VALKYRIE COMODO

Summary

File Name: A0017793.exe

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

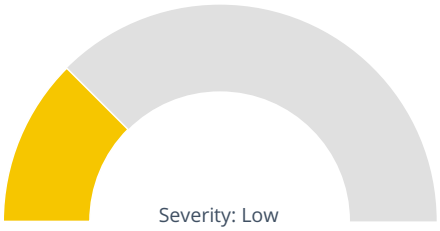
SHA1: 50b322435a8475c50d5a3ac96e49bb2afb88cc5c

MD5: 136b7535bad1fb83fed047becd96e6cf

PUA

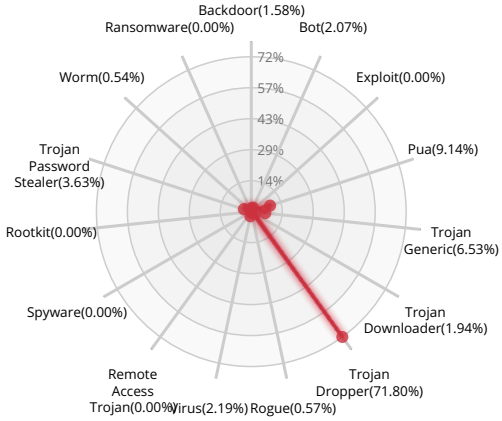
Valkyrie Final Verdict

DETECTION SECTION

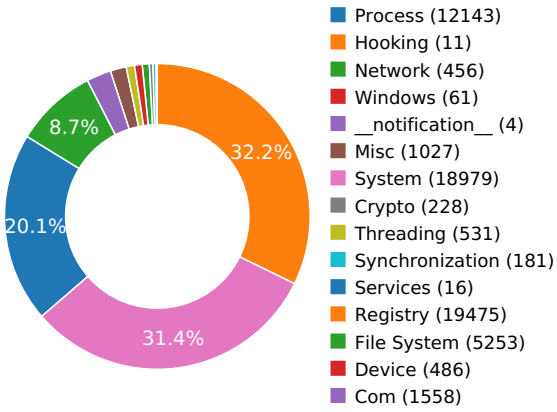


Verdict: PUA

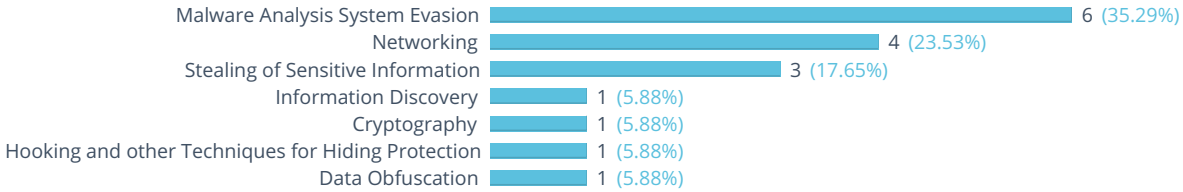
CLASSIFICATION



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 (7 unique times)	Show sources
Starts servers listening on 127.0.0.1:0	
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources

CRYPTOGRAPHY

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

STEALING OF SENSITIVE INFORMATION

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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

DATA OBFUSCATION

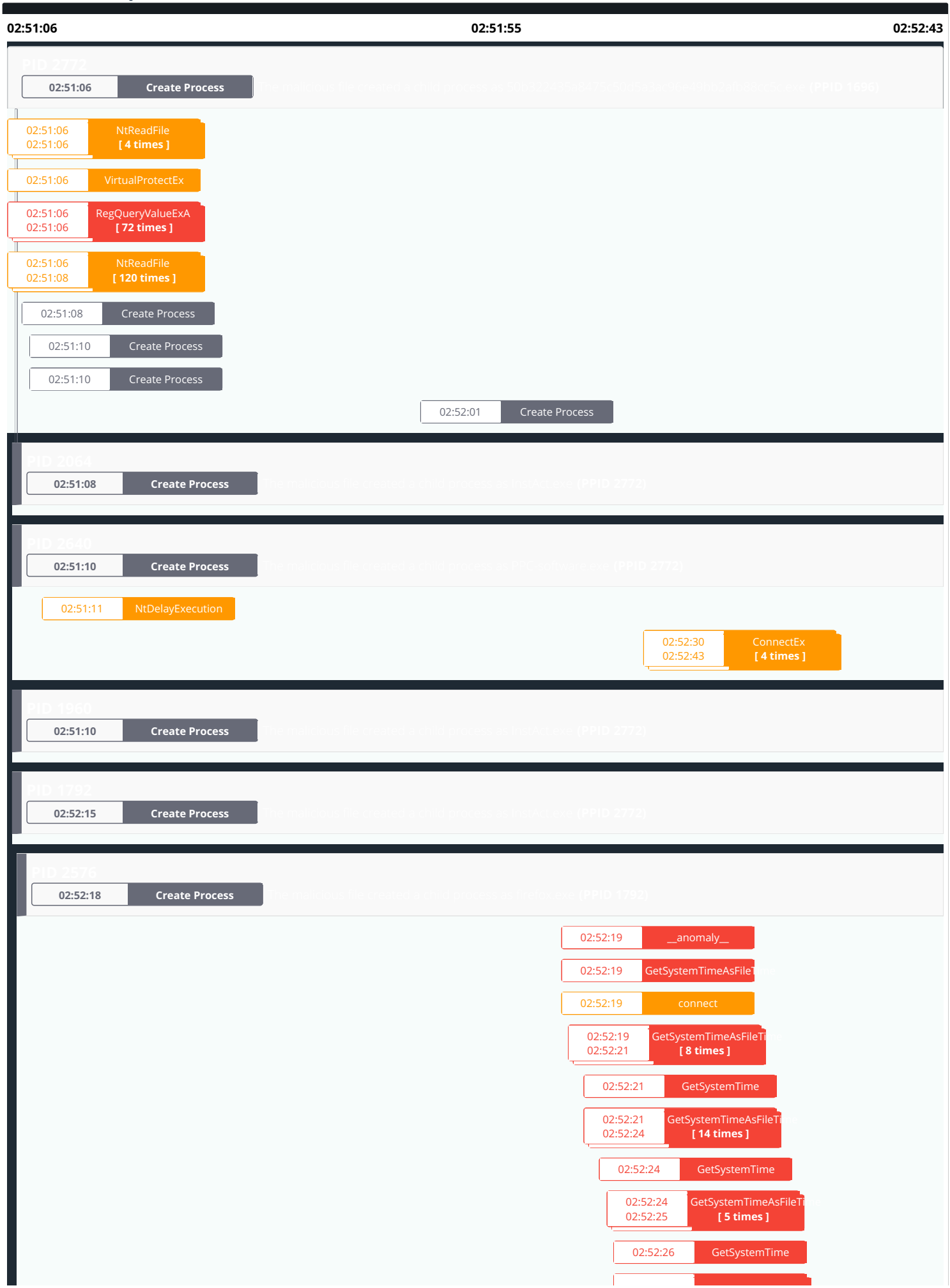
Drops a binary and executes it	Show sources

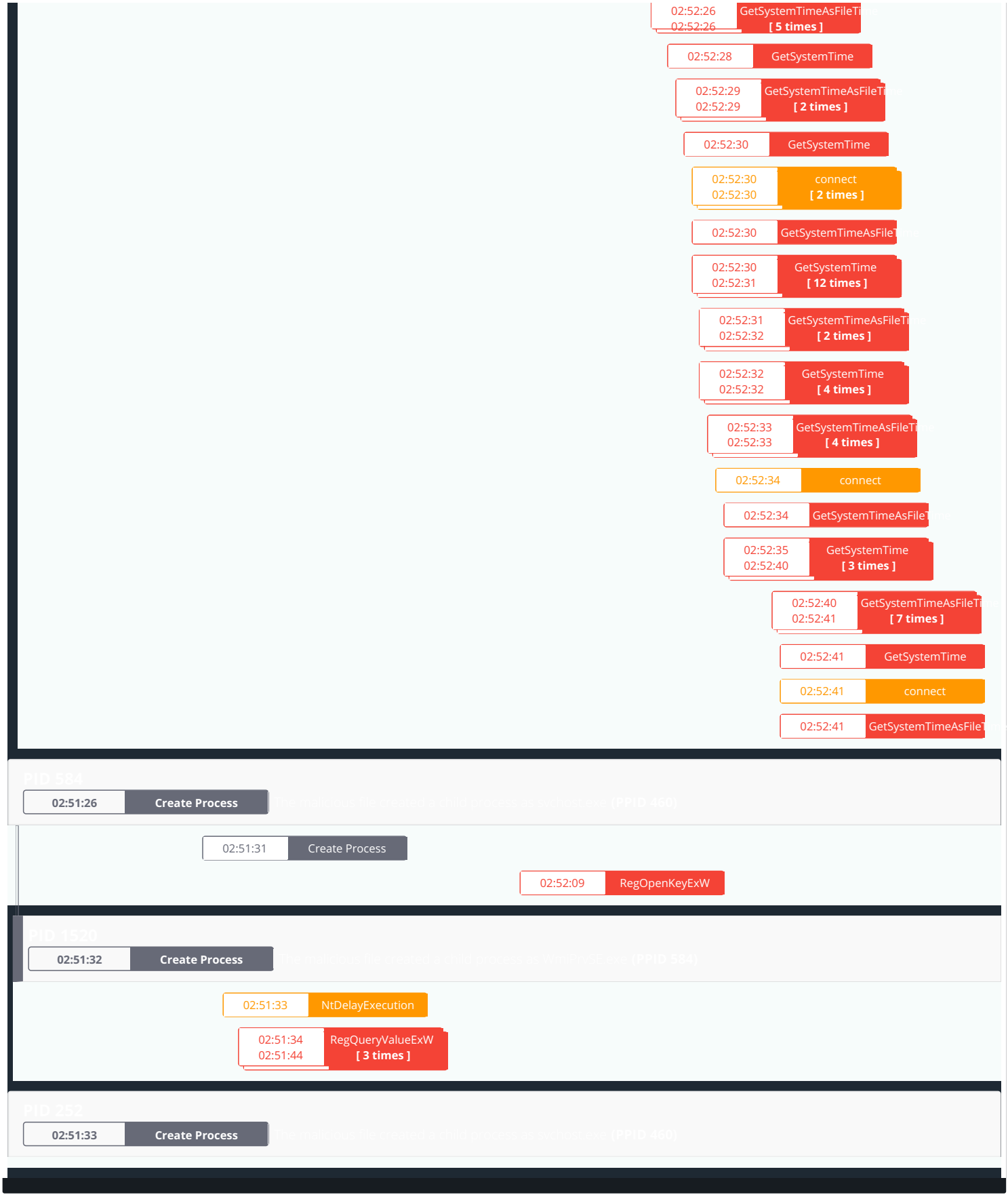
MALWARE ANALYSIS SYSTEM EVASION

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

VALKYRIE COMODO

Behavior Graph




02:52:26 02:52:26 GetSystemTimeAsFileTime [5 times]
02:52:28 GetSystemTime
02:52:29 02:52:29 GetSystemTimeAsFileTime [2 times]
02:52:30 GetSystemTime
02:52:30 02:52:30 connect [2 times]
02:52:30 GetSystemTimeAsFileTime
02:52:30 02:52:31 GetSystemTime [12 times]
02:52:31 02:52:32 GetSystemTimeAsFileTime [2 times]
02:52:32 02:52:32 GetSystemTime [4 times]
02:52:33 02:52:33 GetSystemTimeAsFileTime [4 times]
02:52:34 connect
02:52:34 GetSystemTimeAsFileTime
02:52:35 02:52:40 GetSystemTime [3 times]
02:52:40 02:52:41 GetSystemTimeAsFileTime [7 times]
02:52:41 GetSystemTime
02:52:41 connect
02:52:41 GetSystemTimeAsFileTime
PID 584
02:51:26 Create Process The malicious file created a child process as svchost.exe (PPID 460)
02:51:31 Create Process
02:52:09 RegOpenKeyExW
PID 1520
02:51:32 Create Process The malicious file created a child process as WmiPrvSE.exe (PPID 584)
02:51:33 NtDelayExecution
02:51:34 02:51:44 RegQueryValueExW [3 times]
PID 252
02:51:33 Create Process The malicious file created a child process as svchost.exe (PPID 460)

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\SHFOLDER.DLL
C:\Windows\System32\shfolder.dll
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nsa224E.tmp
C:\Users\user\AppData\Local\Temp\50b322435a8475c50d5a3ac96e49bb2afb88cc5c.exe
C:\Users\user\AppData\Local\Temp\nsa22EB.tmp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\nsa22EB.tmp\System.dll
C:\Program Files (x86)
C:\Program Files (x86)\PPC-software
C:\Program Files (x86)\PPC-software\ComponentFactory.Krypton.Toolkit.dll
C:\Program Files (x86)\PPC-software\DeepClean.dll
C:\Program Files (x86)\PPC-software\DeepClean.dll.config
C:\Program Files (x86)\PPC-software\InstAct.exe
C:\Program Files (x86)\PPC-software\InstAct.exe.config
C:\Program Files (x86)\PPC-software\Interop.IWshRuntimeLibrary.dll
C:\Program Files (x86)\PPC-software\Interop.Shell32.dll
C:\Program Files (x86)\PPC-software\LinqBridge.dll
C:\Program Files (x86)\PPC-software\Microsoft.Win32.TaskScheduler.dll
C:\Program Files (x86)\PPC-software\ObjectListView.dll
C:\Program Files (x86)\PPC-software\PPC-software.exe
C:\Program Files (x86)\PPC-software\PPC-software.exe.config
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe.config
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe.manifest
C:\Program Files (x86)\PPC-software\SQLite.Interop.dll

C:\Program Files (x86)\PPC-software\Setup.dll
C:\Program Files (x86)\PPC-software\Setup.dll.config
C:\Program Files (x86)\PPC-software\Splash.exe
C:\Program Files (x86)\PPC-software\Splash.exe.config
C:\Program Files (x86)\PPC-software\System.Data.SQLite.dll
C:\Program Files (x86)\PPC-software\mlogger.log
C:\Program Files (x86)\PPC-software\ar
C:\Program Files (x86)\PPC-software\ar\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\ar\Splash.resources.dll
C:\Program Files (x86)\PPC-software\bs-Cyrl-BA
C:\Program Files (x86)\PPC-software\bs-Cyrl-BA\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\bs-Cyrl-BA\Splash.resources.dll
C:\Program Files (x86)\PPC-software\bs-Latn-BA
C:\Program Files (x86)\PPC-software\bs-Latn-BA\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\bs-Latn-BA\Splash.resources.dll
C:\Program Files (x86)\PPC-software\da
C:\Program Files (x86)\PPC-software\da\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\da\Splash.resources.dll
C:\Program Files (x86)\PPC-software\de
C:\Program Files (x86)\PPC-software\de\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\de\Splash.resources.dll
C:\Program Files (x86)\PPC-software\es
C:\Program Files (x86)\PPC-software\es\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\es\Splash.resources.dll
C:\Program Files (x86)\PPC-software\fil-PH
C:\Program Files (x86)\PPC-software\fil-PH\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\fil-PH\Splash.resources.dll
C:\Program Files (x86)\PPC-software\fr
C:\Program Files (x86)\PPC-software\fr\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\fr\Splash.resources.dll
C:\Program Files (x86)\PPC-software\he
C:\Program Files (x86)\PPC-software\he\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\he\Splash.resources.dll
C:\Program Files (x86)\PPC-software\hr-HR
C:\Program Files (x86)\PPC-software\hr-HR\PPC-software.resources.dll

C:\Program Files (x86)\PPC-software\hr-HR\Splash.resources.dll
C:\Program Files (x86)\PPC-software\it
C:\Program Files (x86)\PPC-software\it\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\it\Splash.resources.dll
C:\Program Files (x86)\PPC-software\ja
C:\Program Files (x86)\PPC-software\ja\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\ja\Splash.resources.dll
C:\Program Files (x86)\PPC-software\nl
C:\Program Files (x86)\PPC-software\nl\PPC-software.resources.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\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 46.0.1 (x86 en-US)\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PIL-py2.7\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Universal Extractor_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{19A5926D-66E1-46FC-854D-163AA10A52D3}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{1F5C7BAE-1E1A-7C93-1B90-84CE308AFC1C}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{26A24AE4-039D-4CA4-87B4-2F83218091F0}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{29D3773E-54F4-23C2-D523-236A4453B845}_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{34B86C7D-4103-201B-3A13-03934DB11543}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{37464E70-B0B9-9DFF-649A-CBE169BAD657}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{56AD3004-0B49-967F-F682-B05650B61A78}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{60EC980A-BDA2-4CB6-A427-B07A5498B4CA}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{64F3FB9A-9250-B2D6-00B4-50BE0358AEE8}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{74d0e5db-b326-4dae-a6b2-445b9de1836e}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0015-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0015-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0016-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0016-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0018-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0018-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0019-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0019-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001A-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001A-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001B-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001B-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001F-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001F-0409-0000-0000000FF1CE}_ENTERPRISE_{ABDDE972-355B-4AF1-89A8-DA50B7B5C045}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001F-040C-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001F-040C-0000-0000000FF1CE}_ENTERPRISE_{F580DDD5-8D37-4998-968E-EBB76BB86787}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001F-0C0A-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-001F-0C0A-0000-0000000FF1CE}_ENTERPRISE_{187308AB-5FA7-4F14-9AB9-D290383A10D9}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-002A-0000-1000-0000000FF1CE}_ENTERPRISE_{E64BA721-2310-4B55-BE5A-2925F9706192}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-002A-0409-1000-0000000FF1CE}_ENTERPRISE_{DE5A002D-8122-4278-A7EE-3121E7EA254E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-002C-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0030-0000-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0030-0000-0000-0000000FF1CE}_ENTERPRISE_{0B36C6D6-F5D8-4EAF-BF94-4376A230AD5B}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0044-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0044-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-006E-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-006E-0409-0000-0000000FF1CE}_ENTERPRISE_{DE5A002D-8122-4278-A7EE-3121E7EA254E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-00A1-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-00A1-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-00BA-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-00BA-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0114-0409-0000-0000000FF1CE}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0114-0409-0000-0000000FF1CE}_ENTERPRISE_{2FC4457D-409E-466F-861F-FB0CB796B53E}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0115-0409-0000-0000000FF1CE}\DisplayName

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\nsa22EB.tmp\System.dll
C:\Program Files (x86)\PPC-software\ComponentFactory.Krypton.Toolkit.dll
C:\Program Files (x86)\PPC-software\DeepClean.dll
C:\Program Files (x86)\PPC-software\DeepClean.dll.config
C:\Program Files (x86)\PPC-software\InstAct.exe
C:\Program Files (x86)\PPC-software\InstAct.exe.config

C:\Program Files (x86)\PPC-software\Interop.IWshRuntimeLibrary.dll
C:\Program Files (x86)\PPC-software\Interop.Shell32.dll
C:\Program Files (x86)\PPC-software\LinqBridge.dll
C:\Program Files (x86)\PPC-software\Microsoft.Win32.TaskScheduler.dll
C:\Program Files (x86)\PPC-software\ObjectListView.dll
C:\Program Files (x86)\PPC-software\PPC-software.exe
C:\Program Files (x86)\PPC-software\PPC-software.exe.config
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe.config
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe.manifest
C:\Program Files (x86)\PPC-software\SQLite.Interop.dll
C:\Program Files (x86)\PPC-software\Setup.dll
C:\Program Files (x86)\PPC-software\Setup.dll.config
C:\Program Files (x86)\PPC-software\Splash.exe
C:\Program Files (x86)\PPC-software\Splash.exe.config
C:\Program Files (x86)\PPC-software\System.Data.SQLite.dll
C:\Program Files (x86)\PPC-software\mlogger.log
C:\Program Files (x86)\PPC-software\ar\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\ar\Splash.resources.dll
C:\Program Files (x86)\PPC-software\bs-Cyrl-BA\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\bs-Cyrl-BA\Splash.resources.dll
C:\Program Files (x86)\PPC-software\bs-Latn-BA\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\bs-Latn-BA\Splash.resources.dll
C:\Program Files (x86)\PPC-software\da\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\da\Splash.resources.dll
C:\Program Files (x86)\PPC-software\de\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\de\Splash.resources.dll
C:\Program Files (x86)\PPC-software\es\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\es\Splash.resources.dll
C:\Program Files (x86)\PPC-software\fil-PH\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\fil-PH\Splash.resources.dll
C:\Program Files (x86)\PPC-software\fr\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\fr\Splash.resources.dll
C:\Program Files (x86)\PPC-software\he\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\he\Splash.resources.dll

C:\Program Files (x86)\PPC-software\hr-HR\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\hr-HR\Splash.resources.dll
C:\Program Files (x86)\PPC-software\it\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\it\Splash.resources.dll
C:\Program Files (x86)\PPC-software\ja\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\ja\Splash.resources.dll
C:\Program Files (x86)\PPC-software\nl\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\nl\Splash.resources.dll
C:\Program Files (x86)\PPC-software\no\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\no\Splash.resources.dll
C:\Program Files (x86)\PPC-software\pl\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\pl\Splash.resources.dll
C:\Program Files (x86)\PPC-software\pt\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\pt\Splash.resources.dll
C:\Program Files (x86)\PPC-software\ru\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\ru\Splash.resources.dll
C:\Program Files (x86)\PPC-software\se-FI\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\se-FI\Splash.resources.dll
C:\Program Files (x86)\PPC-software\sr-Cyrl-RS\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\sr-Cyrl-RS\Splash.resources.dll
C:\Program Files (x86)\PPC-software\sr-Latn-RS\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\sr-Latn-RS\Splash.resources.dll
C:\Program Files (x86)\PPC-software\sv\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\sv\Splash.resources.dll
C:\Program Files (x86)\PPC-software\th-TH\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\th-TH\Splash.resources.dll
C:\Program Files (x86)\PPC-software\tr-TR\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\tr-TR\Splash.resources.dll
C:\Program Files (x86)\PPC-software\azurant.exe
\??\PIPE\srvsvc
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PPC-software\PPC-software.lnk
C:\Users\user\Desktop\PPC-software.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\My application\Uninstall.lnk
C:\Program Files (x86)\PPC-software\uninst.exe

C:\Program Files (x86)\PPC-software\azurant.ini

RESOLVED APIS

cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
shfolder.dll.SHGetFolderPathA
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
kernel32.dll.GetUserDefaultUILanguage
system.dll.Call
kernel32.dll.GetCurrentProcess
kernel32.dll.IsWow64Process
propsys.dll.PSCreateMemoryPropertyStore
linkinfo.dll.CreateLinkInfoW
user32.dll.IsCharAlphaW
user32.dll.CharPrevW
ntshrui.dll.GetNetResourceFromLocalPathW
srvcli.dll.NetShareEnum
cscapi.dll.CscNetApiGetInterface
slc.dll.SLGetWindowsInformationDWORD
shlwapi.dll.PathRemoveFileSpecW
linkinfo.dll.DestroyLinkInfo
system.dll.Int64Op
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
netutils.dll.NetApiBufferFree
advapi32.dll.UnregisterTraceGuids
comctl32.dll.#321
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx

kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCMapStringEx
kernel32.dll.GetTickCount64
advapi32.dll.EventRegister
mscoree.dll.#142

DELETED FILES

C:\Users\user\AppData\Local\Temp\nsa224E.tmp
C:\Users\user\AppData\Local\Temp\nsa22EB.tmp
C:\Users\user\AppData\Local\Temp\nsa22EB.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsa22EB.tmp\
C:\Users\user\AppData\Local\PPC-software\PPC-software.exe_Url_1xuetxnfnbprkyvp4f3fgknib3pg5muj\3.1.5.0\bajca21k.newcfg
C:\Users\user\AppData\Local\PPC-software\PPC-software.exe_Url_1xuetxnfnbprkyvp4f3fgknib3pg5muj\3.1.5.0\bajca21k.tmp
C:\Users\user\Documents\PPC-software\log.txt
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\19952
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\Temp\mozilla-temp-files
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm
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-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\storage\permanent\moz-safe-about+home\idb\818200132aebmoouht.sqlite-wal
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
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\Windows\CurrentVersion\App Paths\PPC-software.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE40
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IEData
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 46.0.1 (x86 en-US)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 46.0.1 (x86 en-US)\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PIL-py2.7
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PIL-py2.7\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Universal Extractor_is1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Universal Extractor_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WIC
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{19A5926D-66E1-46FC-854D-163AA10A52D3}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{19A5926D-66E1-46FC-854D-163AA10A52D3}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{1F5C7BAE-1E1A-7C93-1B90-84CE308AFC1C}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{1F5C7BAE-1E1A-7C93-1B90-84CE308AFC1C}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{26A24AE4-039D-4CA4-87B4-2F83218091F0}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{26A24AE4-039D-4CA4-87B4-2F83218091F0}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{29D3773E-54F4-23C2-D523-236A4453B845}_is1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{29D3773E-54F4-23C2-D523-236A4453B845}_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{34B86C7D-4103-201B-3A13-03934DB11543}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{34B86C7D-4103-201B-3A13-03934DB11543}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{37464E70-B0B9-9DFF-649A-CBE169BAD657}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{37464E70-B0B9-9DFF-649A-CBE169BAD657}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{56AD3004-0B49-967F-F682-B05650B61A78}

EXECUTED COMMANDS

"C:\Program Files (x86)\PPC-software\InstAct.exe" createini
"C:\Program Files (x86)\PPC-software\PPC-software.exe" startscan
"C:\Program Files (x86)\PPC-software\InstAct.exe" install
"C:\Program Files (x86)\PPC-software\InstAct.exe" installurl
C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
https://safe-registration.com/welcome5

READ FILES

\Device\KsecDD
C:\Windows\System32\shfolder.dll
C:\Users\user\AppData\Local\Temp\nsa224E.tmp
C:\Users\user\AppData\Local\Temp\50b322435a8475c50d5a3ac96e49bb2afb88cc5c.exe
C:\Users\user\AppData\Local\Temp\nsa22EB.tmp
C:\Users\user\AppData\Local\Temp\nsa22EB.tmp\System.dll
C:\
C:\Program Files (x86)\desktop.ini
C:\Program Files (x86)
C:\Program Files (x86)\PPC-software

\??\PIPE\srvsvc
C:\Program Files (x86)\PPC-software\PPC-software.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PPC-software\PPC-software.lnk
C:\Users\user\Desktop\PPC-software.lnk
C:\Program Files (x86)\PPC-software\uninst.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\My application\Uninstall.lnk
C:\Program Files (x86)\PPC-software\azurant.exe
C:\Program Files (x86)\PPC-software\ComponentFactory.Krypton.Toolkit.dll
C:\Program Files (x86)\PPC-software\DeepClean.dll
C:\Program Files (x86)\PPC-software\DeepClean.dll.config
C:\Program Files (x86)\PPC-software\InstAct.exe
C:\Program Files (x86)\PPC-software\InstAct.exe.config
C:\Program Files (x86)\PPC-software\Interop.IWshRuntimeLibrary.dll
C:\Program Files (x86)\PPC-software\Interop.Shell32.dll
C:\Program Files (x86)\PPC-software\LinqBridge.dll
C:\Program Files (x86)\PPC-software\Microsoft.Win32.TaskScheduler.dll
C:\Program Files (x86)\PPC-software\mlogger.log
C:\Program Files (x86)\PPC-software\ObjectListView.dll
C:\Program Files (x86)\PPC-software\PPC-software.exe.config
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe.config
C:\Program Files (x86)\PPC-software\PPC-software.vshost.exe.manifest
C:\Program Files (x86)\PPC-software\Setup.dll
C:\Program Files (x86)\PPC-software\Setup.dll.config
C:\Program Files (x86)\PPC-software\Splash.exe
C:\Program Files (x86)\PPC-software\Splash.exe.config
C:\Program Files (x86)\PPC-software\SQLite.Interop.dll
C:\Program Files (x86)\PPC-software\System.Data.SQLite.dll
C:\Program Files (x86)\PPC-software\tr-TR\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\tr-TR\Splash.resources.dll
C:\Program Files (x86)\PPC-software\th-TH\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\th-TH\Splash.resources.dll
C:\Program Files (x86)\PPC-software\sv\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\sv\Splash.resources.dll
C:\Program Files (x86)\PPC-software\sr-Latn-RS\PPC-software.resources.dll

C:\Program Files (x86)\PPC-software\sr-Latn-RS\Splash.resources.dll
C:\Program Files (x86)\PPC-software\sr-Cyrl-RS\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\sr-Cyrl-RS\Splash.resources.dll
C:\Program Files (x86)\PPC-software\se-FI\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\se-FI\Splash.resources.dll
C:\Program Files (x86)\PPC-software\ru\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\ru\Splash.resources.dll
C:\Program Files (x86)\PPC-software\pt\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\pt\Splash.resources.dll
C:\Program Files (x86)\PPC-software\pl\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\pl\Splash.resources.dll
C:\Program Files (x86)\PPC-software\no\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\no\Splash.resources.dll
C:\Program Files (x86)\PPC-software\nl\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\nl\Splash.resources.dll
C:\Program Files (x86)\PPC-software\ja\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\ja\Splash.resources.dll
C:\Program Files (x86)\PPC-software\it\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\it\Splash.resources.dll
C:\Program Files (x86)\PPC-software\hr-HR\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\hr-HR\Splash.resources.dll
C:\Program Files (x86)\PPC-software\he\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\he\Splash.resources.dll
C:\Program Files (x86)\PPC-software\fr\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\fr\Splash.resources.dll
C:\Program Files (x86)\PPC-software\fil-PH\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\fil-PH\Splash.resources.dll
C:\Program Files (x86)\PPC-software\es\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\es\Splash.resources.dll
C:\Program Files (x86)\PPC-software\de\PPC-software.resources.dll
C:\Program Files (x86)\PPC-software\de\Splash.resources.dll

MUTEXES

PPC-software
CicLoadWinStaWinSta0

Local\MSCTF.CtfMonitorInstMutexDefault1
Local\ZonesCounterMutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\!IETld!Mutex
Local\FirefoxStartupMutex
Local\MSCTF.Asm.MutexDefault1
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
Local\WininetStartupMutex
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex

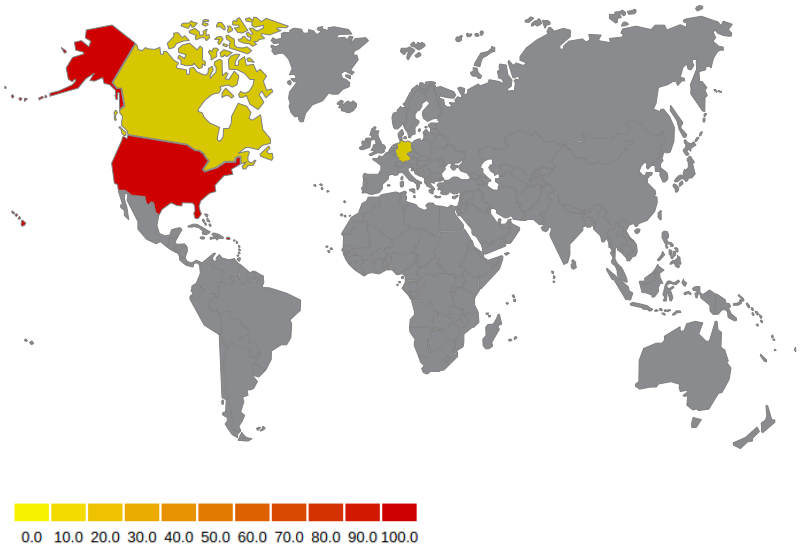
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\PPC-software.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\PPC-software.exe\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\DisplayIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\DisplayVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\Publisher
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\QuietUninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\NoModify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\NoRepair
HKEY_LOCAL_MACHINE\SOFTWARE\PPC-software\PPC-software
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PPC-software\PPC-software\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PPC-software\PPC-software\Version
HKEY_CURRENT_USER\SOFTWARE\PPC-software\PPC-software
HKEY_CURRENT_USER\Software\PPC-software\PPC-software\Custom1
HKEY_CURRENT_USER\Software\PPC-software\PPC-software\Custom2
HKEY_CURRENT_USER\Software\PPC-software\PPC-software\ResName

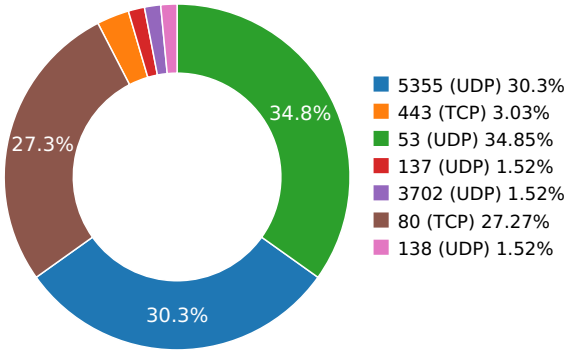
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\PPC-software\EstimatedSize
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\PPC-software_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\PPC-software_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\PPC-software_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\PPC-software_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\PPC-software_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\PPC-software_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\PPC-software_RASAPI32\FileDirectory
HKEY_CURRENT_USER\Software\PPC-softwareLanguage
HKEY_CURRENT_USER\Software\PPC-softwareLanguage\lang
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

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
	104.18.20.226	United States	13335	Cloudflare, Inc.	Malware Process
	23.215.131.169	United States	20940	Akamai Technologies, Inc.	OS Process
	23.215.131.200	United States	20940	Akamai Technologies, Inc.	OS Process
	192.241.99.194	Canada	55286	B2 Net Solutions Inc.	Malware Process
secure.informaction.com	69.195.158.196	United States	19969	Joe's Datacenter, LLC	Malware Process
s2.symcb.com	23.50.75.27	United States	3257	Akamai Technologies, Inc.	Malware Process
crl.microsoft.com	208.185.118.88	United States	6461	Zayo Bandwidth	OS Process
a652.dscb.akamai.net	38.69.238.19	United States	174	PSINet, Inc.	Malware Process
sv.symcd.com	23.50.75.27	United States	3257	Akamai Technologies, Inc.	Malware Process
ocsp.int-x3.letsencrypt.org	38.69.238.113	United States	174	PSINet, Inc.	Malware Process
sv.symcb.com	72.21.91.29	United States	15133	MCI Communications Serv...	Malware Process
ocsp.usertrust.com	38.69.238.11	United States	174	PSINet, Inc.	OS Process
a207.dscb.akamai.net	38.69.238.10	United States	174	PSINet, Inc.	Malware Process
notification.adblockplus.org	78.47.138.56	Germany	24940		Malware Process
ctldl.windowsupdate.com	208.185.118.89	United States	6461	Zayo Bandwidth	OS Process
ocsp.comodoca.com	38.69.238.19	United States	174	PSINet, Inc.	OS Process
a771.dscq.akamai.net	38.93.140.16	United States	26769	PSINet, Inc.	Malware Process
safe-registration.com	172.99.100.191	United States	33070	Cloud Loadbalancing as a S...	Malware Process
crl.globalsign.net	151.101.22.133	United States	54113	Fastly	Malware Process
easylist-downloads.adblockplus.org	176.9.122.53	Germany	24940		Malware Process
pppcw.shieldapps.ml	37.97.173.64	Netherlands	20857		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	1	90.3878748417
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?63600f0772d56571 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?63600f0772d56571						
s2.symcb.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	97.6835708618
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCED141%2Fl2SWCyYX308B7Khio%3D **URI:** http://s2.symcb.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCED141%2Fl2SWCyYX308B7Khio%3D						
pppcw.shieldapps.ml	80	POST	1.1		1	103.33739686
Path: /pppcw/pppcw.php **URI:** http://pppcw.shieldapps.ml/pppcw/pppcw.php						
sv.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	103.849877834
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQe6LNDJdqx%2BJOp7hVgTeaGFJ%2FCQgQUljtT8Hkzl699g%2B8uK8zKt4YecmYCEGllzqlxaYVWCPVm%2BOHAM%2FM%3D **URI:** http://sv.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQe6LNDJdqx%2BJOp7hVgTeaGFJ%2FCQgQUljtT8Hkzl699g%2B8uK8zKt4YecmYCEGllzqlxaYVWCPVm%2BOHAM%2FM%3D						
sv.symcb.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	103.875424862
Path: /sv.crl **URI:** http://sv.symcb.com/sv.crl						
pppcw.shieldapps.ml	80	POST	1.1		1	123.092378855
Path: /pppcw/pppcw.php **URI:** http://pppcw.shieldapps.ml/pppcw/pppcw.php						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	148.779680014
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	154.108059883
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	159.375500917
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	164.84492898
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
notification.adblockplus.org	A

Request	Type
Answers - 136.243.55.39 (A) - 94.130.73.110 (A) - 88.99.186.153 (A) - 95.216.27.38 (A) - 144.76.116.39 (A) - 148.251.12.230 (A) - easylist-downloads.adblockplus.org (CNAME) - 5.9.15.86 (A) - 176.9.122.53 (A) - 94.130.104.89 (A) - 176.9.26.105 (A) - 46.4.115.44 (A) - 148.251.66.238 (A)	
easylist-downloads.adblockplus.org	A
Answers - 136.243.88.49 (A) - 46.4.68.226 (A) - 78.46.39.215 (A) - 88.99.186.149 (A) - 144.76.20.58 (A) - 94.130.168.30 (A) - 85.10.210.166 (A) - 136.243.62.212 (A) - 78.46.27.186 (A) - 178.63.70.146 (A)	
easylist-downloads.adblockplus.org	AAAA
Answers - 2a01:4f8:151:8129::2 (AAAA) - 2a01:4f9:2a:1b5f::2 (AAAA) - 2a01:4f8:200:2175::2 (AAAA) - 2a01:4f8:222:1982::2 (AAAA)	
ocsp.comodoca.com	A
Answers - ocsp.comodoca.com.edgesuite.net (CNAME) - a652.dscb.akamai.net (CNAME) - 184.84.243.42 (A) - 184.84.243.34 (A)	
ocsp.usertrust.com	A
Answers - ocsp.usertrust.com.edgesuite.net (CNAME) - 23.67.251.26 (A) - a207.dscb.akamai.net (CNAME) - 23.67.251.33 (A)	
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)	
a652.dscb.akamai.net	A
a207.dscb.akamai.net	A

Request	Type
Answers - 184.84.243.57 (A) - 184.84.243.10 (A)	
a652.dscb.akamai.net	AAAA
Answers - 2600:140a::48f6:2b21 (AAAA) - 2600:140a::48f6:2b33 (AAAA)	
secure.informaction.com	AAAA
a207.dscb.akamai.net	AAAA
Answers - 2600:140a::48f6:2b10 (AAAA) - 2600:140a::48f6:2b08 (AAAA)	
ocsp.int-x3.letsencrypt.org	A
Answers - a771.dscq.akamai.net (CNAME) - 184.24.97.217 (A) - ocsp.int-x3.letsencrypt.org.edgesuite.net (CNAME) - 184.24.97.216 (A)	
safe-registration.com	A
Answers - 172.99.100.191 (A)	
a771.dscq.akamai.net	A
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 23.215.131.169 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME) - 23.215.131.176 (A)	
s2.symcb.com	A
Answers - ocsp-ds.ws.symantec.com.edgekey.net (CNAME) - e8218.dscb1.akamaiedge.net (CNAME) - 23.50.75.27 (A)	
pppcw.shieldapps.ml	A
Answers - 37.97.173.64 (A)	
sv.symcd.com	A
sv.symcb.com	A
Answers - crl-symcprod.digicert.com (CNAME) - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
crl.microsoft.com	A

Request	Type
Answers - 23.215.131.202 (A) - 23.215.131.200 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.18.21.226 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.18.20.226 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
76.9187979698	Sandbox	144.76.116.39	443
80.5211699009	Sandbox	69.195.158.196	443
90.3878748417	Sandbox	23.215.131.169	80
97.6835708618	Sandbox	23.50.75.27	80
103.33739686	Sandbox	37.97.173.64	80
103.849877834	Sandbox	23.50.75.27	80
103.875424862	Sandbox	72.21.91.29	80
123.092378855	Sandbox	37.97.173.64	80
148.779680014	Sandbox	23.215.131.200	80
164.84492898	Sandbox	104.18.20.226	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.96035003662	Sandbox	224.0.0.252	5355
6.97356891632	Sandbox	224.0.0.252	5355
6.98036384583	Sandbox	239.255.255.250	3702
6.99124383926	Sandbox	192.168.56.255	137
9.57113289833	Sandbox	224.0.0.252	5355
10.0054399967	Sandbox	192.168.56.255	138
76.5283858776	Sandbox	8.8.4.4	53
76.6774120331	Sandbox	8.8.4.4	53
76.6878638268	Sandbox	8.8.4.4	53
80.2184848785	Sandbox	8.8.4.4	53
80.3716700077	Sandbox	8.8.4.4	53
80.4592218399	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
80.4599430561	Sandbox	8.8.4.4	53
80.6019940376	Sandbox	8.8.4.4	53
80.6022689342	Sandbox	8.8.4.4	53
80.6028249264	Sandbox	8.8.4.4	53
80.6137189865	Sandbox	8.8.4.4	53
80.6417798996	Sandbox	8.8.4.4	53
83.4602408409	Sandbox	224.0.0.252	5355
87.5926530361	Sandbox	224.0.0.252	5355
87.7331709862	Sandbox	8.8.4.4	53
87.7335448265	Sandbox	8.8.4.4	53
87.8054759502	Sandbox	8.8.4.4	53
87.8059568405	Sandbox	8.8.4.4	53
90.255854845	Sandbox	8.8.4.4	53
92.1211760044	Sandbox	224.0.0.252	5355
94.9425868988	Sandbox	224.0.0.252	5355
97.6374230385	Sandbox	8.8.4.4	53
98.4237060547	Sandbox	224.0.0.252	5355
98.489689827	Sandbox	224.0.0.252	5355
100.33285594	Sandbox	224.0.0.252	5355
101.092857838	Sandbox	224.0.0.252	5355
101.11003089	Sandbox	224.0.0.252	5355
103.152148008	Sandbox	8.8.4.4	53
103.81050992	Sandbox	8.8.4.4	53
103.827497959	Sandbox	8.8.4.4	53
143.288633823	Sandbox	224.0.0.252	5355
145.997442007	Sandbox	224.0.0.252	5355
148.580873966	Sandbox	8.8.4.4	53
148.845846891	Sandbox	224.0.0.252	5355
151.524047852	Sandbox	224.0.0.252	5355
154.128706932	Sandbox	224.0.0.252	5355
156.811919928	Sandbox	224.0.0.252	5355
159.502957821	Sandbox	224.0.0.252	5355
162.19451499	Sandbox	224.0.0.252	5355
164.797171831	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8ED B95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** ee4cf7c98d4d9d7e9406174997690bb7 **SHA-1 :** c768babec716a4b20336511ee4dcafcd0c39ed80 **SHA-256 :** 51012914ec503245430f4df71ce9ed1197a4cb0c **SHA-512 :** 81134800bfd2ab4b632e29ccfedfb247af73eedc2 **Size :** 0.342 Kilobytes.
C:\Program Files (X86)\PPC-Software\Ja\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 2aa2f7f7ff0f25ed7ec875fa516011c7 **SHA-1 :** ca759e0182f9a3942153d32440717441a9498be5 **SHA-256 :** b4b04a8ecaa44090879a555797c9e26296ff3ad3 **SHA-512 :** e493a8ced2607665de1cf796a2c1efc24624634a **Size :** 104.448 Kilobytes.
C:\Program Files (X86)\PPC-Software\Fr\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 7342250599b51f2a72e7b6f3dbc4124f **SHA-1 :** b7952d9e1cf99da4477b8303385b546d8658bc9d **SHA-256 :** 3ec0ef2602ee5822686dbe20a481b122f82b7e8b **SHA-512 :** 1ec5cfe607eef615d9ccf377347423931a957e92d **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Sr-Latn-RS\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** aea4abba79df181e43a91a4129dc98ec **SHA-1 :** 9d66fec8b228cd297ae3008c834aed27182a0dd5 **SHA-256 :** 1ae59ec5c2bd0ca8af459a73e4ba65fad5309114 **SHA-512 :** 05ce963d41eb5f168bdd03ada5c6e5324e247aca **Size :** 68.096 Kilobytes.
C:\Program Files (X86)\PPC-Software\DeepClean.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 7402be4396b5f6c6af5b5b9368701e24 **SHA-1 :** 99ecbd51a7be8f919f73a33bad3bb36333dc1707 **SHA-256 :** 9957ad9676638292b792720591193787e29ec04 **SHA-512 :** 0b6e7859349294c116043dbb934c4560f364fc70 **Size :** 157.184 Kilobytes.
C:\Program Files (X86)\PPC-Software\Ja\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 001b9c918a5b4f1bbab58bf90ffb790a **SHA-1 :** a801cd0732a7e621ee1c93fa4b4efff86bcd1449 **SHA-256 :** 70694eae0d024b32cf831b7c479a9ca09912731a **SHA-512 :** eb58f65b4b3de04e1c149ecddcd4470d9e8379ab **Size :** 6.144 Kilobytes.
C:\Program Files (X86)\PPC-Software\InstAct.Exe.Config **C:\Program Files (X86)\PPC-Software\Splash.Exe.Config**	**Type :** XML document text **MD5 :** 0147569a84082745173115350c3e28ba **SHA-1 :** a8c42db365e56a2d3ce19ba062c9c3ad7455fd94 **SHA-256 :** 8bd37a6478c79da70cecccb45d15fb9a2fa841d5 **SHA-512 :** 90e62ae6df3191e21088d06922384f3c78638fcc3 **Size :** 0.224 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Pt\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 96c614f215a77fdaf6b1a0a8bf11a08b **SHA-1 :** af97d15fa4065b136dc1427b5095992eb6c35bf2 **SHA-256 :** 16db7c21be032416d7a80b735ffdff7b087f852a2 **SHA-512 :** 8402f084750e51ea7f9ba9fd1cd04a467b5eee01 **Size :** 5.632 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Places.Sqlite-Wal	**Type :** data **MD5 :** 414dee5eb38ee25e01c4daf7315f04d5 **SHA-1 :** 161c6a9be0222a31e2a58b050d4c000c16180867 **SHA-256 :** 66bb308058c789300ff994c99d74176d23ecb7e4 **SHA-512 :** 4fad91e245218a9769d010d3061936e6c60b4a8 **Size :** 32.824 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Places.Sqlite-Shm	**Type :** data **MD5 :** 6e16c92f097efde8ef21713ca244e9c8 **SHA-1 :** c182a91b4c4ec1407596408ab4790d7d9b8556d3 **SHA-256 :** 5d81ffc894fdd1fdff2a54deef9ce9e58e1b3cc4d7 **SHA-512 :** 2d444c0fbac04c0d6680e5056cfa43dd8c851fd9 **Size :** 32.768 Kilobytes.
C:\Program Files (X86)\PPC-Software\Se-FI\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 2a9cba4324c7aa3cc7850886a9307709 **SHA-1 :** da393e4d21e1802d8ef53708a7b09cdb76c5e297 **SHA-256 :** 56a4f33bbd4a054309da1d665cb8a94cfc69fe1af **SHA-512 :** 5bf53827c37d6177dfa0fd4463e15c81fa80e3bc8 **Size :** 5.632 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\ECF3006D44DA211141391220EE5049F4	**Type :** data **MD5 :** d43fb26775aedd0d49065f37aafd90b4 **SHA-1 :** cfab013b0e92f4b9f2257fc6d1254a59a130966c **SHA-256 :** 576b88470b647e2ab7ebb8ca5b8007337f8a5aa **SHA-512 :** 591b2308b9cdd8d44ec2d8bbf6bdcd1338aeaa4 **Size :** 0.196 Kilobytes.
C:\Program Files (X86)\PPC-Software\InstAct.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** b8637633bddbc51ceaddd1a851259f8f **SHA-1 :** 792eb5dd23ceca95f56a68bbbf1526f84d819f9b **SHA-256 :** b387e8bad56c9ac67fbf9187107fcba7d13526bd **SHA-512 :** fcae902a8a1a014cb1163937bf9981b5f19b792fc **Size :** 26.888 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872 **Size :** 6.509 Kilobytes.
C:\Program Files (X86)\PPC-Software\Fil-PH\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 63ca3044b29694a5657936ba4b31d7f0 **SHA-1 :** 025d0f62d150ab1fc53882e52e224c5f94d07037 **SHA-256 :** c7f51acda9e4ea09bfdf32aedba755a286bb2539 **SHA-512 :** 3a5f1168f54aa8eac55e55036ee6fe32e911866c1 **Size :** 5.632 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Sv\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 0d462b4069272a8d64dc9a3dc1e862b3 **SHA-1 :** 5517ddaf69d26d3d5c7b720344a0b32df349af10 **SHA-256 :** bb060ab99aac6077c287bf10d040812fd7c7ce28 **SHA-512 :** 255b56113690014d217634a90c8dd3207cbdad4 **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Da\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** d9ad8979c33e7c28b2561d9c8f6fa8bd **SHA-1 :** 318b19a4e5153b24e7546ee118e05287a6cbf670 **SHA-256 :** 22bc9ced9ead2150068437f8341967c2a8696ec7 **SHA-512 :** fd524a3e48fc29cdd3f976c4d10b97f101bd5cf9a **Size :** 96.256 Kilobytes.
C:\Program Files (X86)\PPC-Software\SQLite.Interop.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 9b19dcee960dc215e64b1d82348707a9 **SHA-1 :** 9c1e0f76673eb385787120e17404df179316ca2b **SHA-256 :** 3515f704b0012c01fc8be5b717905c0587b29255 **SHA-512 :** cc1304ab171feb2ac6df941f4b35aab8ce7b503f9 **Size :** 811.008 Kilobytes.
C:\Program Files (X86)\PPC-Software\Sr-Latn-RS\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 47ad41fbb7f006ad2dfa1c816ebf412f **SHA-1 :** 7dbe6703a1f246ccc930d2a41549f6b0e04645b1 **SHA-256 :** 46aba2c393be5cf28913bcd6e2a01ca083ad1708 **SHA-512 :** 31ffe1b488340d0ee3e035fdc22b496d4af3475e6 **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\PPC-Software.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** c2845501ac919219bd092d992c369711 **SHA-1 :** a6d57cb5cd2992bcdbcbb403e99881355c054b0f **SHA-256 :** 5d92afcd6e2903c3203176ec2674e7a3f805664b **SHA-512 :** 98814797126ce3328ff921d750c23029681a7bc9 **Size :** 2682.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Bs-Cyrl-BA\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** b3c79e8cadc21bfb302c55fd9df33068 **SHA-1 :** 6c322d9bcaad297c63259ddd23283b52bed04c59 **SHA-256 :** 6a3808f6a7fc374d84e6018ce5f7a6171c574eabe **SHA-512 :** fa65d8a14cb0b364f991930765810d1d63750666 **Size :** 77.824 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:\Program Files (X86)\PPC-Software\Fil-PH\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 721679548e47d84893710e7852494648 **SHA-1 :** 64d13a38d31c790670f6fb5a6d3fc3b1303eb7b6 **SHA-256 :** e14296d42976a57967fbe3d504ea937a664c444 **SHA-512 :** 11e8282aef7ab5360baca83b745f2bf21d98a453 **Size :** 69.632 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Mlogger.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** 6c91ecb87f41159e67970e02e342f4e6 **SHA-1 :** 34f71d6ad5b719d542fa915ea4cbacbef003da66 **SHA-256 :** 5f53d862ab2f8cb58036b9be5a1e063a7af00f21e **SHA-512 :** 2ba7d735fcfe6f3401a2e65992cfff4fe18f22d2801 **Size :** 0.049 Kilobytes.
C:\Program Files (X86)\PPC-Software\It\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 84e74940e6be467328032e0c6a796a39 **SHA-1 :** b2fedacff02457df161a6ef070bfb42945c642c4 **SHA-256 :** a1152b37bd26bacfee4e6f4525f0195d787dcbe9 **SHA-512 :** 5dd2e4aed6dd0314756409f1890c092d9fb8eedc **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Uninst.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 7078291ca670085295de7f42ce5ff826 **SHA-1 :** 8e197ef76333c2e0ac805aac252c2d2adecf75ad **SHA-256 :** 6f0b106a63474339966d38a97bcfc280684d105a **SHA-512 :** f37c0a96cd7bacafdb170b7758347a990a72ed0d **Size :** 136.173 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C46E7B0F942663A1EDC8D9D6D7869173_6043FC604A395E1485AF7AC16D16B7CE	**Type :** data **MD5 :** bf3e1d69cc551ed5bcb5211641e7097e **SHA-1 :** f42844ada1dc5f3f2fa478dec2a0c372b121ceaf **SHA-256 :** 1ac10ed99f882f31470b773642ab92535063d8c1 **SHA-512 :** 90e653a2985fab43c2792870a50ddc09d334c786 **Size :** 1.754 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Entries\9BBE93EE66A24A6574E0B0B292F1184CC816B4A0	**Type :** data **MD5 :** e690126d48fab2163a4dbcedc30194f3 **SHA-1 :** e29ef447e929ad9afe9f49520c251eace6734625 **SHA-256 :** 27abf28d7510f42318bef60988f7b57ad7c786f9c **SHA-512 :** ecbd92739add2e737e42e11ba06f25243421f3df **Size :** 0.265 Kilobytes.
C:\Program Files (X86)\PPC-Software\Ru\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 09570af736831a293577e9388bbf1948 **SHA-1 :** 4d8ea48502a387315b42e623caff9603d3712f1d **SHA-256 :** e18fd23c99e2301e5d3de88a00c3ff9385a3980eb **SHA-512 :** a90fabe282eddf643b4b65c836f64e059c997aba **Size :** 5.632 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 645ccdde38bb039eb271a4f120e6be5f **SHA-1 :** 475a264964d84a2c6c335202262fa6c76275a515 **SHA-256 :** a9b45e98f41bfcc23bc82cf17b3381b9820a2be6c **SHA-512 :** 0f5aa71c7c0b1a574c4a6c306a24006ad175e7c85 **Size :** 49.152 Kilobytes.
C:\Program Files (X86)\PPC-Software\He\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 7c257c6487ba0d0bf1a0c310bfd2b0ec **SHA-1 :** 6d2863607523fe88d84e88f64805f079bc92dc12 **SHA-256 :** a9ca5b62ea695e3ac1f6a8a54963c53cf7f864910 **SHA-512 :** fd169c737ee560c04d5f4775aa6fe6a7c628e7469 **Size :** 97.792 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Ar\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 30e42fee99d227b341cf87098231ed36 **SHA-1 :** 2516a5e9c71dc0bbc12833048c2209e2ace23a64 **SHA-256 :** 313a8d14fa44027349b6c1c855474c0e5f554e43 **SHA-512 :** 55147a81e44f02f5e1380e532583d319320ba414 **Size :** 74.24 Kilobytes.
C:\Program Files (X86)\PPC-Software\Sv\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 2ae1576364d1ef4969b10f2db8a6c6aa **SHA-1 :** 2e8595953b1422e4cb458bbcc9c6a5ce968df8d0 **SHA-256 :** 6d4e6a52d63a0157d0c2e0caa5d2ba22eedf436c **SHA-512 :** 72506f0f985bba40ea9a64cfd7f105b8150d5d2a **Size :** 97.28 Kilobytes.
C:\Program Files (X86)\PPC-Software\Setup.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 7863682083e1e20f0f854cd8ac1be694 **SHA-1 :** 6e138b03b55e52588acfc5bb095ea2182a1e733f **SHA-256 :** 1765153a2fb05500242abe32f45f0172aa7ff57a6 **SHA-512 :** d056da0def7896f8de1cbf557278046d6ae7f05b **Size :** 87.552 Kilobytes.
C:\Program Files (X86)\PPC-Software\De\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 71632cd50823c98621098d4f194ba732 **SHA-1 :** ac027fcb98b3f8900692d5c7518e388309a27d7b **SHA-256 :** 72ae3535066d9fdef84d9a5ab136550ae2978a7 **SHA-512 :** e65fd3c8c4428ff32005df0c01542a69e973112c0 **Size :** 99.84 Kilobytes.
C:\Program Files (X86)\PPC-Software\Pl\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** d7c209ab273ad138f339469afde3fe05 **SHA-1 :** c810fc490cb97f0865d7fdd558936225558a8246 **SHA-256 :** 4bce6bc6811746e2c6e459a27cb89f4d74fef6cb5 **SHA-512 :** 30f4b45d890246e286f20857e2c367bb22d6f41c **Size :** 5.632 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 :** fb168db35a2f660de021b8e3a1f9297ee5b11fc5 **Size :** 10485.76 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PPC-Software\PPC-Software.Lnk	**Type :** MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Wed Mar 30 03:20:36 2016, mtime=Mon Aug 13 20:51:07 2018, atime=Wed Mar 30 03:20:36 2016, length=2682632, window=hide **MD5 :** 04e8ab07521de7f0ba5b9ec27cbbea19 **SHA-1 :** 2b2fb09409d7c32cd3b8ead0501515087dab6216 **SHA-256 :** cb312e51713141d2465ed2a7fa8a7fb6a165ef64 **SHA-512 :** 15f07343dd62427051418ef5f07cc84d951a7c7a **Size :** 1.091 Kilobytes.
C:\Users\User\AppData\Local\PPC-Software\PPC-Software.Exe_Url_1xuetxnfnbprkyvp4f3fgknib3pg5muj\3.1.5.0\User.Config	**Type :** XML document text **MD5 :** c3712a40a97b4ca4d23d92e582c3ab19 **SHA-1 :** 3129333c2c32a7238570e57c348b3e9e9963ca2c **SHA-256 :** e39c48e501f99cf9c50fba3d74c105d55c42fc766 **SHA-512 :** df184a90728c0f251c10d5db10cdc4f675dcd8e4 **Size :** 0.319 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Hr-HR\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 64a2f189a7c15e4cc5625f3e56de131d **SHA-1 :** 07a8da2dd1cfbf06e92665b311d9ae21a1fb8b39 **SHA-256 :** 28782e257ce52e01ce50f8f7c7c44bb5b5208956 **SHA-512 :** db1da2ca8fd53c0e34b89a1ee8a660f3c08133c2 **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Azurant.Ini	**Type :** ASCII text, with CRLF line terminators **MD5 :** 5f1c9b49b5ad604357d8ae38b196719e **SHA-1 :** 63a804898303fb3ef2fee1c064316c72b3b4417b **SHA-256 :** 3f33ddaeebdada07eac2ef7f097409ff4093d1994 **SHA-512 :** b2c90efa58687a29f2b369aa65ebb594e55896b2 **Size :** 0.391 Kilobytes.
C:\Program Files (X86)\PPC-Software\Tr-TR\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 52505d999335777d6dec7a2ba3ada14b **SHA-1 :** 416bbd2d32c03c10f625f699a68ce06917152c92 **SHA-256 :** 6d4b651a589c79c5c987ddbefd983428bba44d7 **SHA-512 :** 90817d30e89d821f89a7907b2cda87955e9def18 **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Bs-Cyrl-BA\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** d310e412931fdfcf5c60898a583585a5 **SHA-1 :** 891191190664a160c5c279b3d06f09c9bfe6cd73 **SHA-256 :** 892451c172a9816d0d6f14178c6b144421c5366b **SHA-512 :** b350b5766ec1db996b5d97d716e6b48460b13c0 **Size :** 6.144 Kilobytes.
C:\Program Files (X86)\PPC-Software\Interop.Shell32.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 519c268e7e9ea8f2b7dc42485c3691a8 **SHA-1 :** 0c18b58151dab94a461b1167cb958c1ebdd878fa **SHA-256 :** 5e46ce9fda7c173b4a789acf880aa8f26682f7cd8 **SHA-512 :** f6070dfaaf71cc540695183b218342d24b9beded **Size :** 49.152 Kilobytes.
C:\Program Files (X86)\PPC-Software\Es\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 80b68cd5b27e96a49cf29cdbc7ab18d9 **SHA-1 :** 9ab71e34e2960c5d1e408fce94e6fbb101097e49 **SHA-256 :** 2e78dec8bbec8521895c6d14ae30123565709641 **SHA-512 :** 51dc0e1ad7c36b39f06f6966779564eebfffc5030 **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Pl\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 1ca25fed7efa6d04819577fbb321745b **SHA-1 :** 2cae9afac087bfd9c76441c3e7e3d82fa1c2e5b4 **SHA-256 :** 47bb412f561cce5ab14971bccb643e59c4ea3b46 **SHA-512 :** 45d8d0e6ec46daa386c4b8fc4ca6191a5f9cf025a **Size :** 68.096 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Pt\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 72ad3c7e1b1c2d5324a485f00dd6228e **SHA-1 :** c29f30155011940f07406b757f2ca374d352cc12 **SHA-256 :** 82a2d5bf49dd35a4c7f1d9126d5b34bba063173 **SHA-512 :** efc579432fa254dd01c1eb56a3a0a353e742a29f7 **Size :** 68.608 Kilobytes.
C:\Program Files (X86)\PPC-Software\Nl\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** ea1a955abaa0fc115390e5ab34eeaeb2 **SHA-1 :** b2aebea8614f22ad295a8e1a1ee930bea6ffe6ba **SHA-256 :** 14a3347bc214505f920e01cbd49b3a1cba1c5d75 **SHA-512 :** fd4eb2a770cfcb6dd1ba10316da059566dcbca09 **Size :** 97.792 Kilobytes.
C:\Program Files (X86)\PPC-Software\Da\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 9f184a80dd792f9773dbacf018a153c3 **SHA-1 :** 6f5f87aaf6834f3440db24cfc5f679393e9ba2ec **SHA-256 :** b4f7af692ad1978647f7f03b10a1771abd94b337 **SHA-512 :** 51321981707d1ed900a3d925832342ad71df19b **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Bs-Latn-BA\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** f339bd08a609d3bcdefe61740ac2aefe **SHA-1 :** 901cf4ea5feca24553b972c01b4385e7b51c2be9 **SHA-256 :** 4fb65a2fae8d8c8241f27097026aa8cc588b717d5 **SHA-512 :** b2aa6d1ea2048e8af90f4b8ba65879ad1210c8bc **Size :** 68.096 Kilobytes.
C:\Program Files (X86)\PPC-Software\No\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** d92ee406bc63b95e546abcd48edb33e8 **SHA-1 :** e731163ba67dcd56805a766230ad70104999041a **SHA-256 :** 8e2bb607f68c643f2ac1aff85c81d15c03e523114 **SHA-512 :** b136cbff68889211c976009f06b08c0340be2bd84 **Size :** 5.632 Kilobytes.
C:\Users\User\Desktop\PPC-Software.Lnk	**Type :** MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Wed Mar 30 03:20:36 2016, mtime=Mon Aug 13 20:51:07 2018, atime=Wed Mar 30 03:20:36 2016, length=2682632, window=hide **MD5 :** 22b9fc017577fd4128f27be8ed50f38a **SHA-1 :** 5567a7d04972d295eeb8f0ebcb7cc328f5cc7b54 **SHA-256 :** f9c20d3430d178b110544f16048fdca4e1b3327e **SHA-512 :** f8d99555ff96db542ed638b93a051c61f53be13e9 **Size :** 1.055 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Entries\22C955F323F4044E1C686B6BB4753BAE19159E53	**Type :** data **MD5 :** f4749d4ef0f3d7ed8b7883c805e104c8 **SHA-1 :** fe479d80e39549dac1aff04657e5917a536378f0 **SHA-256 :** affea219eee3cf7efafe7fd2a1f71e3095e0ca66a5 **SHA-512 :** 738603232d20d86a4b9199f9824443ebc66da1e **Size :** 0.108 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Ru\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 653fd471c8c5731315dd7c3d7c5481eb **SHA-1 :** 616172fcb9495d2b04165531bc56937434eaed7a **SHA-256 :** 8b01d77163f5c662b74c4c3836cf19baa18cfbced **SHA-512 :** 6d51febaabf0154a1a4c5c47d251861681ceaeaa **Size :** 79.872 Kilobytes.
C:\Program Files (X86)\PPC-Software\System.Data.SQLite.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** dd3d6f00b1aba3f1d9338d9727ab5f17 **SHA-1 :** faf9364a7ab15f27c93a6e6f97fa025030c9dad7 **SHA-256 :** f0d4beab24e94e61f219df451d90dbba3d0f4853 **SHA-512 :** 0794d850a133a98affe627e3023114b229b982e5 **Size :** 262.144 Kilobytes.
C:\Program Files (X86)\PPC-Software\PPC-Software.Exe.Config **C:\Program Files (X86)\PPC-Software\PPC-Software.Vshost.Exe.Config**	**Type :** XML document text **MD5 :** 33305e2379fd2431cd4c4afb45270904 **SHA-1 :** 8b3949d6022fcab6f97b995229e62891544ca246 **SHA-256 :** 90568f87ed3b0f2e30794766fd9179d78f6c79c17 **SHA-512 :** f0ff81e8a77bc1d2f8265974fb9db1bb8eadec36b **Size :** 6.355 Kilobytes.
C:\Program Files (X86)\PPC-Software\Interop.IWshRuntimeLibrary.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** e326a04d6ed0b10a570ed430d5145d5a **SHA-1 :** 7066df0011d90e54ead9b080ab05dd041fd3825e **SHA-256 :** 918e48c361152b61b0f9b9a696f6ba09ae4485d2 **SHA-512 :** bc24ad636707ce35c7afca001cf8a90e741b6ad6e **Size :** 49.152 Kilobytes.
C:\Program Files (X86)\PPC-Software\PPC-Software.Vshost.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 06fae0e5310fd28f842bde1fc9ee67a7 **SHA-1 :** 3ec631ab4b8f48d23fdef07715d73d4e4e98ee1d **SHA-256 :** 10318a11a37feaedfff671563c9c7d06ca12b6af95 **SHA-512 :** 18d8748d95f25db287da076006b0f3c8a0d06c23 **Size :** 21.656 Kilobytes.
C:\Program Files (X86)\PPC-Software\Tr-TR\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** b59932884c098b68ecd0849feaadfa7d **SHA-1 :** bd04ad6c4405b8152218f9d8368621b9b891afc8 **SHA-256 :** b64b5a688b62c4c0fe2c2039dd66bf2a635b1c6d **SHA-512 :** 190995a195999da98ffabfd0ded80991eecb4e4fe **Size :** 68.608 Kilobytes.
C:\Program Files (X86)\PPC-Software\No\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** e0fb29264c1bbfc0356017059cec9353 **SHA-1 :** 3ba5f7b880a54d8624d6ffa99fbbd0e62ebd4822 **SHA-256 :** 43a04eb3132aaec570e08fe3f5f0eaba2035c48b9 **SHA-512 :** 43f8da054539e8cc95cbf8c129c44a37b9a0b2528 **Size :** 97.28 Kilobytes.
C:\Program Files (X86)\PPC-Software\DeepClean.Dll.Config **C:\Program Files (X86)\PPC-Software\Setup.Dll.Config**	**Type :** XML 1.0 document, UTF-8 Unicode (with BOM) text **MD5 :** 2b501716c1274b0b35543316b410d60c **SHA-1 :** 69e370e1522eab2f66ff11238984a3f288eb7a9e **SHA-256 :** b4daa280754f634f0c289eb06538ad00d6f6bff81 **SHA-512 :** e38523eabe64e4b17cb6d45df7726bdd5b40efc3 **Size :** 0.227 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Sr-Cyrl-RS\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 454b035dc1964ebc40bca6294b01a740 **SHA-1 :** db5d921c873d23151d00f5b118c871450da7e390 **SHA-256 :** 8eba9d86729ec868055cf34d784bbf11ab9b5027 **SHA-512 :** acd0b6a9508e322fa43a5fa9f090e1857b4ae008f **Size :** 6.144 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\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** de20f795b0ea29cbcb8daf8951530db4 **SHA-1 :** 81d7e8a0197a0ea9eba76e4dc856d10aa5ec04d9 **SHA-256 :** f891c989c74d22028cc0dfcd564c186fe6857592c **SHA-512 :** 06ed0fdb0abfcdbc16a7f5adb92ed0c59ba788f08 **Size :** 180.224 Kilobytes.
C:\Program Files (X86)\PPC-Software\Nl\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** ae04439b5b4f673f35ec39b0c50ff3b7 **SHA-1 :** 2dd0915e1b2dfe0d23a32cffa760a3352f420dd9 **SHA-256 :** 775c289a4a0aa328c099aa0b7e6eec6ae54ff49a0 **SHA-512 :** efb68f99c5edba4c06f2c92f10ac1f07ba2d07124e **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\Hr-HR\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** c46f5a067a59c1aa76e907a84d198151 **SHA-1 :** 7d8543d1b894ebcade2469104448b0ff7ac47aba **SHA-256 :** 5772d54e60d841763154aab070fdf1e17fbd3185 **SHA-512 :** 98c272b64194f266cd4a5998e303ed86ae33b133 **Size :** 68.608 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsa22EB.Tmp\System.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 883eff06ac96966270731e4e22817e11 **SHA-1 :** 523c87c98236cbc04430e87ec19b977595092ac8 **SHA-256 :** 44e5dfd551b38e886214bd6b9c8ee913c4c4d1f0 **SHA-512 :** 60333253342476911c84bbc1d9bf8a29f8112077 **Size :** 11.264 Kilobytes.
C:\Users\User\Documents\PPC-Software\Logerror.Txt	**Type :** UTF-8 Unicode text, with CRLF line terminators **MD5 :** b0dbcfdd88cd2781256754cc18c1c847 **SHA-1 :** 011a31b4a06f87eac92b2f1f634e761cd61eeeb4 **SHA-256 :** 1336cd689e12db48a37d398374093c1be5554eb **SHA-512 :** 0121252e58c503a75d717b0f3901a41d7d54b43 **Size :** 0.362 Kilobytes.
C:\Program Files (X86)\PPC-Software\ComponentFactory.Krypton.Toolkit.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 4aa46ecabd3073852f3a778d28d9edae **SHA-1 :** 0011708b8549bfbcbe0596c7a9459d61b072d16f **SHA-256 :** 956ad7e5c070ee129e70a3e7f5d44038d5bb43a **SHA-512 :** 08c025d77fc5e1936b2dd695dea1d4533e3f98e8 **Size :** 2667.52 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\Th-TH\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** ab0a027c724035dd10166566f84fc609 **SHA-1 :** 2f008d346f6a482bcd5f5afe99b0886227e25bd7 **SHA-256 :** 2873337d0975b8998b51e1e9da835172d32b5cc **SHA-512 :** 984180907c01c49d268a8c576b88eb7b8f88407e **Size :** 88.576 Kilobytes.
C:\Program Files (X86)\PPC-Software\Bs-Latn-BA\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** e804b582583f4a4d1fdc9b0a93555dd0 **SHA-1 :** 5df764701f7b4122dbe2685d39a35e02dd0d95d0 **SHA-256 :** d1c64104a081d5de868a3ed548ec3fedbfb81a72 **SHA-512 :** 796487ae0dc1883cb29fd51f9b129e8400b1eaf9 **Size :** 5.632 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C46E7B0F942663A1EDC8D9D6D7869173_6043FC604A395E1485AF7AC16D16B7CE	**Type :** data **MD5 :** 025988936405c0ef3a4873dd7a1d8f75 **SHA-1 :** 7b7eefb6a199e433fb9f62abcaa020c8cfe9f566 **SHA-256 :** 4eef3b72edcb7c765e6d884365ef57136ec36282 **SHA-512 :** 40d411cd61f7fbe79ceff7f02bfa198631cc396db7 **Size :** 0.398 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Entries\B1BF484310B181937E88AFC02D2B2F23B1FBCC38	**Type :** data **MD5 :** 9c308024c1be339bce3c466ad51cfce7 **SHA-1 :** 47c1ccced2a570d8bd5304a6311007f2420c788b **SHA-256 :** 696c29ed26209ac244806cfb34609b334569c928 **SHA-512 :** f33787ed8ca0815fc9da1dab43012405ed554749 **Size :** 2.621 Kilobytes.
C:\Program Files (X86)\PPC-Software\Th-TH\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 2c6c4c910458eab15427ad5ea48f4c9a **SHA-1 :** 1d59e68d61eb9e4f9cb18fc03e8347e8f1d0fed2 **SHA-256 :** 1e80f6bbef542a686b1115c33d122371deb119e4 **SHA-512 :** 0da954917add1d433aa2396158d049054a744e0 **Size :** 6.144 Kilobytes.
C:\Program Files (X86)\PPC-Software\Ar\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** cce59604ca991bb2bd44de559b187621 **SHA-1 :** c6052364d6bd6fe080bafc80b028e0a387512ae6 **SHA-256 :** f0f9dcb1c766884949a6f1b54b1202f91607613c5 **SHA-512 :** 6beb058b6718769d1f8148f1043801e3b5f90768 **Size :** 5.632 Kilobytes.
C:\Users\User\AppData\Local\GDIPFONTCACHEV1.DAT	**Type :** data **MD5 :** 696bad2ef23da7f0ccaaa7f76ab9fdf0 **SHA-1 :** 0efe907b47e8331cf56a95c0c06d324257ece202 **SHA-256 :** bd27979561fac15e4043fc980ad62f24f00738cba **SHA-512 :** fb1a4afdbf5f9e3d7e55eb806f660057927d6c357 **Size :** 84.528 Kilobytes.
C:\Program Files (X86)\PPC-Software\ObjectListView.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** d212910c8f5c65597651bd53d377f764 **SHA-1 :** cc1d84057c62c74fd08f7aac35eb5a5142cb6dae **SHA-256 :** 3c49c71d5297ab029eef1d3e79dad33d5a8f7e33 **SHA-512 :** ec7692e6c70364d88b1a60a1d076d7224323b6d **Size :** 414.72 Kilobytes.

FILE PATH	TYPE AND HASHES
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:\Program Files (X86)\PPC-Software\Azurant.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** ea86538422597eb9776850b827a9567d **SHA-1 :** 8dd01487e5836a13b372665a3c70c0f78c4a1d59 **SHA-256 :** c345b99e420023d6d07f2d7a97a1d61edc79ce0 **SHA-512 :** be2f85d107c3472c9c5d2afcc5717541b7f446712 **Size :** 436.488 Kilobytes.
C:\Program Files (X86)\PPC-Software\Es\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 996acd2216a92f78731d1362e40d1f63 **SHA-1 :** 142e0e56dfa6fa0c9651e147c9f7ada236ae4c92 **SHA-256 :** 8c6244d6e59de4cbdcaf46e983851a7e37de2203 **SHA-512 :** 7a8454a3212af7e7847bbbccceb396fe82e4f02ba **Size :** 99.84 Kilobytes.
C:\Program Files (X86)\PPC-Software\It\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 88ec962a5bcbfc66ba8a6f89c30729ff **SHA-1 :** 4ae1de1306bed201384788fe343ccd8d0b6169bf **SHA-256 :** e6b47d4efd2968278b368a6aa0facf3d557e866e **SHA-512 :** 48be830df4045aefb1495d2c19cb146d0782e381 **Size :** 99.328 Kilobytes.
C:\Program Files (X86)\PPC-Software\Se-FI\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** d406a529bb1e70b13a67cc7c95fb9c0b **SHA-1 :** cc037127e158955d1799ee6286d5645fad32913e **SHA-256 :** d1094877986aa3d691a3e465c39952eceae8223 **SHA-512 :** 187c7cef9e2dbacfdf392d0eee99892c52318d918 **Size :** 97.792 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EA618097E393409AFA316F0F87E2C202_8A8062BDC796C6D25AAA0A50DD4B6113	**Type :** data **MD5 :** 03745e6a37452e42449d23c6812fc6d9 **SHA-1 :** c20c5cff81b19af883346c7d091b66c76bc80e1c **SHA-256 :** 5c8909f4a8d6e0cdb7f30b39bd2bf1e454d6202e **SHA-512 :** eb4a02b511cd27cb1b698e484e83b127fb2ff0b2 **Size :** 1.611 Kilobytes.
C:\Program Files (X86)\PPC-Software\PPC-Software.Vshost.Exe.Manifest	**Type :** XML 1.0 document, UTF-8 Unicode (with BOM) text **MD5 :** a5fb681350eb8f7d8fd01e830997c8f3 **SHA-1 :** 88bb5e8333296d9a158749bb79d87bb05e908476 **SHA-256 :** 5ffc2af37095403981fed86092583051b766fd81f **SHA-512 :** fb321bbf19d482f53c5879c2e5b61e51b6141fc84 **Size :** 1.486 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Prefs.Js	**Type :** ASCII text, with very long lines, with CRLF line terminators **MD5 :** 8fa363d509d00d8c5ea08978d742cfa0 **SHA-1 :** 6baa95f3cd176437497678c18c7b210ef0a63855 **SHA-256 :** eda912afd8d6d613552673dcca678901cb45ff8b **SHA-512 :** ffb835afeb06b55ef53b3e1353acb46cedfdfc1a9b **Size :** 16.074 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\ECF3006D44DA211141391220EE5049F4	**Type :** data **MD5 :** ba5ff8792a7f20168c7cd73962401350 **SHA-1 :** 1bfcbde6200411ed6aabccf3a793e90c068af375 **SHA-256 :** 9c5653b6b6700943d0083206f7c0cb655780cd09 **SHA-512 :** d97a201007a623eae1c857060b30c22c1fad5f23 **Size :** 59.38 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 2ed7b584633888df7f0114fa4ac6dc69 **SHA-1 :** fa8067b3241b8d9258d9fc88f5bd80fca5433b10 **SHA-256 :** 69a0d29dc846c82d785231dbf94e4c4b731ad588 **SHA-512 :** 678165bd37def22a10615aded1384e97413fce1f **Size :** 32.768 Kilobytes.
C:\Program Files (X86)\PPC-Software\Fr\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 1de1ca551e96ac65b2e05fb70ba52061 **SHA-1 :** a5b0550d3c28f3488a4ee1ac36de5fa43e643cde **SHA-256 :** 104614f9daad19f904d6ad4d86a58f93c9e09adc5 **SHA-512 :** 98ff1043134ad2f03579abd56766b69a4fd873467 **Size :** 100.864 Kilobytes.
C:\Program Files (X86)\PPC-Software\Splash.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 5e5d678bca3ea4efcd9cc2468e354634 **SHA-1 :** a7b1a8edbbe94e189c0171ce70f8d53dd24f94f6 **SHA-256 :** 8b7590f50df3bf282a4a7ff1b9682d4e7ba975668 **SHA-512 :** a59bd2ef9d3c43876b9a5aaf1e152f900b1d7308 **Size :** 265.48 Kilobytes.
C:\Program Files (X86)\PPC-Software\LinqBridge.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** b1d401765196dddc72cd1341a684debc **SHA-1 :** e02bce01f4efd3a1e34edab54a55832fca9ca5cf **SHA-256 :** acb589d7708040e016cf3f25dfc3309d2366a58c8 **SHA-512 :** 893fdc5c009fb6826228f3ddcea9195cb235feec4 **Size :** 62.976 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EA618097E393409AFA316F0F87E2C202_8A8062BDC796C6D25AAA0A50DD4B6113	**Type :** data **MD5 :** 6e5399545cdca5848b821447ed90fa15 **SHA-1 :** 39cfbbc1518d2f2f5fc3e666f33df818d22d25e3 **SHA-256 :** 96bc00b98eb90544c2e044eafce60a95d04f8557 **SHA-512 :** 5d462c5ce4813f0de23107bdcc51095f76b7b96b **Size :** 0.406 Kilobytes.
C:\Program Files (X86)\PPC-Software\Microsoft.Win32.TaskScheduler.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** b72060fc6231f4a67523726bfca497d3 **SHA-1 :** 7e17f141b90f4953081a2d2280c33dc874150929 **SHA-256 :** 69706722182c176e554276c491cf2086732e9879 **SHA-512 :** 9c94450c04b11b34e6e9b6e5ec63697f131fdd87 **Size :** 322.56 Kilobytes.
C:\Program Files (X86)\PPC-Software\Sr-Cyrl-RS\PPC-Software.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 149a7e60163a3355187ef04b3146dad7 **SHA-1 :** 73febc8c7bb906e20060076fa28ef4fd2b3d580c **SHA-256 :** ffcc03270c55635a637e5553c9664c973acf248e7 **SHA-512 :** 193bda42fde2017b6b494cf7e254d587ffb59cc02 **Size :** 77.312 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\PPC-Software\De\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 95da56e0fd1e2c74dabb23c7865d56db **SHA-1 :** f7cec4eef5d25d463562c0e06741ef3d6b317cba **SHA-256 :** 81434b86ab06619cd01caa2009788a6f8ba8cd8c **SHA-512 :** f66a6d0338ac8c2b9cf59629b6e34c8bf2e08632b **Size :** 5.632 Kilobytes.
C:\Program Files (X86)\PPC-Software\He\Splash.Resources.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** c93a6cf166c0975c4d75ad54456cb97e **SHA-1 :** 500fb411e983e099cdd13401a5845d74f0f58ca7 **SHA-256 :** 603d2abc1131143bb4a35dfeee241eb1cf168ca0 **SHA-512 :** b7f51b2f43f860bd603004d26ca1022ca92ecd0bb **Size :** 5.632 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Index	**Type :** data **MD5 :** 837c3d9b6b1066a745fa37ffab967676 **SHA-1 :** 0e3a3e90a25c1aa00225f26911fb12e016296f79 **SHA-256 :** 0b512079376281679ef6687dd5df1986f54d63c9 **SHA-512 :** 45fb626839db7c051fda844ec679e0d53ebbe081 **Size :** 9.484 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\SiteSecurityServiceState.Txt	**Type :** ASCII text, with very long lines **MD5 :** aaa47fcb4e9fc2723e4b55781c6c79bb **SHA-1 :** b5242d440a8f636ccf57c51eabb12bd8f974d150 **SHA-256 :** 0c72b7902ec8276f207881d0f62069d314cfd3287 **SHA-512 :** d883b3f85928381b315201299b7fc8ecf8da959d **Size :** 2.031 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 :** 78173b57c2269495264db6b96c3397dca31bca7c **SHA-512 :** 22b02e96ac16cac9fd8eeca2caf0ddf0736d3e6b3 **Size :** 163.84 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	A0017793.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	50b322435a8475c50d5a3ac96e49bb2afb88cc5c
MD5:	136b7535bad1fb83fed047becd96e6cf
First Seen Date:	2016-06-24 00:32:39.387943 (3 years ago)
Number Of Clients Seen:	9
Last Analysis Date:	2016-06-24 00:32:39.387943 (3 years ago)
Human Expert Analysis Date:	2019-01-20 14:13:52.569458 (5 months ago)
Human Expert Analysis Result:	PUA

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	5
Compilation Time Stamp	0x54336EAA [Tue Oct 7 04:40:10 2014 UTC]
Entry Point	0x4030b6 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	3507176
Sha256	29cd4428b4ae3253fd3ddc1958b4d608240dcfbde0bc07170a9aea7ed22bbc04
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x5a7c	0x5c00	6.422249	-
.rdata	0x7000	0x11ce	0x1200	5.235583	-
.data	0x9000	0x1a7d8	0x400	4.963740	-
.ndata	0x24000	0xb000	0x0	0.000000[SUSPICIOUS]	-
.rsrc	0x2f000	0x19118	0x19200	3.668536	-

CERTIFICATE VALIDATION

- Success ✔

[+] Rainmaker Software Group, LLC	
Status	NoError ✔
Start Date	2016-02-24 00:00:00+00:00
End Date	2017-02-23 23:59:59+00:00
Sha256	e5d98f1be2479f685e977ecdb780f6f2f09c66dea56da27dd583286051447d19
Serial	6965CEA97169855608F566F8E1C033F3
Subject Key Identifier	af 3a ac e4 14 f2 d4 28 ec 8b 63 27 67 de 7d ea c9 fe 73 36
Issuer Name	Symantec Class 3 SHA256 Code Signing CA
Issuer Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca b7 86 1e 72 66
Crl link	http://sv.symcb.com/sv.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

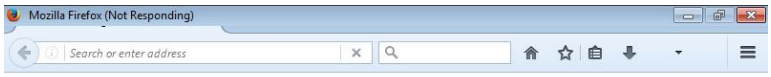
[+] Symantec Class 3 SHA256 Code Signing CA	
Status	NoError ✔
Start Date	2013-12-10 00:00:00+00:00
End Date	2023-12-09 23:59:59+00:00
Sha256	0649cde463467e8e26bb6b7c23965e030248f95df21f6dcf28c51507fbb77c08
Serial	3D78D7F9764960B2617DF4F01ECA862A
Subject Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca b7 86 1e 72 66
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Crl link	http://s1.symcb.com/pca3-g5.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

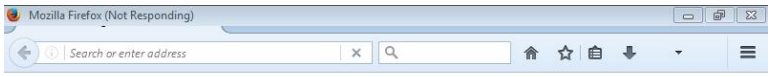
[+] VeriSign Class 3 Public Primary Certification Authority - G5	
Status	NoError ✔
Start Date	2006-11-08 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7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

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

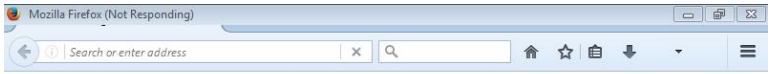
[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 00:00:00+00:00
End Date	2020-12-31 23:59:59+00:00
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	undefined
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl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

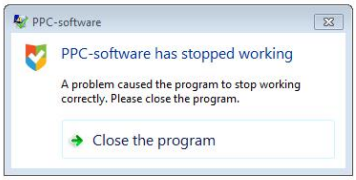
SCREENSHOTS




Mozilla Firefox (Not Responding)
Search or enter address

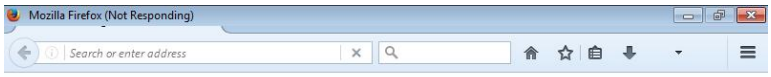

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM


Mozilla Firefox (Not Responding)
Search or enter address

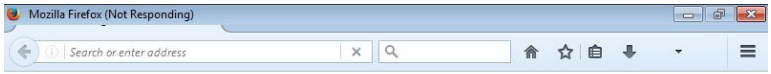

PPC-software
PPC-software has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program

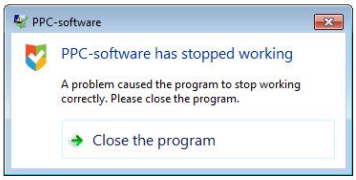

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
PPC-software
2:53 AM


Computer
PPC-soft...
2:51 AM

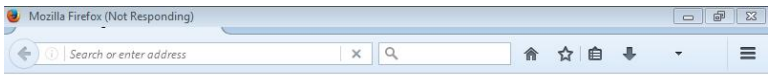

Mozilla Firefox (Not Responding)
Search or enter address

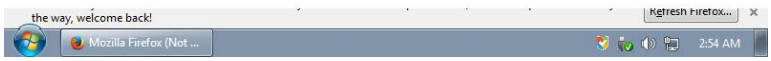

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM

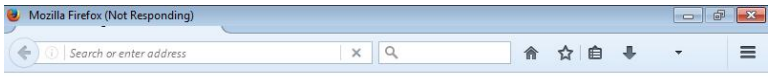

Mozilla Firefox (Not Responding)
Search or enter address


PPC-software
PPC-software has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program

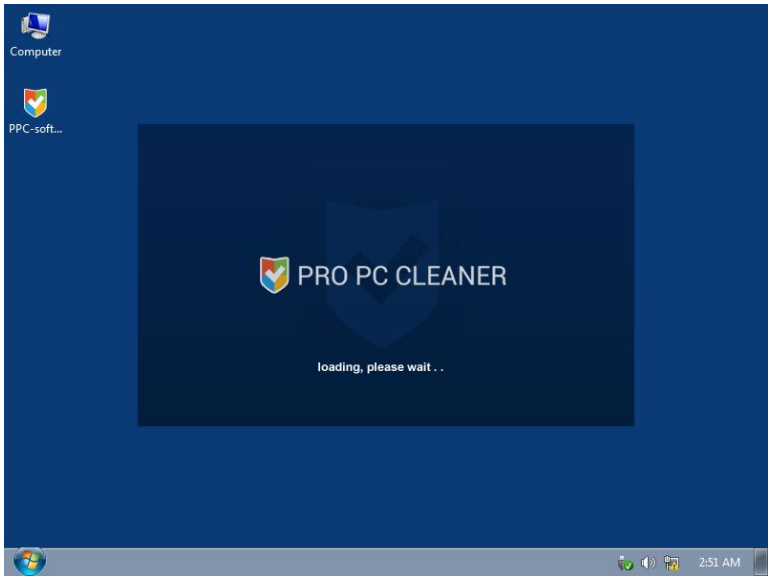

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
PPC-software
2:53 AM

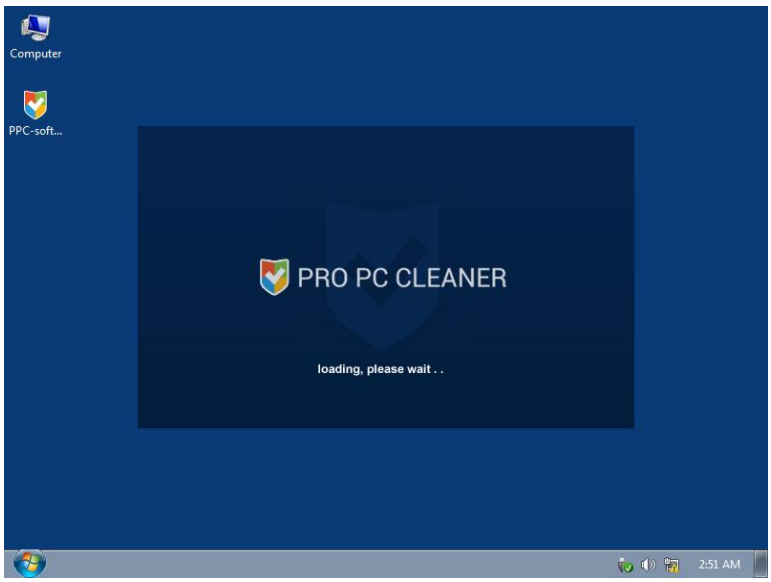

Mozilla Firefox (Not Responding)
Search or enter address

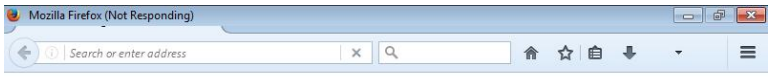

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:54 AM


Mozilla Firefox (Not Responding)
Search or enter address

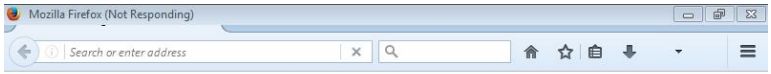

the way, welcome back!
Network 4
Internet access
Mozilla Firefox (Not ...
2:54 AM


Computer
PPC-soft...
PRO PC CLEANER
loading, please wait . .
2:51 AM


Computer
PPC-soft...
PRO PC CLEANER
loading, please wait . .
2:51 AM

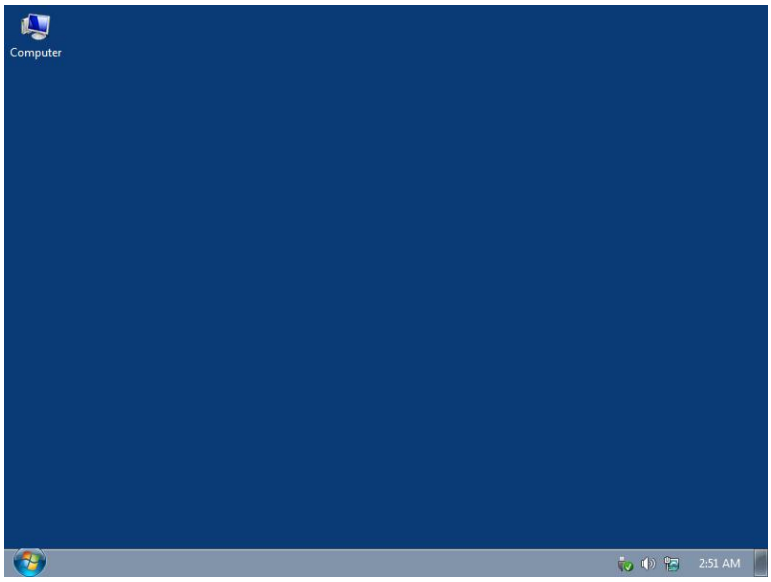

Mozilla Firefox (Not Responding)
Search or enter address


the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM


Mozilla Firefox (Not Responding)
Search or enter address

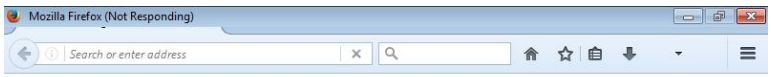

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM

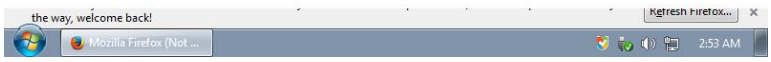

Computer
PPC-soft...
2:51 AM

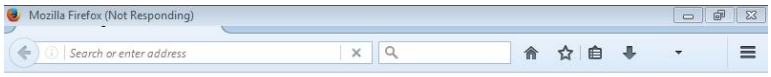

Computer
2:51 AM


Mozilla Firefox (Not Responding)
Search or enter address

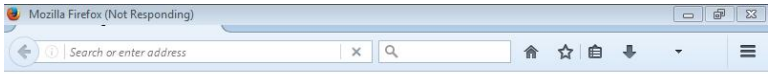

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM


Mozilla Firefox (Not Responding)
Search or enter address

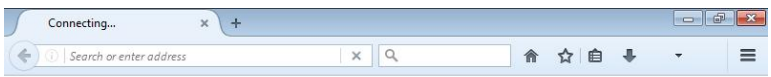

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM


Mozilla Firefox (Not Responding)
Search or enter address

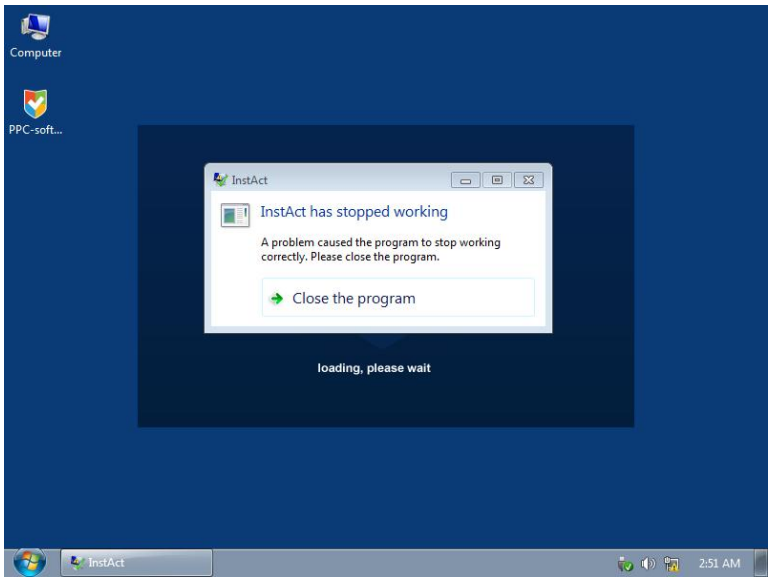

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM

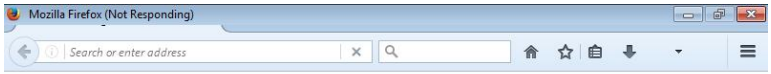

Mozilla Firefox (Not Responding)
Search or enter address


the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM

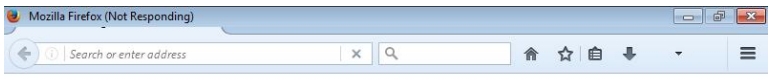

Connecting...
Search or enter address

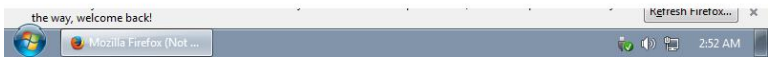

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:52 AM

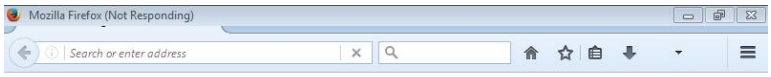

Computer
PPC-soft...
InstAct
InstAct has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
loading, please wait
InstAct
2:51 AM


Mozilla Firefox (Not Responding)
Search or enter address


the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:54 AM

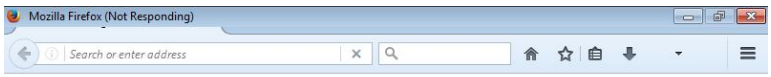

Mozilla Firefox (Not Responding)
Search or enter address

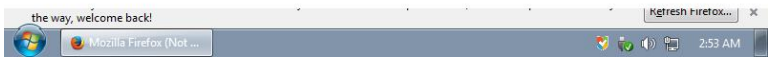

the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:52 AM


Mozilla Firefox (Not Responding)
Search or enter address


the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM


Computer
PPC-soft...
2:51 AM


Mozilla Firefox (Not Responding)
Search or enter address


the way, welcome back!
Refresh Firefox...
Mozilla Firefox (Not ...
2:53 AM