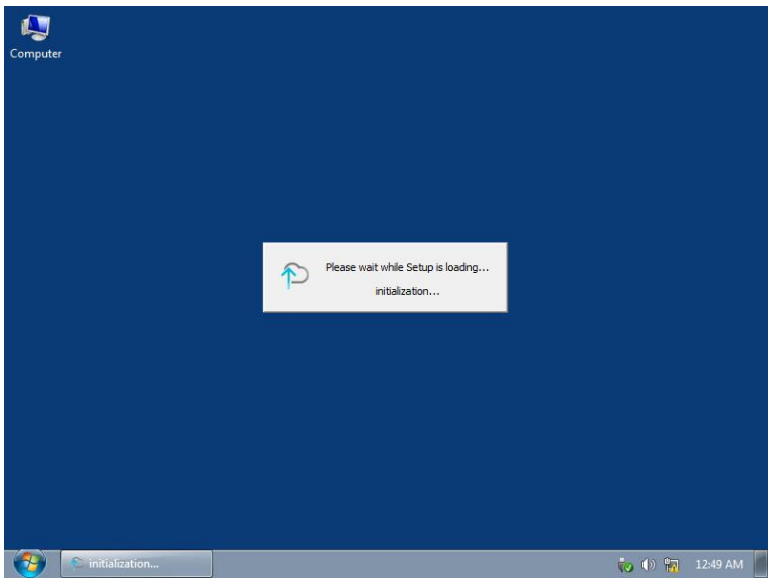

Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
Prime _ Updater
12:50 AM

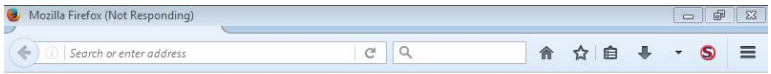

New Tab
Search or enter address

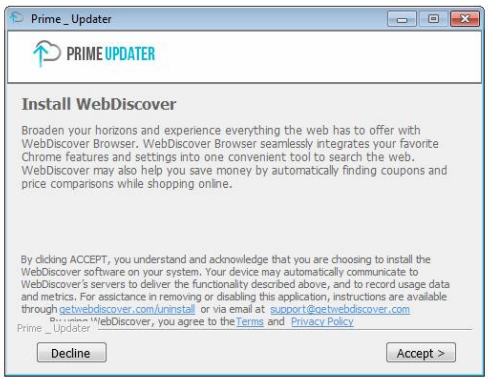

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:50 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
12:53 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
12:51 AM


Computer
Please wait while Setup is loading...
initialization...
initialization...
12:49 AM


Mozilla Firefox (Not Responding)
Search or enter address

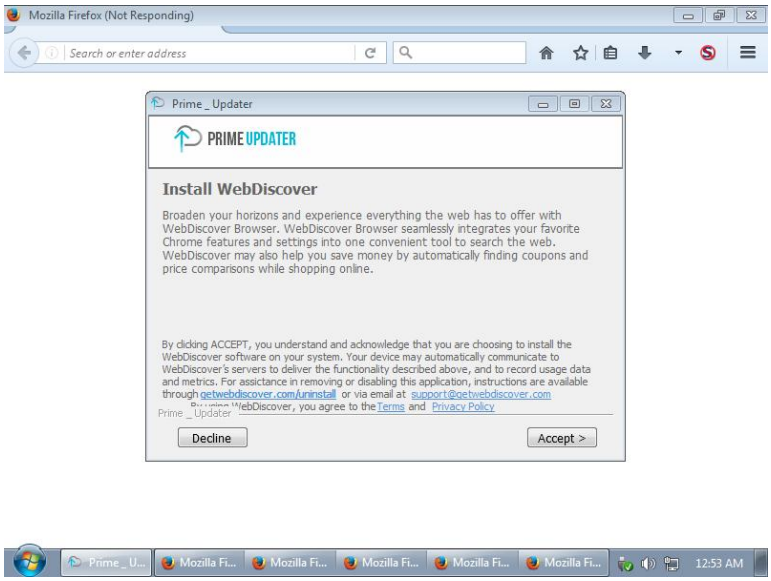

Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >

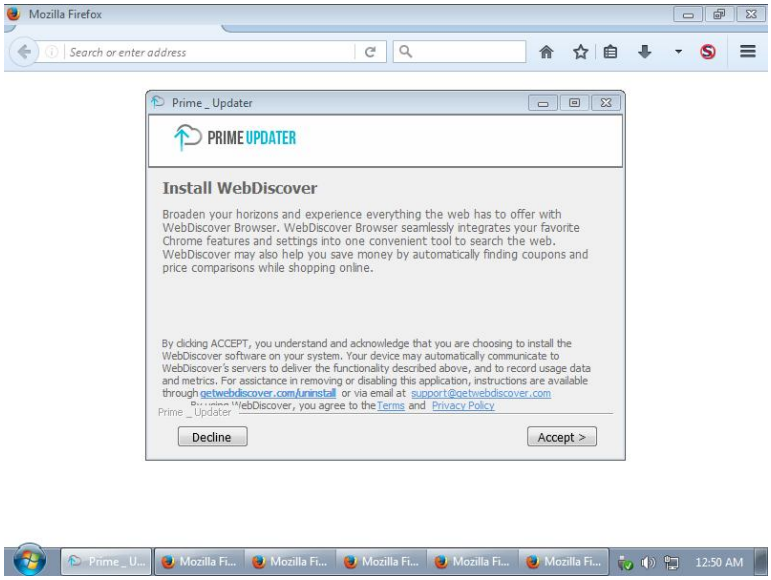

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:52 AM

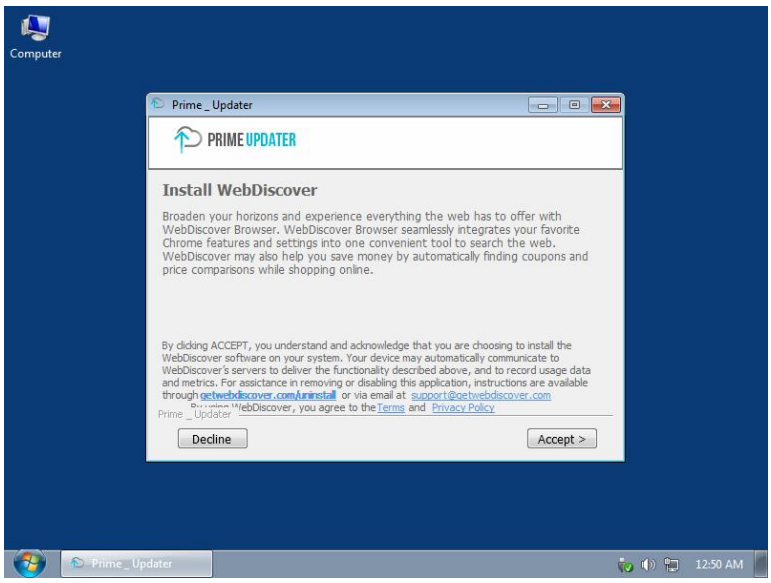

Computer
12:49 AM


Mozilla Firefox (Not Responding)
Search or enter address


Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:53 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
Prime _ U...
Mozilla Fi...
12:53 AM


Mozilla Firefox
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
Prime _ U...
Mozilla Fi...
12:50 AM


Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
Prime _ Updater
12:50 AM

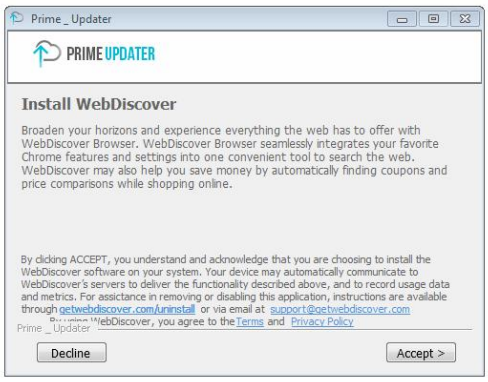

New Tab
Search or enter address


Prime _ Upd...
Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
Mozilla Firefox
12:50 AM

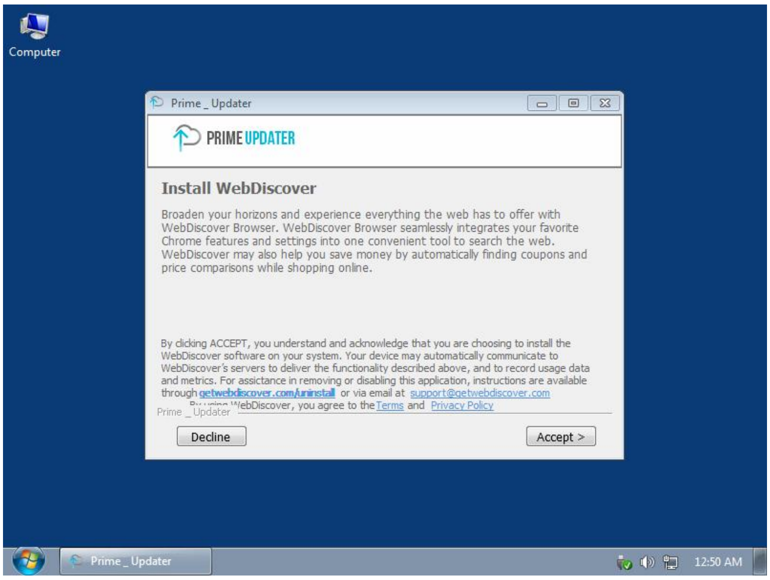

Mozilla Firefox (Not Responding)
Search or enter address

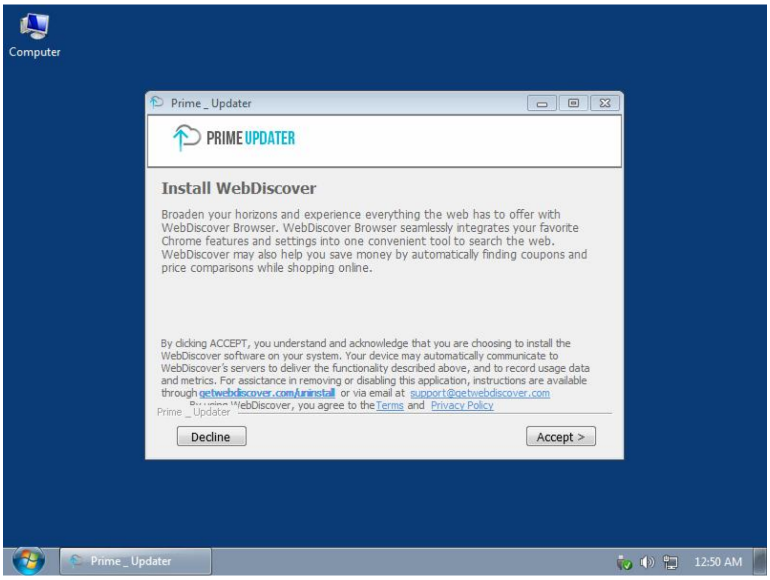

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:53 AM

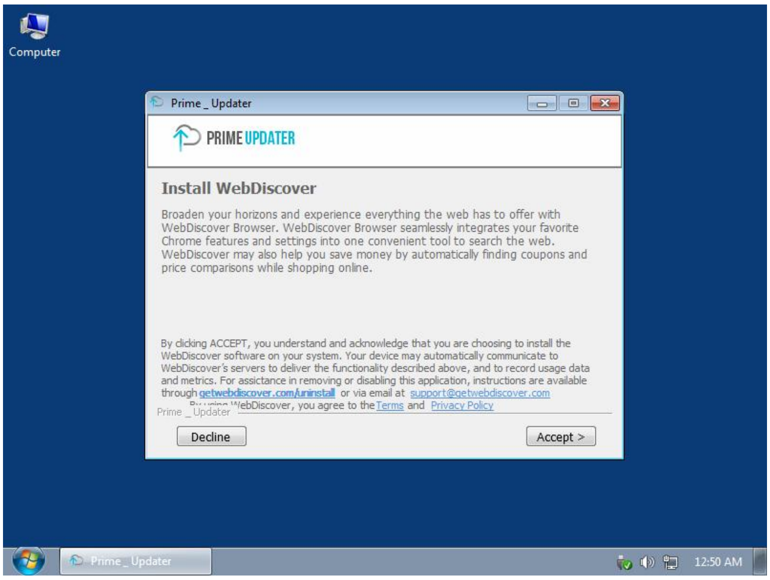

Mozilla Firefox (Not Responding)
Search or enter address

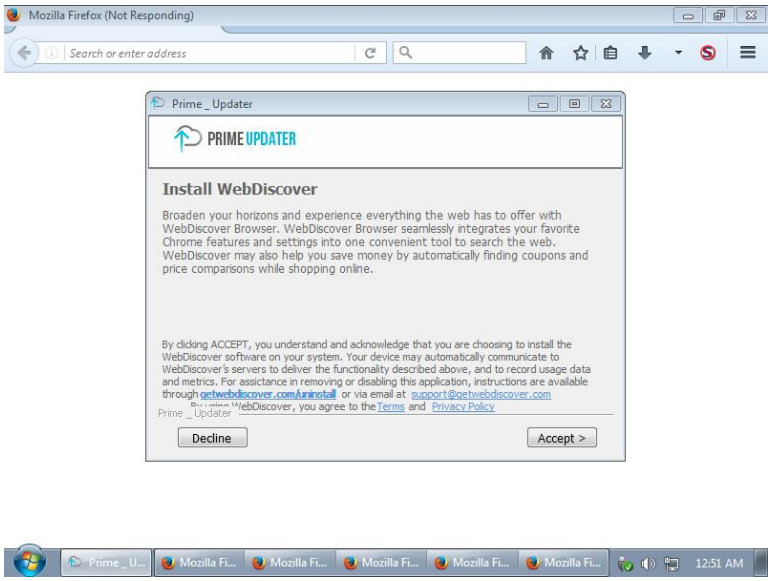

Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >

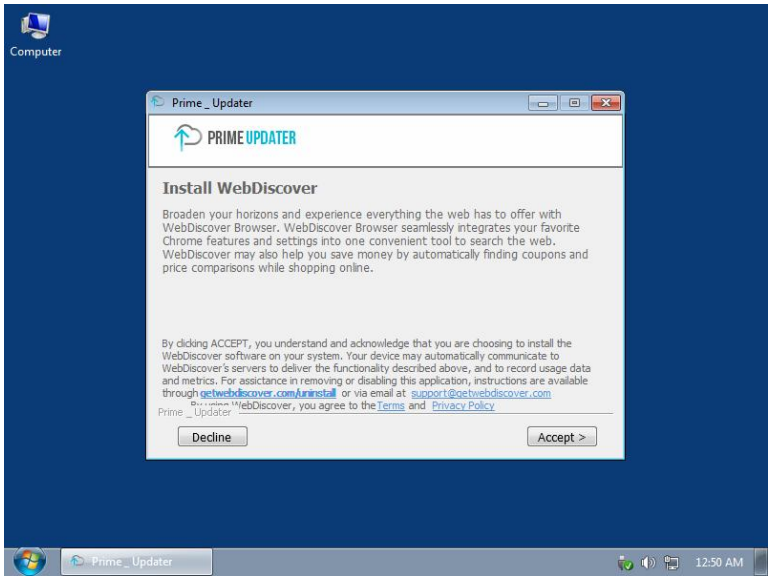

Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:53 AM

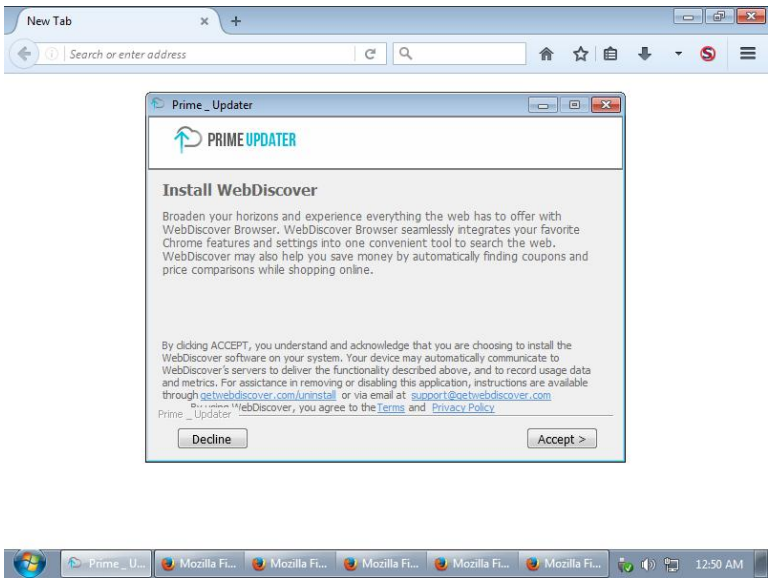

Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
WebDiscover, you agree to the Terms and Privacy Policy
Prime _Updater
Decline
Accept >
Prime _ Updater
12:50 AM

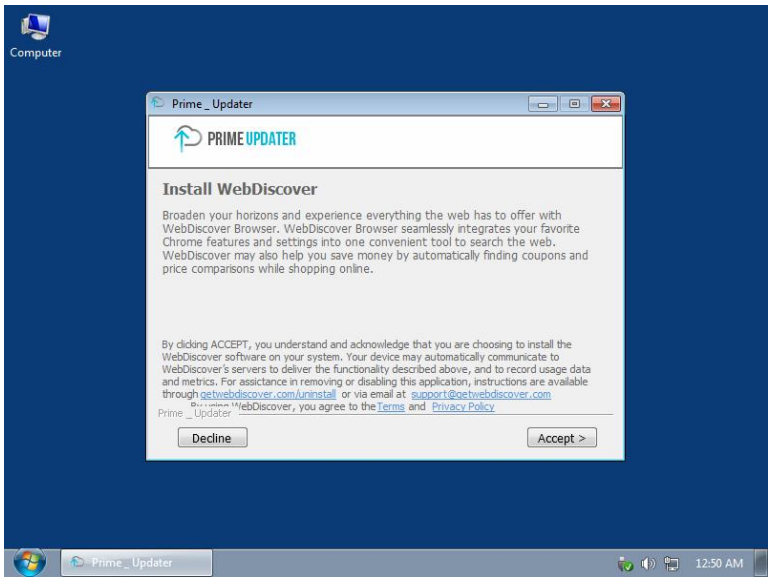

Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
WebDiscover, you agree to the Terms and Privacy Policy
Prime _Updater
Decline
Accept >
Prime _ Updater
12:50 AM

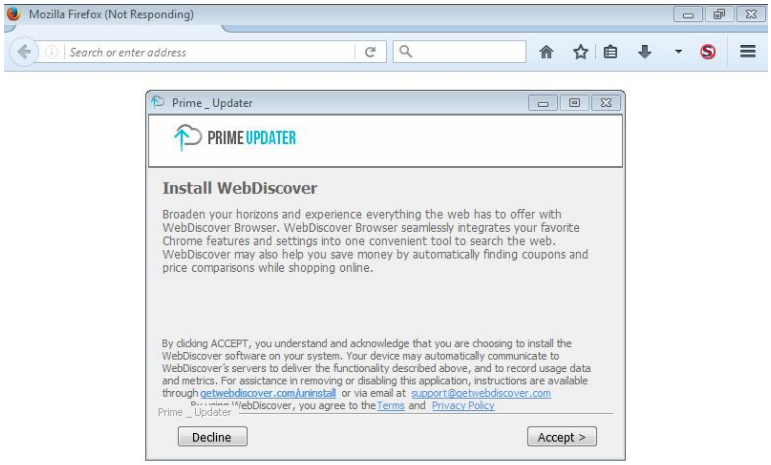

Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
WebDiscover, you agree to the Terms and Privacy Policy
Prime _Updater
Decline
Accept >
Prime _ Updater
12:50 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >
12:51 AM

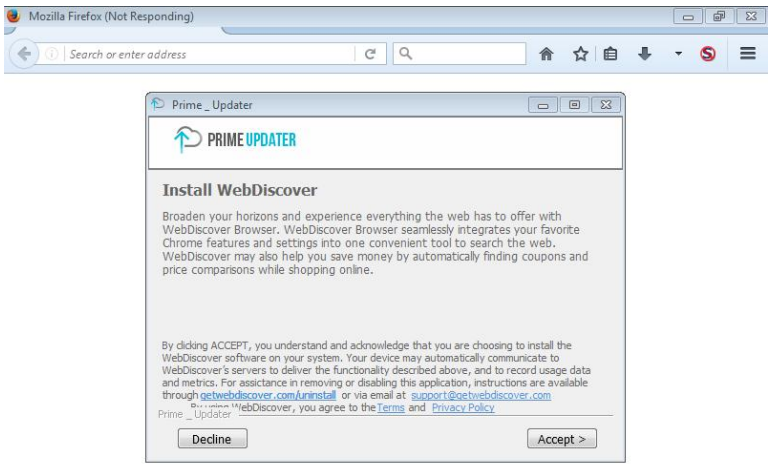

Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >
Prime _ Updater
12:50 AM


New Tab
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
By using WebDiscover, you agree to the Terms and Privacy Policy
Prime _ Updater
Decline
Accept >
12:50 AM


Computer
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >
Prime _ Updater
12:50 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >


Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:52 AM


Mozilla Firefox (Not Responding)
Search or enter address
Prime _ Updater
PRIME UPDATER
Install WebDiscover
Broaden your horizons and experience everything the web has to offer with WebDiscover Browser. WebDiscover Browser seamlessly integrates your favorite Chrome features and settings into one convenient tool to search the web. WebDiscover may also help you save money by automatically finding coupons and price comparisons while shopping online.
By clicking ACCEPT, you understand and acknowledge that you are choosing to install the WebDiscover software on your system. Your device may automatically communicate to WebDiscover's servers to deliver the functionality described above, and to record usage data and metrics. For assistance in removing or disabling this application, instructions are available through getwebdiscover.com/uninstall or via email at support@getwebdiscover.com
Prime _ Updater
Decline
Accept >


Prime _ U...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
Mozilla Fi...
12:51 AM