VALKYRIE COMODO

Summary

File Name: DriverPack-17-Online_903364983.1505480122.exe

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

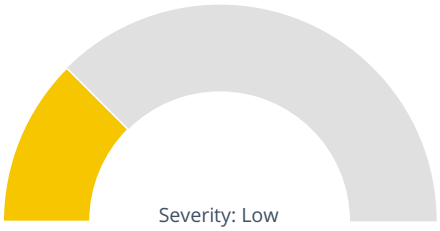
SHA1: 332c6d7a41782059a0ce7bb28047a76f91b34a98

MD5: 8cf070e06d243b0966fed6bb24c955b2

PUA

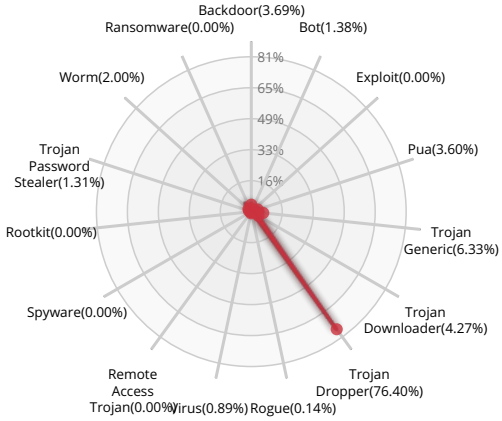
Valkyrie Final Verdict

DETECTION SECTION

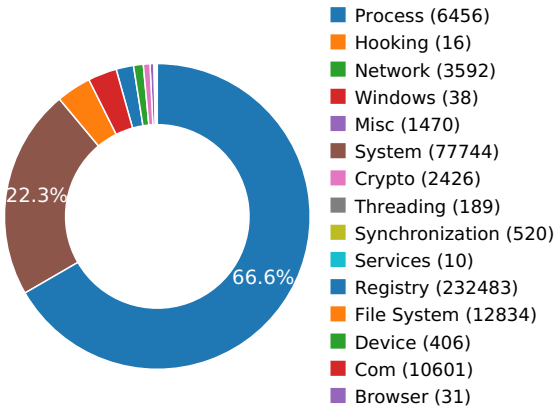


Verdict: PUA

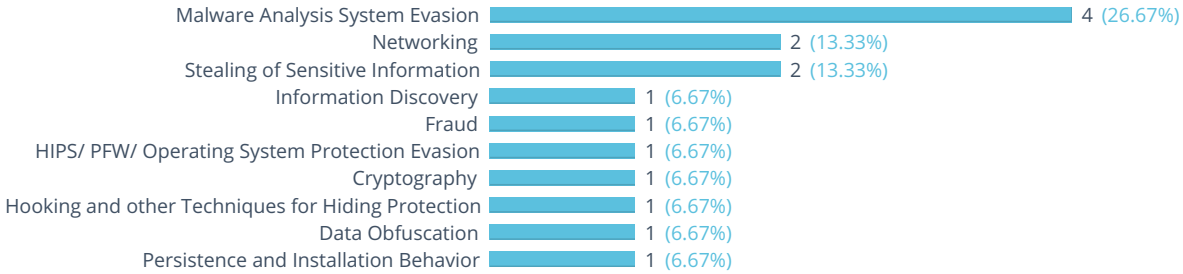
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

FRAUD

Attempts to modify browser security settings — Show sources

NETWORKING

Attempts to connect to a dead IP:Port (8 unique times) — Show sources

Performs some HTTP requests — Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory — 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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Attempts to interact with an Alternate Data Stream (ADS)	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects VirtualBox through the presence of a registry key	Show sources
A process attempted to delay the analysis task by a long amount of time.	Show sources
Detects VirtualBox through the presence of a file	Show sources
Attempts to repeatedly call a single API many times in order to delay analysis time	Show sources

VALKYRIE COMODO

Behavior Graph

07:35:04 **07:37:04** **07:39:04**

PID 2476

07:35:04 **Create Process** The malicious file created a child process as 332c6d7a41782059a0ce7bb28047a76f91b34a98.exe **(PPID 2576)**

07:35:04 07:35:05 NtReadFile **[6 times]**

PID 1660

07:35:05 **Create Process** The malicious file created a child process as wscript.exe **(PPID 2476)**

07:35:05 07:35:05 NtReadFile **[12 times]**

07:35:06 NtDelayExecution

PID 416

07:35:05 **Create Process** The malicious file created a child process as wscript.exe **(PPID 2476)**

07:35:05 07:35:05 NtReadFile **[12 times]**

PID 1336

07:35:05 **Create Process** The malicious file created a child process as wscript.exe **(PPID 2476)**

07:35:05 07:35:05 NtReadFile **[12 times]**

PID 1464

07:35:05 **Create Process** The malicious file created a child process as wscript.exe **(PPID 2476)**

07:35:06 07:35:06 NtReadFile **[12 times]**

PID 1948

07:35:05 **Create Process** The malicious file created a child process as wscript.exe **(PPID 2476)**

07:35:06 07:35:06 NtReadFile **[12 times]**

07:35:38 07:35:41 ConnectEx **[3 times]**

PID 1924

07:35:06 **Create Process** The malicious file created a child process as DriverPack.exe **(PPID 2476)**

07:35:06 Create Process

07:35:10 Create Process

PID 2708

07:35:07 **Create Process** The malicious file created a child process as cmd.exe **(PPID 1924)**

07:35:08 Create Process

07:35:08 Create Process

PID 2216

07:35:08 **Create Process** The malicious file created a child process as reg.exe **(PPID 2708)**

07:35:08 RegCreateKeyExW

PID 3016

07:35:08 **Create Process** The malicious file created a child process as reg.exe **(PPID 2708)**

PID 1656

07:35:10 **Create Process** The malicious file created a child process as mshta.exe **(PPID 1924)**

07:35:11 NtDelayExecution

07:35:13 07:35:13 NtReadFile **[2 times]**

07:35:13 07:35:21 ConnectEx **[2 times]**

07:35:24 07:35:51 connect **[13 times]**

07:35:39 Create Process

07:35:39 Create Process

07:35:45 Create Process

07:35:52 ConnectEx

07:35:52 connect

07:35:53 ConnectEx

PID 524

07:35:45 **Create Process** The malicious file created a child process as cmd.exe **(PPID 1656)**

07:35:46 Create Process

PID 2732

07:35:47 **Create Process** The malicious file created a child process as powershell.exe **(PPID 524)**

07:35:47 07:35:47 NtQueryFullAttributesF **[12 times]**

07:35:48 NtProtectVirtualMemo

07:37:13 Create Process

PID 2728

07:37:15 **Create Process** The malicious file created a child process as csc.exe **(PPID 2732)**

07:37:18 Create Process

PID 2764

07:37:18 **Create Process** The malicious file created a child process as cvtres.exe **(PPID 2728)**

PID 1728

07:35:46 **Create Process** The malicious file created a child process as rundll32.exe **(PPID 1656)**

07:35:46 NtDelayExecution

PID 1400

07:35:54 **Create Process** The malicious file created a child process as rundll32.exe **(PPID 1656)**

PID 584

07:35:19 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

- 07:35:23 Create Process
- 07:35:26 Create Process
- 07:35:29 Create Process
- 07:36:24 RegOpenKeyExW
- 07:36:37 Create Process

PID 1708

07:35:24 **Create Process** The malicious file created a child process as WmiPrvSE.exe **(PPID 584)**

- 07:35:24 NtDelayExecution
- 07:35:30 07:39:04 RegQueryValueExW **[23 times]**

PID 2820

07:35:28 **Create Process** The malicious file created a child process as WmiPrvSE.exe **(PPID 584)**

- 07:35:31 GetSystemTimeAsFileTime

PID 2664

07:35:30 **Create Process** The malicious file created a child process as WmiPrvSE.exe **(PPID 584)**

- 07:35:39 RegQueryValueExW

PID 2600

07:36:52 **Create Process** The malicious file created a child process as WmiPrvSE.exe **(PPID 584)**

- 07:37:21 07:37:21 NtQueryFullAttributesF **[2 times]**
- 07:37:21 NtCreateFile
- 07:37:21 NtQueryFullAttributes
- 07:37:21 NtCreateFile
- 07:37:21 FindFirstFileExW
- 07:37:21 NtCreateFile
- 07:37:45 ConnectEx

PID 2660

07:35:24 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\332c6d7a41782059a0ce7bb28047a76f91b34a98.exe
C:\Users\user\AppData\Local\Temp\7ZipSfx.000
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\loading.gif
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\header\header-logo.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\header
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\screens\new-logo.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\screens
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet\no_internet-complete.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet\no_internet-connection.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet\no_internet-step1.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet\no_internet-step2.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\Icon.ico
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\init.cmd
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\onexit.cmd
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\drp.css
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\run.hta
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\config.js
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\prepare.js
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\patch.reg
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\DriverPack.exe
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\modules
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\languages
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\screens
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\programs

C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\no_internet
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\installation\statuses
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\installation
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\installation\soft
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\installation\drivers
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\installation\controls
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\header
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\games
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\final
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\device-class
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\charms
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\burger
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\img\bugreport
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\css\fonts\Roboto
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\css\fonts
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\css
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\css\fonts\ProximaNova
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\css\fonts\Open-Sans
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\css\fonts\DRPicons
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\css\fonts\DRPcheckbox
\??\MountPointManager
C:\Windows\SysWOW64\wscript.exe
C:\Windows\SysWOW64\en-US\jscript.dll.mui
C:\Windows\System32\tzres.dll
C:\Windows\SysWOW64\wshom.ocx
C:\Windows\SysWOW64\stdole2.tlb
C:\Windows\System32\wbem\wbemdisp.tlb
C:\Users\Public\Desktop
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini

C:\Users\Public
C:\Users\Public\desktop.ini
C:\Users\Public\Desktop\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-

aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_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 Script Host\Settings\IgnoreUserSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\Enabled
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\TrustPolicy
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\TrustPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\UseWINSAFER
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\Timeout
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\DisplayLogo
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Timeout
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\DisplayLogo
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.js\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\JSFile\ScriptEngine\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\JScript\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\COM+Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\DA0C75D6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{F935DC20-1CF0-11D0-ADB9-00C04FD58A0B}\1.0\0\win32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{00020430-0000-0000-C000-000000000046}\2.0\0\win32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\WBEM\Scripting\Default Impersonation Level
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{565783C6-CB41-11D1-8B02-00600806D9B6}\1.2\0\win32\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Domain
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32\(Default)

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\loading.gif
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\header\header-logo.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\screens\new-logo.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet\no_internet-complete.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet\no_internet-connection.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet\no_internet-step1.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\no_internet\no_internet-step2.png
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\Icon.ico
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\init.cmd
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\onexit.cmd
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\drp.css
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\run.hta
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\config.js

C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\prepare.js
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\patch.reg
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\DriverPack.exe
C:\Users\user\AppData\Roaming\DRPSu\diagnostics\hardware.json
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\driverpack-wget.exe
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\driverpack-7za.exe
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\devcon64.exe
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\modules\clientid.js
\??\nul
C:\Users\user\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\DriverPackSolution[1].html
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\open-sans[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\normalize.min[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\proximanova[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\roboto[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\icons-checkbox[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\icons[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\custom-control[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\drp[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\lte-ie9[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\lte-ie8[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\config[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\drp[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\opensans-bold-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\opensans-semibold-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\opensans-italic-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\opensans-regular-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\style[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\roboto-regular-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\roboto-light-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\roboto-thin-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\proxima_nova_light-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\proxima_nova_regular-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\proxima_nova_semibold-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\ie7[1].css

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\DRPcheckbox[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\DRPicons-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\new-logo[1].png
C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6xx.b4rlq.ps1
C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.cmd.txt
\Device\NamedPipe
C:\Users\user\AppData\Roaming\DRPSu\Logs\log___2018-04-08-18-46-12.html
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\en[1].js
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\ACF244F1A10D4DBED0D88EBA0C43A9B5_16756CC7371BB76A269719AA1471E96C
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\ACF244F1A10D4DBED0D88EBA0C43A9B5_16756CC7371BB76A269719AA1471E96C
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\watch[1].js
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
\??\WMIDataDevice
\??\PIPE\wkssvc
\??\PIPE\srvsvc
\??\PIPE\lsarpc
C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.stdout.log
C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.stderr.log
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\27W5GVRAFPRZVEG8E233.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms
C:\Users\user\AppData\Local\Temp\3_uhqegk.tmp
C:\Users\user\AppData\Local\Temp\3_uhqegk.0.cs
C:\Users\user\AppData\Local\Temp\3_uhqegk.dll
C:\Users\user\AppData\Local\Temp\3_uhqegk.cmdline
C:\Users\user\AppData\Local\Temp\3_uhqegk.out

RESOLVED APIS

comctl32.dll.RegisterClassNameW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
dwmapi.dll.DwmIsCompositionEnabled

uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeColor
uxtheme.dll.GetThemeMargins
uxtheme.dll.GetThemeFont
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
cryptbase.dll.SystemFunction036
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
kernel32.dll.GetNativeSystemInfo
kernel32.dll.SetProcessPreferredUILanguages
uxtheme.dll.EnableThemeDialogTexture
uxtheme.dll.IsThemePartDefined
uxtheme.dll.GetThemeBool
imm32.dll.ImmIsIME
uxtheme.dll.GetThemeInt
gdi32.dll.GdiIsMetaPrintDC
uxtheme.dll.SetWindowTheme
uxtheme.dll.CloseThemeData
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386
uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware
sechost.dll.LookupAccountNameLocalW
advapi32.dll.LookupAccountSidW
sechost.dll.LookupAccountSidLocalW
kernel32.dll.HeapSetInformation
sxs.dll.SxsOleAut32MapConfiguredClsidToReferenceClsid
ole32.dll.CoGetObjectContext
ole32.dll.CoCreateInstance
advapi32.dll.SaferIdentifyLevel
advapi32.dll.SaferComputeTokenFromLevel
advapi32.dll.SaferCloseLevel
cryptsp.dll.CryptAcquireContextW
cryptsp.dll.CryptGenRandom
rpcrtremote.dll.I_RpcExtInitializeExtensionPoint
ole32.dll.CLSIDFromProgIDEx
ole32.dll.CoGetClassObject
wscript.exe.#1
sxs.dll.SxsOleAut32RedirectTypeLibrary
advapi32.dll.RegOpenKeyW
advapi32.dll.RegQueryValueW
advapi32.dll.DuplicateTokenEx
advapi32.dll.RegEnumKeyW
oleaut32.dll.#2
oleaut32.dll.#6
kernel32.dll.GetThreadPreferredUILanguages
kernel32.dll.SetThreadPreferredUILanguages
kernel32.dll.LocaleNameToLCID
kernel32.dll.GetLocaleInfoEx
kernel32.dll.LCIDToLocaleName
kernel32.dll.GetSystemDefaultLocaleName
oleaut32.dll.#283
oleaut32.dll.#284
ole32.dll.CoGetMalloc
ole32.dll.StringFromGUID2

advapi32.dll.OpenThreadToken
ole32.dll.CreateBindCtx
ole32.dll.CoTaskMemAlloc

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\27W5GVRAFPRZVEG8E233.temp
C:\Users\user\AppData\Local\Temp\3_uhqegk.tmp
C:\Users\user\AppData\Local\Temp\3_uhqegk.pdb
C:\Users\user\AppData\Local\Temp\3_uhqegk.err
C:\Users\user\AppData\Local\Temp\3_uhqegk.0.cs
C:\Users\user\AppData\Local\Temp\3_uhqegk.dll
C:\Users\user\AppData\Local\Temp\3_uhqegk.cmdline
C:\Users\user\AppData\Local\Temp\3_uhqegk.out
C:\Users\user\AppData\Local\Temp\RESB91.tmp
C:\Users\user\AppData\Local\Temp\CSCA86.tmp

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\332c6d7a41782059a0ce7bb28047a76f91b34a98.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_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_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\IgnoreUserSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\Enabled
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\AppID\wscript.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\TrustPolicy
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\TrustPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\UseWINSAFER
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\Timeout
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\DisplayLogo
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Timeout
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\DisplayLogo
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_CLASSES_ROOT\.js
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.js\(Default)
HKEY_CLASSES_ROOT\JSFile\ScriptEngine
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\JSFile\ScriptEngine\(Default)
HKEY_CURRENT_USER\Software\Classes\JScript

EXECUTED COMMANDS

wscript.exe //B "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\prepare.js" localdiagnostics
wscript.exe //B "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\prepare.js" drivers
wscript.exe //B "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\prepare.js" newsoft
wscript.exe //B "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\prepare.js" hardware
wscript.exe //B "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\prepare.js" binaries
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\DriverPack.exe --sfx "332c6d7a41782059a0ce7bb28047a76f91b34a98.exe"
"C:\Windows\System32\cmd.exe" /c Tools\init.cmd "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\run.hta" "--sfx" "332c6d7a41782059a0ce7bb28047a76f91b34a98.exe"

C:\Windows\System32\cmd.exe /c Tools\init.cmd "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\run.hta" "--sfx" "332c6d7a41782059a0ce7bb28047a76f91b34a98.exe"
"C:\Windows\System32\mshta.exe" "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\run.hta" "--sfx" "332c6d7a41782059a0ce7bb28047a76f91b34a98.exe"
C:\Windows\System32\mshta.exe "C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\run.hta" "--sfx" "332c6d7a41782059a0ce7bb28047a76f91b34a98.exe"
reg import C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\\patch.reg
C:\Windows\sysnative\reg.exe import C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\\patch.reg
"C:\Windows\System32\cmd.exe" /C powershell -NonInteractive -NoLogo -NoProfile -ExecutionPolicy Bypass "Get-Content 'C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.cmd.txt' -Wait | Invoke-Expression" > "C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.stdout.log" 2> "C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.stderr.log"
cmd /C powershell -NonInteractive -NoLogo -NoProfile -ExecutionPolicy Bypass "Get-Content 'C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.cmd.txt' -Wait | Invoke-Expression" > "C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.stdout.log" 2> "C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.stderr.log"
rundll32 kernel32,Sleep
C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
C:\Windows\system32\wbem\wmiprvse.exe -Embedding
C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
powershell -NonInteractive -NoLogo -NoProfile -ExecutionPolicy Bypass "Get-Content 'C:\Users\user\AppData\Roaming\DRPSu\temp\ps.jfqzb6yi.qslyd.cmd.txt' -Wait | Invoke-Expression"
"C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\3_uhqegk.cmdline"
C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESB91.tmp" "c:\Users\user\AppData\Local\Temp\CSCA86.tmp"

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\332c6d7a41782059a0ce7bb28047a76f91b34a98.exe
C:\Windows\SysWOW64\wscript.exe
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\prepare.js
C:\Windows\SysWOW64\en-US\jscript.dll.mui
C:\Windows\System32\tzres.dll
C:\Windows\SysWOW64\wshom.ocx
C:\Windows\SysWOW64\stdole2.tlb
C:\Windows\System32\wbem\wbemdisp.tlb
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db

C:\Users\desktop.ini
C:\Users
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Windows
C:\Windows\Fonts\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user\Favorites\desktop.ini
C:\Users\user\Documents\desktop.ini
C:\Windows\System32\wbem\en-US\wmiutils.dll.mui
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\init.cmd

C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\patch.reg
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\run.hta
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\config.js
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\drp.css
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\Icon.ico
C:\Windows\win.ini
C:\Windows\SysWOW64\mshta.exe
C:\Windows\System32\dxtmsft.dll
C:\Users\user\AppData\Local\Temp\7ZipSfx.000\bin\Tools\img\screens\new-logo.png
C:\Windows\System32\dxtrans.dll
C:\Windows\SysWOW64\wininet.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\DriverPackSolution[1].html
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\normalize.min[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\open-sans[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\roboto[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\proximanova[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\icons-checkbox[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\icons[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\custom-control[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\drp[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\lte-ie9[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\lte-ie8[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\config[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\drp[1].js

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\!BrowserEmulation!SharedMemory!Mutex
Local__DDrawExclMode__
Local__DDrawCheckExclMode__
Local\DDrawWindowListMutex
Local\DDrawDriverObjectListMutex

Local\WininetStartupMutex
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex
Local\c:!users!user!appdata!roaming!microsoft!windows!ietldcache!
IESQMMUTEX_0_208
Global\CLR_CASOFF_MUTEX
DBWinMutex

MODIFIED REGISTRY KEYS

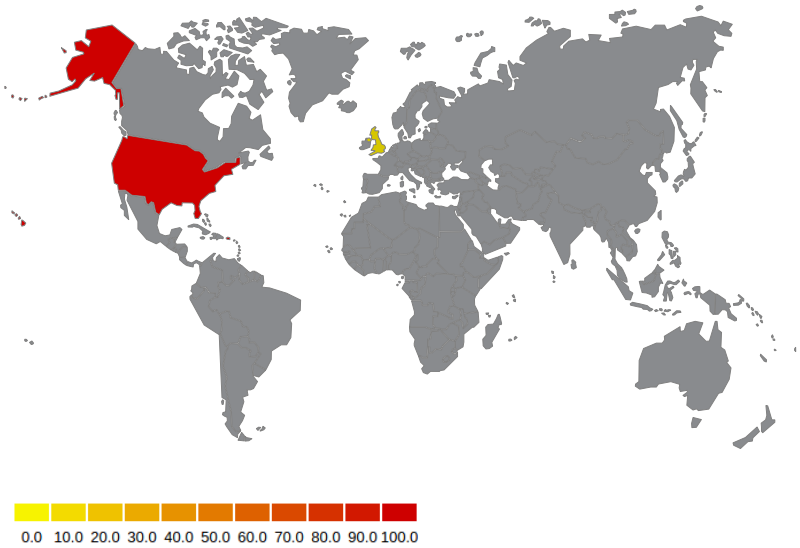
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Microsoft-Windows-Diagnostics-Performance/Operational\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Diagnostics-Performance/Operational
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\drp.su\update
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\drp.su\update\http
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\drp.su\update\https
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\GlobalUserOffline
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles\MaxScriptStatements
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Styles\MaxScriptStatements
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_GPU_RENDERING
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_GPU_RENDERING\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_NINPUT_LEGACYMODE
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_NINPUT_LEGACYMODE\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_SSLUX\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ADDON_MANAGEMENT\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BROWSER_EMULATION\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_XMLHTTP
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_XMLHTTP\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBSOCKET
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_WEBSOCKET\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_AJAX_CONNECTIONEVENTS
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_AJAX_CONNECTIONEVENTS\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_XDOMAINREQUEST
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_XDOMAINREQUEST\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BLOCK_LMZ_OBJECT\mshta.exe

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BLOCK_LMZ_SCRIPT\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_SECURITYBAND\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ZONE_ELEVATION\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_96DPI_PIXEL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_96DPI_PIXEL\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_IVIEWOBJECTDRAW_DMLT9_WITH_GDI
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_IVIEWOBJECTDRAW_DMLT9_WITH_GDI\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_NAVIGATION_SOUNDS
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_NAVIGATION_SOUNDS\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SPELLCHECKING
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_SPELLCHECKING\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_STATUS_BAR_THROTTLING
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_STATUS_BAR_THROTTLING\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.css\Content Type
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.htm\Content Type
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.html\Content Type
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.js\Content Type
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Styles\MaxScriptStatements
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_GPU_RENDERING\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_NINPUT_LEGACYMODE\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_SSLUX\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ADDON_MANAGEMENT\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BROWSER_EMULATION\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_XMLHTTP\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_WEBSOCKET\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_AJAX_CONNECTIONEVENTS\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_XDOMAINREQUEST\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BLOCK_LMZ_OBJECT\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BLOCK_LMZ_SCRIPT\mshta.exe

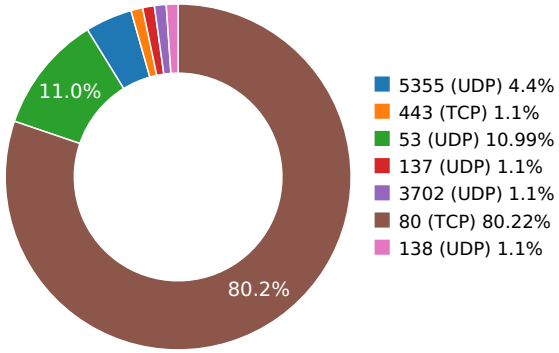
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_SECURITYBAND\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ZONE_ELEVATION\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_96DPI_PIXEL\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_IVIEWOBJECTDRAW_DMLT9_WITH_GDI\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_NAVIGATION_SOUNDS\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_SPELLCHECKING\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_STATUS_BAR_THROTTLING\mshta.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DirectDraw\MostRecentApplication\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DirectDraw\MostRecentApplication\ID
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName

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
	104.31.75.124	United States	13335	Cloudflare, Inc.	Malware Process
	184.26.44.105	United States	20940	Akamai Technologies, Inc.	OS Process
	184.26.44.97	United States	20940	Akamai Technologies, Inc.	OS Process
	184.26.44.98	United States	20940	Akamai Technologies, Inc.	OS Process
	87.250.250.119		13238		Malware Process
	23.63.227.177		20940	Akamai Technologies, Inc.	OS Process
	13.93.50.202		8075	Microsoft Corporation	Malware Process
	87.117.235.116		20860		Malware Process
	81.94.205.66		20860		Malware Process
	104.31.74.124		13335	Cloudflare, Inc.	Malware Process
	104.31.74.124		13335	Cloudflare, Inc.	Malware Process
	184.50.239.65		20940	Akamai Technologies, Inc.	OS Process
	172.217.10.238		15169	Google LLC	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; W...	1	19.307256937
Path: /v2/ **URI:** http://update.drp.su/v2/						
www.google-analytics.com	80	GET	1.1	Mozilla/4.0 (compatible; W...	1	26.7378640175

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /collect?v=1&t=event&ec=pico&ea=updatescript+downloaded&tid=UA-68879973-12&cid=15231915325600.23116904517547937&el=17.7.63&z=25966299481927085 **URI:** http://www.google-analytics.com/collect?v=1&t=event&ec=pico&ea=updatescript+downloaded&tid=UA-68879973-12&cid=15231915325600.23116904517547937&el=17.7.63&z=25966299481927085						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	29.9299769402
Path: /beetle/17.7.93/DriverPackSolution.html **URI:** http://update.drp.su/beetle/17.7.93/DriverPackSolution.html						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.2515769005
Path: /beetle/17.7.93/css/open-sans.css **URI:** http://update.drp.su/beetle/17.7.93/css/open-sans.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.2517879009
Path: /beetle/17.7.93/css/normalize.min.css **URI:** http://update.drp.su/beetle/17.7.93/css/normalize.min.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.3499109745
Path: /beetle/17.7.93/css/proximanova.css **URI:** http://update.drp.su/beetle/17.7.93/css/proximanova.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.3512198925
Path: /beetle/17.7.93/css/roboto.css **URI:** http://update.drp.su/beetle/17.7.93/css/roboto.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.5650558472
Path: /beetle/17.7.93/css/icons-checkbox.css **URI:** http://update.drp.su/beetle/17.7.93/css/icons-checkbox.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.565253973
Path: /beetle/17.7.93/css/icons.css **URI:** http://update.drp.su/beetle/17.7.93/css/icons.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.664940834
Path: /beetle/17.7.93/drp.css **URI:** http://update.drp.su/beetle/17.7.93/drp.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.6652579308
Path: /beetle/17.7.93/css/custom-control.css **URI:** http://update.drp.su/beetle/17.7.93/css/custom-control.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.7886359692
Path: /beetle/17.7.93/css/lte-ie9.css **URI:** http://update.drp.su/beetle/17.7.93/css/lte-ie9.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.8290989399
Path: /beetle/17.7.93/css/lte-ie8.css **URI:** http://update.drp.su/beetle/17.7.93/css/lte-ie8.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.9117720127
Path: /beetle/17.7.93/config.js **URI:** http://update.drp.su/beetle/17.7.93/config.js						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.9563498497

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /beetle/17.7.93/drp.js **URI:** http://update.drp.su/beetle/17.7.93/drp.js						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	30.9997859001
Path: /beetle/17.7.93/css/fonts/Open-Sans/opensans-bold-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/Open-Sans/opensans-bold-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	31.1904668808
Path: /beetle/17.7.93/css/fonts/Open-Sans/opensans-semibold-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/Open-Sans/opensans-semibold-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	31.3974838257
Path: /beetle/17.7.93/css/fonts/Open-Sans/opensans-italic-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/Open-Sans/opensans-italic-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	31.617866993
Path: /beetle/17.7.93/css/fonts/Open-Sans/opensans-regular-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/Open-Sans/opensans-regular-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	31.8081498146
Path: /beetle/17.7.93/css/style.css **URI:** http://update.drp.su/beetle/17.7.93/css/style.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.0352509022
Path: /beetle/17.7.93/css/fonts/Roboto/roboto-regular-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/Roboto/roboto-regular-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.2029838562
Path: /beetle/17.7.93/css/fonts/Roboto/roboto-light-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/Roboto/roboto-light-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.2652049065
Path: /beetle/17.7.93/css/fonts/Roboto/roboto-thin-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/Roboto/roboto-thin-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.48335886
Path: /beetle/17.7.93/css/fonts/ProximaNova/proxima_nova_light-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/ProximaNova/proxima_nova_light-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.5336940289
Path: /beetle/17.7.93/css/fonts/ProximaNova/proxima_nova_regular-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/ProximaNova/proxima_nova_regular-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.7279868126
Path: /beetle/17.7.93/css/fonts/ProximaNova/proxima_nova_semibold-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/ProximaNova/proxima_nova_semibold-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.7553110123
Path: /beetle/17.7.93/css/ie7.css **URI:** http://update.drp.su/beetle/17.7.93/css/ie7.css						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.8380498886
Path: /beetle/17.7.93/css/fonts/DRPcheckbox/DRPcheckbox.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/DRPcheckbox/DRPcheckbox.eot?						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	32.9447069168
Path: /beetle/17.7.93/css/fonts/DRPicons/DRPicons-webfont.eot? **URI:** http://update.drp.su/beetle/17.7.93/css/fonts/DRPicons/DRPicons-webfont.eot?						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	33.3192148209
Path: /beetle/17.7.93/img/screens/new-logo.png **URI:** http://update.drp.su/beetle/17.7.93/img/screens/new-logo.png						
download.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; W...	1	44.0484969616
Path: /updates/beetle/driverpack-wget.exe **URI:** http://download.drp.su/updates/beetle/driverpack-wget.exe						
download.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; W...	1	45.8721849918
Path: /updates/beetle/driverpack-7za.exe **URI:** http://download.drp.su/updates/beetle/driverpack-7za.exe						
download.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; W...	1	47.2774958611
Path: /updates/beetle/devcon64.exe **URI:** http://download.drp.su/updates/beetle/devcon64.exe						
auth.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	50.6237819195
Path: /api/session **URI:** http://auth.drp.su/api/session						
update.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	55.4339048862
Path: /api/logs **URI:** http://update.drp.su/api/logs						
update.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	55.5127208233
Path: /api/logs **URI:** http://update.drp.su/api/logs						
update.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	55.9524629116
Path: /api/logs **URI:** http://update.drp.su/api/logs						
update.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	55.9527280331
Path: /api/logs **URI:** http://update.drp.su/api/logs						
update.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	56.2432658672
Path: /api/logs **URI:** http://update.drp.su/api/logs						
update.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	56.2442378998
Path: /api/logs **URI:** http://update.drp.su/api/logs						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	56.4093298912
Path: /beetle/17.7.93/languages/en.js **URI:** http://update.drp.su/beetle/17.7.93/languages/en.js						
update.drp.su	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	57.4413709641
Path: /beetle/17.7.93/languages/en-us.js **URI:** http://update.drp.su/beetle/17.7.93/languages/en-us.js						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	57.6342508793
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9f58e753ca858ae5 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9f58e753ca858ae5						
update.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	57.8086309433
Path: /api/logs **URI:** http://update.drp.su/api/logs						
ocsp.globalsign.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	58.7970368862
Path: /rootr1/MEwwSjBIMEYwRDAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCCwQAAAAAAURO8EJH **URI:** http://ocsp.globalsign.com/rootr1/MEwwSjBIMEYwRDAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCCwQAAAAAAURO8EJH						
update.drp.su	80	POST	1.1	Mozilla/4.0 (compatible; M...	1	62.6340699196
Path: /api/logs **URI:** http://update.drp.su/api/logs						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	93.484254837
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	93.9358189106
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	93.9915928841
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	94.5525999069
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	154.671916962
Path: /pki/crl/products/microsoftrootcert.crl **URI:** http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl						

DNS QUERIES

Request	Type
update.drp.su	A
Answers - 87.117.235.116 (A) - 82.145.55.124 (A)	
www.google-analytics.com	A
Answers - www-google-analytics.l.google.com (CNAME) - 172.217.10.238 (A)	
download.drp.su	A

Request	Type
Answers - 81.94.192.167 (A) - 87.117.231.157 (A) - 81.94.205.66 (A) - 88.150.137.207 (A) - 87.117.239.148 (A) - 87.117.239.150 (A) - 80.243.178.242 (A) - 109.169.53.106 (A)	
auth.drp.su	A
Answers - 13.93.50.202 (A)	
mc.yandex.ru	A
Answers - 87.250.251.119 (A) - 87.250.250.119 (A) - 93.158.134.119 (A) - 213.180.193.119 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 184.26.44.105 (A) - a1621.g.akamai.net (CNAME) - 184.26.44.97 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
ocsp.globalsign.com	A
Answers - 104.31.75.124 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.31.74.124 (A)	
crl.microsoft.com	A
Answers - 184.26.44.98 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
19.307256937	Sandbox	87.117.235.116	80
26.7378640175	Sandbox	172.217.10.238	80
29.9299769402	Sandbox	87.117.235.116	80
30.2515769005	Sandbox	87.117.235.116	80
30.2517879009	Sandbox	87.117.235.116	80
44.0484969616	Sandbox	87.117.231.157	80
45.8721849918	Sandbox	87.117.231.157	80
47.2774958611	Sandbox	87.117.231.157	80
50.6237819195	Sandbox	13.93.50.202	80
55.4339048862	Sandbox	87.117.235.116	80
55.5127208233	Sandbox	87.117.235.116	80
55.9524629116	Sandbox	87.117.235.116	80
55.9527280331	Sandbox	87.117.235.116	80
56.2176449299	Sandbox	87.250.250.119	443
56.2432658672	Sandbox	87.117.235.116	80
56.2442378998	Sandbox	87.117.235.116	80
56.4093298912	Sandbox	87.117.235.116	80
57.6342508793	Sandbox	184.26.44.105	80
57.8086309433	Sandbox	87.117.235.116	80
58.7970368862	Sandbox	104.31.74.124	80
93.484254837	Sandbox	184.26.44.97	80
94.5525999069	Sandbox	104.31.75.124	80
154.671916962	Sandbox	184.26.44.98	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.24554181099	Sandbox	224.0.0.252	5355
7.24766182899	Sandbox	192.168.56.255	137
7.31037282944	Sandbox	224.0.0.252	5355
7.31609892845	Sandbox	239.255.255.250	3702
9.87168288231	Sandbox	224.0.0.252	5355
13.3080718517	Sandbox	192.168.56.255	138
19.1533949375	Sandbox	8.8.4.4	53
26.7006180286	Sandbox	8.8.4.4	53
27.1985988617	Sandbox	224.0.0.252	5355
43.7425608635	Sandbox	8.8.4.4	53
50.3430399895	Sandbox	8.8.4.4	53
56.0371768475	Sandbox	8.8.4.4	53
57.4842989445	Sandbox	8.8.4.4	53
58.7493629456	Sandbox	8.8.4.4	53
93.4286928177	Sandbox	8.8.4.4	53
94.5019569397	Sandbox	8.8.4.4	53
154.028152943	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Config[1].Js	**Type :** ASCII text **MD5 :** 6ad30bbb0f86b7f8793173c3f8f9df20 **SHA-1 :** 46acdabd37ecce75961ca242b4924fbbdd651c80 **SHA-256 :** 7357c5c81e7674ab9640b0eff9c70abbb9cf7a4bc **SHA-512 :** c8b9d4ffdf9fd8b201149d92e6d7f368e74cb4f5a(**Size :** 3.086 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Driverpack-Wget.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows, UPX compressed **MD5 :** 0cb361806ce3293f5ad9bbe673a6512d **SHA-1 :** 24290e7d7cf174bac5b28bea034b1705553f8fa5 **SHA-256 :** a6e080385e6212dec00ff527783e1cd5f3a075ab(**SHA-512 :** e522b596733d14a51a258fac4d7cf863f21b2651: **Size :** 419.216 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Prepare.Js	**Type :** UTF-8 Unicode text, with very long lines **MD5 :** 0a421fe8d683eb726f3f9be8cecbd679 **SHA-1 :** 93f2cb5029ed86e201de059429a9a41c058f870b **SHA-256 :** ccf2b2c9d80a2491ce3ac250de7fd747fbd618191 **SHA-512 :** ecb68886b8f2724643273d98fb7d59ac4791b6d6 **Size :** 107.182 Kilobytes.
C:\Users\User\AppData\Roaming\DRPSu\Temp\Ps.Jfqzb6xx.B4rlq.Ps1	**Type :** Little-endian UTF-16 Unicode text **MD5 :** b4ded2e77fcbe68b59f99f90c3a80081 **SHA-1 :** 232b067374f7b58d4dd3ec5bc0d949153ee08a45 **SHA-256 :** 0fe8c4b4886f5de8bdaf6e6cce4a33e77242f08f2f **SHA-512 :** f482c67bff6469b92ea757f20416a1bfd8cf127f1c **Size :** 7.79 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Proxima_nova_semibold-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** 044aa0b596161750cb58aca15c52cf38 **SHA-1 :** d40e645b34188a54d909fa40f7eddeefb8b9df03 **SHA-256 :** 790579e11608136663d073bc6f99848c04b4dcd6 **SHA-512 :** 1a3b3abc614a7ddf673e34a936de63809f8c18a8 **Size :** 66.676 Kilobytes.
C:\Users\User\AppData\Local\Temp\RESB91.Tmp	**Type :** 80386 COFF executable not stripped - version 25189 **MD5 :** 8ccad99257ce919c4ebe0481e096d2b4 **SHA-1 :** 05920106d5337bec5f546b7a52df9d41ffa44ab9 **SHA-256 :** fc8fabe91213db3d1815db47b67a8ddb48eed23(**SHA-512 :** d6aba984ee8e585d3c878ed4bf4080eb5e1896b4 **Size :** 1.196 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Style[1].Css	**Type :** ASCII text **MD5 :** bb5d8b40a24f14522d3231ed24796c40 **SHA-1 :** 59490a8e190d59688ecfead121154daa4b513ad5 **SHA-256 :** 21a30dd5296d49f9508a69c0202f167f87a1573d **SHA-512 :** 335ab25fba01598890416ccde19b716d022ced79 **Size :** 14.068 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\3_uhqegk.Out	**Type :** UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators **MD5 :** 29ca2bd04f22b188606b72121b683e43 **SHA-1 :** 701a18385ea9ed1fafa43320b57fc2ff265aa643 **SHA-256 :** e76fb7684bdf757b5310b88e18c5a1c42129050e **SHA-512 :** 14894a6774778da1219e7eacfa70e0f3a5d3aefa5 **Size :** 0.617 Kilobytes.
C:\Users\User\AppData\Local\Temp\CSCA86.Tmp	**Type :** MSVC .res **MD5 :** 8490f7579c180879a21e770f353d81c2 **SHA-1 :** 8b24497b06bd4dbd09231bb89e8ae726945c02d6 **SHA-256 :** d22686163147408350ee90a0ecbe5915d519714 **SHA-512 :** 8f40d9c1050897c3967e3ac8c03bce2351a65b7a **Size :** 0.652 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Drp[1].Js	**Type :** ASCII text, with very long lines **MD5 :** 87b5369343feb5b9f849d0aeee2c5fcf **SHA-1 :** f8b22a166deb3331e0d87d1e6ace95370c3471f9 **SHA-256 :** cc8db724d8dd1b135c3905ff3c24faa5a62a010e4 **SHA-512 :** 9af8cb7537679e2962fe3705c5e0185298701a42 **Size :** 2393.313 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Modules\Clientid.Js	**Type :** ASCII text, with CRLF line terminators **MD5 :** 08847315a4aad39d83ff8ec1af662472 **SHA-1 :** 170cb592bda211a42a2dc12d110263a83ab6fd90 **SHA-256 :** 7c443dab2d67f59266b656ee0a762b6d6231791 **SHA-512 :** bce7251892b5c9b9a4eb8dbdd6ec967f6823f652 **Size :** 0.07 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\En[1].Js	**Type :** UTF-8 Unicode text, with very long lines **MD5 :** 04d1e82d88c73245e01fd1c24821563a **SHA-1 :** d67b07fbfb2fabdeb3a3d1a791a6888cbf765386 **SHA-256 :** c57642189b7977cff1e04b52ab025212114f7080 **SHA-512 :** 2d33008a74622786e70cd458a9b0e7e8a909524 **Size :** 42.139 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Ie7[1].Css	**Type :** ASCII text **MD5 :** 80521e1e4857e94d07bb3127b72eeef1 **SHA-1 :** 490252434bd8532115883bf08123c2c757d91871 **SHA-256 :** 38cc050a7c3e3aa004558c96fa0983b3059ab041 **SHA-512 :** 3d1917710d3405a9c6980bb95d3153fce122afd5 **Size :** 0.271 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\ACF244F1A10D4DBED0D88EBA0C43A9B5_16756CC7371BB76A269719AA1471E96C	**Type :** data **MD5 :** 4c2653d1b7e2ed26f623cf04a474933c **SHA-1 :** e4d4777a8f3fdfb3e42a9754b2cd6754becd55fc **SHA-256 :** 6291f0c82b47d67322061a3804be142818bb305 **SHA-512 :** 238e80e9c3af833e925fbf8484f62d2341b0d368 **Size :** 1.518 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Init.Cmd	**Type :** DOS batch file, ASCII text, with CRLF line terminators **MD5 :** 2d07f324a539ade610cd86f3788db114 **SHA-1 :** c898927fe8eddab9997daefe21241ed211221676 **SHA-256 :** 20692738398af39ee4c65eda97b70f65466baacc **SHA-512 :** 12a2e9cb3de9ce4113b85c54bc6a0845f604608a **Size :** 0.852 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Icons-Checkbox[1].Css	**Type :** ASCII text **MD5 :** 3be98220035017d9b818f3cc94f87587 **SHA-1 :** bc07f11d0a59f942ac942dba02214a7041ad6e3a **SHA-256 :** cb134dcb95a407795c671a512c389894d3525fba **SHA-512 :** d2e7d57cb7b7e771c82c75a04fbfb86ebecbb409 **Size :** 0.444 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Opensans-Semibold-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** 3fab39a75284a0a9c09563cb64e683d2 **SHA-1 :** bae936c579e21f00462c125bc9e7929a59104362 **SHA-256 :** b3e6e116a5e39acecd9afd4bade07e96b4cc79ce **SHA-512 :** 54128e527b8680cf9900c0c17465b9d1ae00addb **Size :** 39.702 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\DRPicons-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** d85a00ccb58d531afd9ad80a067fbf0e **SHA-1 :** 0a3c0cfea5b9c0fdd5f17a1df49cb1512316330d **SHA-256 :** 0a04d85875091cc334f63b90c8ccfa0838f200239 **SHA-512 :** bce1796d0c71291cb779e2e99399a213b030663 **Size :** 7.996 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Drp[1].Css	**Type :** ASCII text **MD5 :** b05a61ac461505c866d5ea7fa3f3350d **SHA-1 :** 069495e49c7e51d1b19627ddcb6bf35adb9af1bb **SHA-256 :** 702d275cebdb939bbddf6aab5e6d042af41b30a **SHA-512 :** faab85212938e49c6d27b89c38e4069701c2a66d **Size :** 90.331 Kilobytes.
C:\Users\User\AppData\Local\Temp\3_uhqegk.Pdb	**Type :** MSVC program database ver \002 **MD5 :** c348601bafe6dfc49a9c78c2d3efdf79 **SHA-1 :** c97f738f15e3b47d1935c601368b31678f16c71d **SHA-256 :** e1ef772d89ca9b606366bf6493884be96832c940 **SHA-512 :** 09937c222fca0defb3ec261d762f0234ed223289 **Size :** 7.68 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\ACF244F1A10D4DBED0D88EBA0C43A9B5_16756CC7371BB76A269719AA1471E96C	**Type :** data **MD5 :** bdc5bc6c1fd84b498fc40ce09ed6fa0f **SHA-1 :** 6d143f13d92d33eaf64372753c269213b4dee268 **SHA-256 :** 7edb7158ca8c489fb40b2bbeac878429c07fce1a **SHA-512 :** eca2e0c88266db1ffdba701031995d13045c51c0 **Size :** 0.492 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Proxima_nova_regular-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** e5835857d5dddda8d5f0725a386a2d0e **SHA-1 :** 4c92001174816e973c374986e52af2428af2f6b6 **SHA-256 :** 750e86dc4965d1d63216327777239692fcaf3771 **SHA-512 :** 4eee43c691475031bc219bd6bd7001128b62a22 **Size :** 66.124 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Onexit.Cmd	**Type :** DOS batch file, ASCII text, with CRLF line terminators **MD5 :** 898a4306c45f626e1f158596a7403ed6 **SHA-1 :** 0d3227c24082948485706649ebae9b9c01337702 **SHA-256 :** d686c59e90a1ae6053760f244a5a1ae01db4b18 **SHA-512 :** 713db6b587e4657419beb32174444948e64b3f0 **Size :** 0.782 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Opensans-Regular-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** 88a9c629f26f8563a72eac95cb0744bc **SHA-1 :** 484bca13532678133dc14a668c580be2c1346526 **SHA-256 :** 3ae576bfa96d7cf6614c8c97290c7abe03191a8ce **SHA-512 :** b4cdaa3a5a46ef368e9138c9874aa1173b466bc6 **Size :** 41.447 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Img\Header\Header-Logo.Png	**Type :** PNG image data, 168 x 22, 8-bit/color RGBA, non-interlaced **MD5 :** 30b1427e1898d584fbf4347e65e522bb **SHA-1 :** 4f954a8698c9b193f7d62635d13dbf85f0fb892e **SHA-256 :** dc34c8bba856ee83f3bdda4a46898f86c553e59c **SHA-512 :** 7a03cf5cc9ee78dc8d5158319fb0604a7342cfe66 **Size :** 2.351 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Devcon64.Exe	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** 537e673545c63caea220b75d07c02e0a **SHA-1 :** 414f1972a1d94658905a1b2b8463c588209d5e83 **SHA-256 :** f0b2e7fa78b98d87006e18c6cb70aa9f122fc5d4f **SHA-512 :** d6082434fdc4cb28670acc11926744bcef1392b4 **Size :** 87.952 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Patch.Reg	**Type :** Windows Registry text (Win2K or above) **MD5 :** 9297860413f4cc8b0c933650aaed46be **SHA-1 :** 4d243560a8425e6a7af72285db55d09d9e50bdf1 **SHA-256 :** c21a2dab523467d5fcfa8a9ce83a8284a6e92561 **SHA-512 :** 3f68d1e35bd84a845c828b9c253164d9ee8cdc4b **Size :** 5.331 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Custom-Control[1].Css	**Type :** ASCII text **MD5 :** a4abf0bb03d5f5e78b03a07ad395b44b **SHA-1 :** db95841a366f3f41141ddf6e63f02a2bff8ac059 **SHA-256 :** f16936215c5068a55ffc87342283362bacdd1648 **SHA-512 :** 9ae07d70123a5c23e40f46346e55bed8b65ce335 **Size :** 11.158 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Opensans-Italic-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** 66a0b9bd337a3668e953e92f7f3fc6ec **SHA-1 :** 7abf2d65772b80c3a1967a1a03998dd2b84e6a3b **SHA-256 :** f725e655a42ab99b3f59ca4770e0c5fa9de28efd1 **SHA-512 :** 50b87738329765ce4b480cecf568325f3d5d6fe9c **Size :** 49.728 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Icons[1].Css	**Type :** ASCII text **MD5 :** ebae852f3327fdaf3e2fc2bf1cdecb8f **SHA-1 :** f9753fe176069974fc9bce49eae877745282e183 **SHA-256 :** b5f111103f7f090c246a223b1ff497b94c4dd3ac6 **SHA-512 :** bf8e7c5db7a1eacd4344d5facfee1cd66e883389b **Size :** 0.509 Kilobytes.
C:\Users\User\AppData\Roaming\DRPSu\Logs\Log___2018-04-08-18-46-12.Html	**Type :** HTML document, ASCII text, with very long lines, with CRLF, LF line terminators **MD5 :** b6d0512c4c17bdf20e8f22e1efad9111 **SHA-1 :** 9beaae69323f089d4fa118e59bd7892373e24fc5 **SHA-256 :** 8a183417faeda31ecabfa8b9d57ecf3a3713c6fd9 **SHA-512 :** cd5b41612d238e020912a65bf7c3ff00e6a7a0e0 **Size :** 65.13 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD	**Type :** data **MD5 :** e03ce4599a8aa4434501d9297b1c29ac **SHA-1 :** 72b847d64984b4cfd87d96ae199fe79c58d72533 **SHA-256 :** e7e8859a02ddd04d502dd2ae95c7731466a983c **SHA-512 :** a8b15df89241ec444541db33039874d457fdd838 **Size :** 0.781 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Img\No_internet\No_internet-Step1.Png	**Type :** PNG image data, 210 x 130, 8-bit/color RGBA, non-interlaced **MD5 :** fedbae40f618a1315dbca54071708013 **SHA-1 :** 554b12fc2b3b1e09813dc2a8f112d68b1e3e0a65 **SHA-256 :** 018e28f327c21d124bd38dc6c7d80bf8b3a1e61c **SHA-512 :** 78f6d9ca1dd023172cd780230e96ffc50f32bf0a6 **Size :** 2.157 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Roboto-Light-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** 889478bc69a9cfe7ce00665a2d307606 **SHA-1 :** 54ad4852e48a7e4762531fe1dce91b2b95dd5406 **SHA-256 :** 1ee590bcbf3a5f0c1b70e93ab1332e6a230cd44d **SHA-512 :** ca1be8f6816206b0fcbd1b131a09424a7ab6c0fd **Size :** 45.474 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Drp.Css	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** 144a4406e55e4298c1a2ef96c7388046 **SHA-1 :** e0d6434efc95f62e3be9fe4a002ba3ebf9509426 **SHA-256 :** 0d38177bc68156c16912278321baba661081a38 **SHA-512 :** 5c8f89c2bc0613503b808b2b80e63a4f61e7578e **Size :** 9.075 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Icon.Ico	**Type :** MS Windows icon resource - 9 icons, 48x48, 16-colors **MD5 :** 733d67c2e70bc804cd9497d20fe96696 **SHA-1 :** 3ec7c1330af77d2684a88e87642cdec98136f424 **SHA-256 :** 0a3edd3d1fd9ae649d0d6164858705017dc482c **SHA-512 :** 9f44031ce6888f01256bd9ffc663b6e535309d173 **Size :** 25.214 Kilobytes.
C:\Users\User\AppData\Roaming\DRPSu\Diagnostics\Hardware.Json	**Type :** Little-endian UTF-16 Unicode text, with CR line terminators **MD5 :** be072de2f95b8e3df9d52245406e34d4 **SHA-1 :** f000ede55962a2b05eaac3212fb46a07ba5d09b1 **SHA-256 :** dbd1711ff44f2d6b1347bbcdfda4a1702237465e **SHA-512 :** 74dbd7342fb3c14bbad3cab5e0aec9214066fc74 **Size :** 0.354 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\DRPcheckbox[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** 96d44740679ffaf2e5e1d2a8a75c48ee **SHA-1 :** d7b354e3524bea85e065675d61e0d37c637c87e1 **SHA-256 :** c0c660ec085e958acdb6dab93f7df3b8c2375df2 **SHA-512 :** 32f60040c4ef1d3e8a7c46f1d078ea0307bbf9487 **Size :** 1.224 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Img\No_internet\No_internet-Complete.Png	**Type :** PNG image data, 210 x 130, 8-bit/color RGBA, non-interlaced **MD5 :** 9317f902a1a6c30f7b7d2d6be2002803 **SHA-1 :** 0eb579bcc8fffbebfc8e21de3a470bd0ee8c0d7b **SHA-256 :** 196da0c1548eb42d823cf27f62dd25ba79b4e70c **SHA-512 :** 0423c6af3f949597a03f58b87cf5a3e8c963d07a1 **Size :** 1.666 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Proximanova[1].Css	**Type :** ASCII text **MD5 :** cf0c65f6d17307ccd7914e984ac86a6f **SHA-1 :** 4fcef85545731123eb5e3e1886817f8014f22e21 **SHA-256 :** 58a658fd04bb4aa2ff90ff7125ca6e1775b1a9d05 **SHA-512 :** 0f171b8839385cd192d10c5c06e1b2284e6f2d7d **Size :** 1.708 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Watch[1].Js	**Type :** UTF-8 Unicode (with BOM) text, with very long lines **MD5 :** 321eee33aa300ec046c59051479b8e37 **SHA-1 :** 66bc47b54b9f15dc6bc9005a65280a886b2c2e37 **SHA-256 :** 28260f875972606c77a2b0ae4c50ae6037777d64 **SHA-512 :** 9d0ef801ab6d62e2155ab1bb7f70d17b65a20d8 **Size :** 99.481 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Opensans-Bold-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** df57bee75c4ecca2e6bec4793f2dcc99 **SHA-1 :** aac68c6f573368a5380db763a8beb62d189b336c **SHA-256 :** dc84d56ec591269f07466d69fd0e2de2a79c8f44 **SHA-512 :** a0627a1b4122f7699bd0794293f0788b280808a5 **Size :** 41.499 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Proxima_nova_light-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** ee9163c34f600221169f8ff531e97182 **SHA-1 :** 57f0b2c837c94f2a0df47ee62b4639fd6426bfa0 **SHA-256 :** 53f30a622db68cebe92dbd384cc292aef13ad7e3 **SHA-512 :** d51e2a5f6df706eaa2c5ffa071a9a9c08e58a30b4 **Size :** 63.036 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Lte-Ie9[1].Css	**Type :** ASCII text, with very long lines **MD5 :** eb1b588625d45e4bbce3be7cb38bfbef **SHA-1 :** e5585d59a3e5427011652becb45f7e1ff60b89cc **SHA-256 :** f54e1dda592f4e3e6ed8482589ef821085a8eb79 **SHA-512 :** c9608c05dd195fa78c5d6f6413e2a54581d28b3f **Size :** 6.402 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Img\No_internet\No_internet-Step2.Png	**Type :** PNG image data, 210 x 130, 8-bit/color RGBA, non-interlaced **MD5 :** 8bff39ae83783ccacb7175347102549a **SHA-1 :** aa69e573803c07ebeecc502f2a6d3f0e07250d51 **SHA-256 :** 9a940e08c97cdb82c181a98ee99e1c145ac96ba9 **SHA-512 :** 65144e4ed0d6827d9f6053d26b3fb1ba1259e00 **Size :** 1.872 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 98665a1f34390d63f059348507a9bc52 **SHA-1 :** d4486a0ecbf745254b99e69d877dea556f329430 **SHA-256 :** 5117827486982f94f948cb090968e99c52b76805 **SHA-512 :** 247e1b9ffd4f62efa9469d1930389fc3cddff9431e **Size :** 0.34 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Driverpack-7za.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** bea00893c9b3ccf819e2131985e2f15d **SHA-1 :** 2e102c933414f3e42d4aceaadfa34197711f5255 **SHA-256 :** 7b0c35bb84e153defb2f22c409c912a7eadea1e2 **SHA-512 :** d51dc2a252295b20319493519ad77c6576cefd07 **Size :** 661.392 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Img\No_internet\No_internet-Connection.Png	**Type :** PNG image data, 204 x 149, 8-bit/color RGBA, non-interlaced **MD5 :** a43605b4ab97297a27ac68b3747e61fb **SHA-1 :** a9143208894c6a667ce121bd13f57f2f3bf53da3 **SHA-256 :** 677b6ae48b0a71e404d57534f943ef323c41e582 **SHA-512 :** 66fec12729c4b4045ac674274cb5cd15a9cf3453 **Size :** 4.972 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Config.Js	**Type :** ASCII text **MD5 :** 859b7d313e9ae56de24b7409c718e68f **SHA-1 :** f9b0ce15df67e74bd5de3b48a71eb253ee19d647 **SHA-256 :** 9d3415c35614f856d3122d4ade4ed8c7b172ace3 **SHA-512 :** 1f4d28bf86ebef274410cae287966b3b662f8f3f6 **Size :** 3.085 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\IETldCache\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 73f66dbeea4b5833334065f993ae561a **SHA-1 :** 867f37a1dc85bafe6633165b3fab2f7965412afa **SHA-256 :** baf57b866794ac49e94b046b783f96109b3f73cd **SHA-512 :** c15aa8321e9f84672479c17b05a1f58222ee44a6 **Size :** 262.144 Kilobytes.
C:\Users\User\AppData\Local\Temp\3_uhqegk.Cmdline	**Type :** UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators **MD5 :** ab3539125985d96206a71dd7ddaf59ca **SHA-1 :** eec95ff8f2eba3216c2f2399b75cb2ea3a9bb418 **SHA-256 :** 1371d202459c59058d4994ac3bff15053b585f30 **SHA-512 :** d22600fe1c9641b2a33ff5d6bb3a854a15d2d49e **Size :** 0.307 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Roboto[1].Css	**Type :** ASCII text **MD5 :** f5f5b5e4955262430e7b496247425d2d **SHA-1 :** d4bea186a0d525ce3060e8dd7901311ae4a0735a **SHA-256 :** 2537efe2fb974f58cddbc99abfcd7aed6e9df8199 **SHA-512 :** 16a7ec3d95ed773a0a1ce2c2dc4430677106f0d1 **Size :** 1.001 Kilobytes.
C:\Users\User\AppData\Roaming\DRPSu\Temp\Ps.Jfqzb6yi.Qslyd.Cmd.Txt	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators **MD5 :** 3c7be8b8238730308586becaf8bc1528 **SHA-1 :** c8e6bf35dfc10cef8c65b740efaf74a75f1c2ffc **SHA-256 :** e072028133185ab6a0b5333eaf9e102318af6e74 **SHA-512 :** ef7a6a18b066850af913002a407bc9284ca3ed21 **Size :** 1.356 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Roboto-Thin-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** fccc99f55cc8fe49b6757eb00ec75f13 **SHA-1 :** 5f1f59df4e58767e57b7d4c4d1103187ca62824a **SHA-256 :** ac968c15f07a6f899a1c17580714311c62d5d135 **SHA-512 :** 07169d4646916a41da6718514f47e20c67e2834c **Size :** 44.082 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\D93f411851d7c929.CustomDestinations-Ms	**Type :** data **MD5 :** a8ae2c5044908cd62502366cae176d48 **SHA-1 :** 7922dba5946c378697073a58e0d61f5d69d6a15b **SHA-256 :** 92c80a4509e39dddb5ba995db25311773788407 **SHA-512 :** 8a5f665b29b932c893bd6f4a5c68884c44e24fcb **Size :** 8.016 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Lte-Ie8[1].Css	**Type :** ASCII text **MD5 :** aa212039c66d8291bf69d539c386afbb **SHA-1 :** f252ed58cd6465b2630948f35c7d901146daabc0 **SHA-256 :** 43877f60a9f82978c39f9981c64df9de697b6d81c **SHA-512 :** f39d382e428549cf705759e69a66f1ef10d7ea688 **Size :** 1.844 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Normalize.Min[1].Css	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** e8908cf9cb9504b285327d240187f53b **SHA-1 :** 20eadf1695eb38bcd92d1706de5335db61b96502 **SHA-256 :** 86235e2c477078adfe1188d07ca1e5d8198443aa **SHA-512 :** 9c828e8942d40da89f33d1db459a7fc126216603 **Size :** 1.858 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6564 bytes, 1 file **MD5 :** 16e8e953c65d610c3bfc595240f3f5b7 **SHA-1 :** 231a802e6ff1fae42f2b12561fff2767d473210b **SHA-256 :** 048846ed8ed185a26394adeb3f63274d1029bbd **SHA-512 :** 8cf223f68cd118be6bef746d4ccef2bc293e7e0f44 **Size :** 6.564 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Open-Sans[1].Css	**Type :** ASCII text **MD5 :** 9ed298542b45ef98492e159f68e89f48 **SHA-1 :** c4521d9a5dff8a71804c40a909378e8eb5bd66c2 **SHA-256 :** b9bd51ae6ccc7df20417e0ef341295b86bf8f74f6 **SHA-512 :** 1c7d5b378d6c627fbbef864035b157c3e7647b69 **Size :** 1.392 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD	**Type :** data **MD5 :** f0e1de312ef315d20a9d70272744119a **SHA-1 :** e1417322654df980fa3be21e4ec11b20d884bd63 **SHA-256 :** 6db3eaf119f7dfdbadc91f0a367af82ca098b1f125 **SHA-512 :** 96ec814ba4f6e2efeb46a2e6d34302670472cce0 **Size :** 0.244 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\DriverPack.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** c0ca26c103f6bd073484470241458623 **SHA-1 :** d58a2716c80ed21899d685646953ada4973d8cf6 **SHA-256 :** 16d3f869cb262e5448342ad0123b6a45b0e9abc5 **SHA-512 :** 8d53cacb7f665545f20e35a58ef562d94edc56dc7 **Size :** 77.96 Kilobytes.
C:\Users\User\AppData\Local\Temp\3_uhqegk.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 6582994ccef775773a5cbaa3ae20ed71 **SHA-1 :** 55364270921316ae3e75a547f621d9fc6d2cc633 **SHA-256 :** 207f612423e351665df4d16e05bcbc4c6f8b3583 **SHA-512 :** 9a6cf91fd99924459d8e747d98657730269f574f5 **Size :** 3.584 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Img\Screens\New-Logo.Png **C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\New-Logo[1].Png**	**Type :** PNG image data, 371 x 165, 8-bit/color RGBA, non-interlaced **MD5 :** 3878a76a6b6724b2f7847e13cce4b320 **SHA-1 :** 96a39b7ea48a99d09f6ea65f911bb696c3900603 **SHA-256 :** 78d8a5c194abf73d655126c8cd09fba5ca4b46f37 **SHA-512 :** dfda00b0daebb0812335318e4381d83d3da273d **Size :** 12.133 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Run.Hta	**Type :** HTML document, UTF-8 Unicode text, with very long lines **MD5 :** 27cbad32cdf9e772949b9fffba8929e6 **SHA-1 :** a6e71dae63d5400c67bbfb5981aac65239cd5522 **SHA-256 :** 11e026c306d8da6a9091fc426bf942f876f3064f1 **SHA-512 :** 110927a3a9706bb5e7abb57e262456ff6fc479e3 **Size :** 16.611 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\3_uhqegk.0.Cs	**Type :** UTF-8 Unicode (with BOM) text, with very long lines **MD5 :** 91758722dc7e495caa693882723676a2 **SHA-1 :** 7dc3b526c084605a82acf57f3f1884795b67a7b8 **SHA-256 :** afaee024b1d79b00a1db67cb4f03bc2dad739022 **SHA-512 :** 0cdad9195c3ab82e0da68fb1783ecc2636d7b3b6 **Size :** 0.496 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Roboto-Regular-Webfont[1].Eot	**Type :** Embedded OpenType (EOT) **MD5 :** 421fb62d91794710d5d619e8e6cbcef2 **SHA-1 :** 78c81537a3eccf79df8fc7fa7e01be868e403f62 **SHA-256 :** 989894dded80beddf3970f998c8a53d34d083a7c **SHA-512 :** edee257cb727e157198702e9ff7984ecbf65a5841 **Size :** 52.409 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZipSfx.000\Bin\Tools\Img\Loading.Gif	**Type :** GIF image data, version 89a, 400 x 400 **MD5 :** a90e737d05ebfa82bf96168def807c36 **SHA-1 :** ddc76a0c64ebefe5b9a12546c59a37c03d5d1f5b **SHA-256 :** 24ed9db3eb0d97ecf1f0832cbd30bd37744e0d2b **SHA-512 :** bf1944b5daf9747d98f489eb3edbae84e7bc29ff5 **Size :** 19.11 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	DriverPack-17-Online_903364983.1505480122.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	332c6d7a41782059a0ce7bb28047a76f91b34a98
MD5:	8cf070e06d243b0966fed6bb24c955b2
First Seen Date:	2017-09-16 00:25:57.489669 (2 years ago)
Number Of Clients Seen:	5
Last Analysis Date:	2018-03-02 12:59:53.756060 (about a year ago)
Human Expert Analysis Date:	2019-07-22 09:35:33.254986 (33 minutes ago)
Human Expert Analysis Result:	PUA

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	4
Trid	[[50.0, u'Generic Win/DOS Executable'], [49.9, u'DOS Executable Generic']]
Compilation Time Stamp	0x5700444A [Sat Apr 2 22:14:34 2016 UTC]
LegalCopyright	Copyright \xa9 Kuzyakov Artur
InternalName	DriverPack
FileVersion	1.0
CompanyName	DriverPack
PrivateBuild	2016
ProductName	DriverPack
ProductVersion	1.0
FileDescription	DriverPack
OriginalFilename	DriverPack.exe
Translation	0x0000 0x04b0
Entry Point	0x41c35f (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	282040
Ssdeep	6144:75VP9Ge3+hoAvdeJBbLncZjOEj5hoNvPrzziF+Mp:75393whFOBbnM5hoNXvziFf
Sha256	3959275e664d29b44b85a000534da249daf4614d460bd8954bb9b35a6202ab13
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'EXE:PrivateBuild': 2016, u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/3/2/c/332c6d7a41782059a0ce7bb28047a76f91b34a98', u'EXE:OriginalFileName': u'DriverPack.exe', u'EXE:ProductName': u'DriverPack', u'EXE:InternalName': u'DriverPack', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:03:02 12:58:39+00:00', u'EXE:InitializedDataSize': 64512, u'File:FileModifyDate': u'2018:03:02 12:58:39+00:00', u'EXE:FileVersionNumber': u'1.0.0.0', u'EXE:FileVersion': 1.0, u'File:FileSize': u'275 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': 1.0, u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'DriverPack', u'File:FileName': u'332c6d7a41782059a0ce7bb28047a76f91b34a98', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2016:04:02 22:14:34+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 Kuzyakov Artur', u'EXE:LinkerVersion': 8.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/3/2/c', u'EXE:FileDescription': u'DriverPack', u'EXE:EntryPoint': u'0x1c35f', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 114176, u'File:FileInodeChangeDate': u'2018:03:02 12:58:39+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	a1a66d588dcf1394354ebf6ec400c223

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1bd4a	0x1be00	6.71052533174	c820c58aedd8916d0cfdfacf6518a796
.rdata	0x1d000	0x41a8	0x4200	5.74601891947	61e5f1569be02d293c2f1941c8014c11
.data	0x22000	0x4c90	0x800	3.69661077531	df838379d053bbc0adb49e5333be876c
.rsrc	0x27000	0x6b0d	0x6c00	5.43214401076	d1f865c117acd85aed0af4a692fe0cdc

PE Imports

- COMCTL32.dll
  - None
- SHELL32.dll
  - ShellExecuteExW
  - ShellExecuteW
  - SHGetMalloc
  - SHGetPathFromIDListW
  - SHBrowseForFolderW
  - SHGetFileInfoW
  - SHGetSpecialFolderPathW
- GDI32.dll
  - CreateCompatibleDC
  - CreateFontIndirectW
  - DeleteObject
  - DeleteDC
  - GetCurrentObject
  - StretchBlt
  - GetDeviceCaps
  - CreateCompatibleBitmap
  - SelectObject
  - SetStretchBltMode
  - GetObjectW
- ADVAPI32.dll
  - FreeSid
  - AllocateAndInitializeSid
  - CheckTokenMembership
- USER32.dll
  - GetParent
  - ScreenToClient
  - CreateWindowExW
  - GetDesktopWindow
  - GetWindowTextLengthW
  - SetWindowPos
  - SetTimer
  - GetMessageW
  - CopyImage
  - KillTimer
  - CharUpperW
  - SendMessageW
  - ShowWindow
  - BringWindowToTop
  - wsprintfW
  - MessageBoxW
  - EndDialog
  - ReleaseDC
  - GetWindowDC
  - GetMenu
  - GetWindowLongW
  - GetClassNameA
  - wsprintfA
  - DispatchMessageW
  - SetWindowTextW
  - GetSysColor
  - DestroyWindow
  - MessageBoxA
  - GetKeyState
  - IsWindow
  - GetDlgItem
  - GetClientRect
  - GetSystemMetrics
  - SetWindowLongW

    - UnhookWindowsHookEx
    - SetFocus
    - SystemParametersInfoW
    - DrawTextW
    - GetDC
    - ClientToScreen
    - GetWindow
    - DialogBoxIndirectParamW
    - DrawIconEx
    - CallWindowProcW
    - DefWindowProcW
    - CallNextHookEx
    - PtInRect
    - SetWindowsHookExW
    - LoadImageW
    - LoadIconW
    - MessageBeep
    - EnableWindow
    - EnableMenuItem
    - GetSystemMenu
    - CreateWindowExA
    - wvsprintfW
    - GetWindowTextW
    - GetWindowRect
- ole32.dll
    - CreateStreamOnHGlobal
    - CoCreateInstance
    - CoInitialize
- OLEAUT32.dll
    - SysAllocStringLen
    - VariantClear
    - SysFreeString
    - OleLoadPicture
    - SysAllocString
- KERNEL32.dll
    - SetFileTime
    - SetEndOfFile
    - GetFileInformationByHandle
    - VirtualFree
    - GetModuleHandleA
    - WaitForMultipleObjects
    - VirtualAlloc
    - ReadFile
    - SetFilePointer
    - GetFileSize
    - LeaveCriticalSection
    - EnterCriticalSection
    - DeleteCriticalSection
    - FormatMessageW
    - lstrcpyW
    - LocalFree
    - IsBadReadPtr
    - GetSystemDirectoryW
    - GetCurrentThreadId
    - SuspendThread
    - TerminateThread
    - InitializeCriticalSection
    - ResetEvent
    - SetEvent
    - CreateEventW
    - GetVersionExW
    - GetModuleFileNameW
    - GetCurrentProcess
    - SetProcessWorkingSetSize
    - SetEnvironmentVariableW
    - GetDriveTypeW
    - CreateFileW
    - LoadLibraryA
    - SetThreadLocale
    - GetSystemTimeAsFileTime
    - ExpandEnvironmentStringsW
    - CompareFileTime
    - WideCharToMultiByte
    - GetTempPathW
    - GetCurrentDirectoryW

    - GetEnvironmentVariableW
    - lstrcmpiW
    - GetLocaleInfoW
    - MultiByteToWideChar
    - GetUserDefaultUILanguage
    - GetSystemDefaultUILanguage
    - GetSystemDefaultLCID
    - lstrcmpiA
    - GlobalAlloc
    - GlobalFree
    - MulDiv
    - FindResourceExA
    - SizeofResource
    - LoadResource
    - LockResource
    - GetModuleHandleW
    - FindFirstFileW
    - lstrcmpW
    - DeleteFileW
    - FindNextFileW
    - FindClose
    - RemoveDirectoryW
    - GetStdHandle
    - WriteFile
    - lstrlenA
    - CreateDirectoryW
    - GetFileAttributesW
    - SetCurrentDirectoryW
    - GetLocalTime
    - SystemTimeToFileTime
    - CreateThread
    - GetExitCodeThread
    - Sleep
    - SetFileAttributesW
    - GetDiskFreeSpaceExW
    - SetLastError
    - GetTickCount
    - lstrlenW
    - ExitProcess
    - lstrcatW
    - GetProcAddress
    - CloseHandle
    - WaitForSingleObject
    - GetExitCodeProcess
    - GetQueuedCompletionStatus
    - ResumeThread
    - SetInformationJobObject
    - CreateIoCompletionPort
    - AssignProcessToJobObject
    - CreateJobObjectW
    - GetLastError
    - CreateProcessW
    - GetStartupInfoW
    - GetCommandLineW
    - GetStartupInfoA
- MSVCRT.dll
    - _purecall
    - ??2@YAPAXI@Z
    - _wtol
    - memset
    - memmove
    - memcpy
    - _wcsnicmp
    - _controlfp
    - _except_handler3
    - __set_app_type
    - __p__fmode
    - __p__commode
    - _adjust_fdiv
    - __setusermatherr
    - _initterm
    - __getmainargs
    - _acmdln
    - exit
    - _XcptFilter

- _exit
- ??1type_info@@UAE@XZ
- _onexit
- __dllonexit
- malloc
- realloc
- free
- wcsstr
- _CxxThrowException
- _beginthreadex
- _EH_prolog
- ?_set_new_handler@@YAP6AHI@ZP6AHI@Z@Z
- strncmp
- wcsncmp
- wcsncpy
- strncpy
- ??3@YAXPAX@Z

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 160432, u'sha256': u'ea28f92489b751859c260f8817282bbeb21a3ab47317ec1fedcc7ebc28aa557c', u'type': u'dBase IV DBT of `.DBF, block length 1536, next free block index 40, next free block 2130706656, next used block 65535', u'size': 1640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 162072, u'sha256': u'11323b44ce2c28580214713f4784ae8da6749c44951386d72f9df6caf6d0d03f', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 162816, u'sha256': u'8ba587c1f520a47113a3468d25cff4dd47e434ef95951d5e7731a4dc9a780628', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 163112, u'sha256': u'3a5698fc42b4d31610a49072eec57242ac8e977e8dd5af47e3d174e5c14dfba1', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 166864, u'sha256': u'f63eaa288005e2d691b12aace051ee8473f33c498582e3762a20e103f2392325', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 169080, u'sha256': u'8f23d302942e7828a00a9abe2125f7ec04125058ea92c55b4353a4cf99d244aa', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 170464, u'sha256': u'89d92e824bbb9952dd81fab0bce0d384c2fa13d1dd72340db72c1c6af488004a', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 180104, u'sha256': u'826b20d161cf090f0f4a6507347dcd1e1683e1fa53b91616d029610fe0a3282a', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 184368, u'sha256': u'5657f700b26de46eefc55a7ed2b7d20525b47bf51fcf7748a065a1f18593a9ba', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 185496, u'sha256': u'ca82878ac6f8f5d26249f03257b496eebf06e2d20e02349a0b871bf92766535c', u'type': u'MS Windows icon resource - 9 icons, 48x48, 16 colors', u'size': 132}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 185628, u'sha256': u'0b6b9526c643bfe34256a290466ef3c0a3ccf7cfad80252690ad99f8e33d2725', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 186372, u'sha256': u'1cbef81a3cbf8967be403cb25f824f41bf9f1bea039cb56e9c7d5e1b740c4d90', u'type': u'ASCII text', u'size': 777}

CERTIFICATE VALIDATION

- Success ✔

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

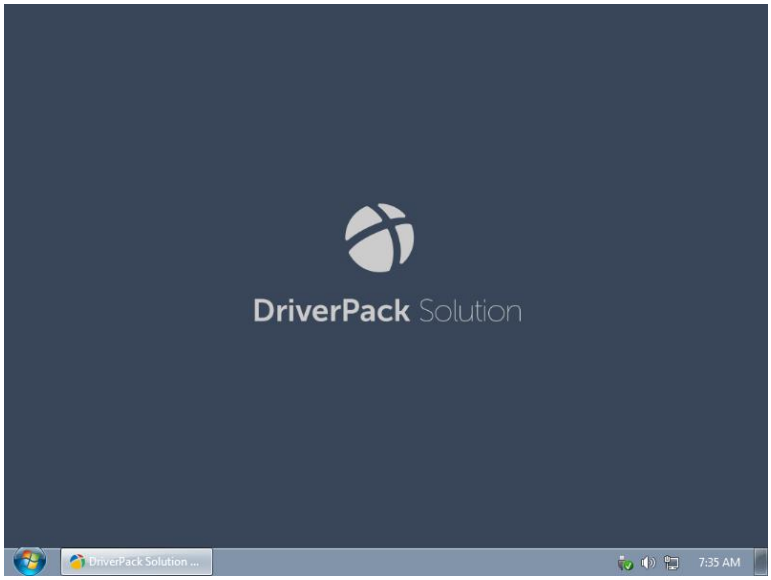
[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 00:00:00
End Date	2020-12-30 23:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
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)"}

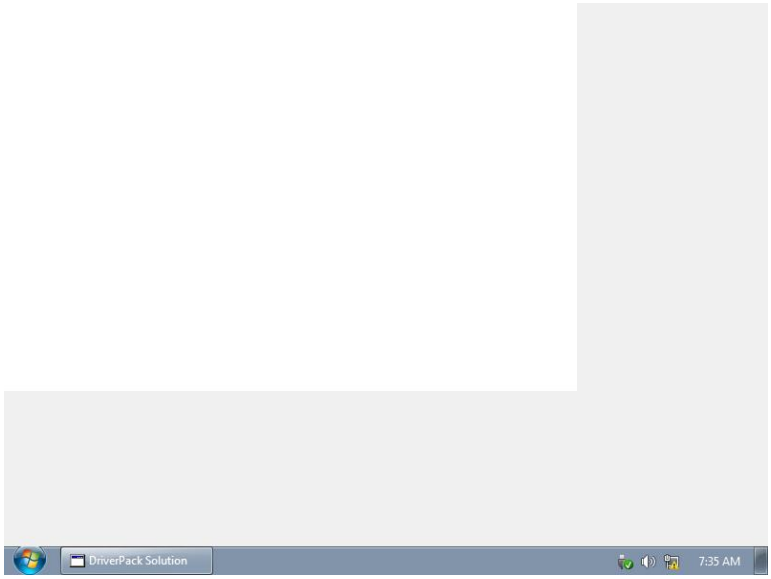
[+] VeriSign Class 3 Public Primary Certification Authority - G5	
Status	NoError ✔
Start Date	2006-11-08 00:00:00
End Date	2036-07-16 23:59:59
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb 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	null
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

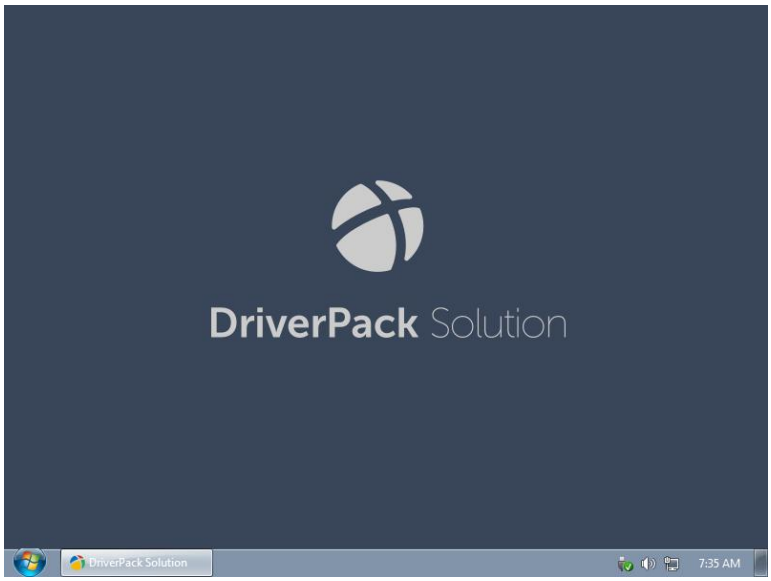
[+] Symantec Class 3 SHA256 Code Signing CA	
Status	NoError ✔
Start Date	2013-12-10 00:00:00
End Date	2023-12-09 23:59:59
Sha256	0649cde463467e8e26bb6b7c23965e030248f95df21f6dcf28c51507fbb77c08
Serial	3D78D7F9764960B2617DF4F01ECA862A
Subject Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca 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)"}

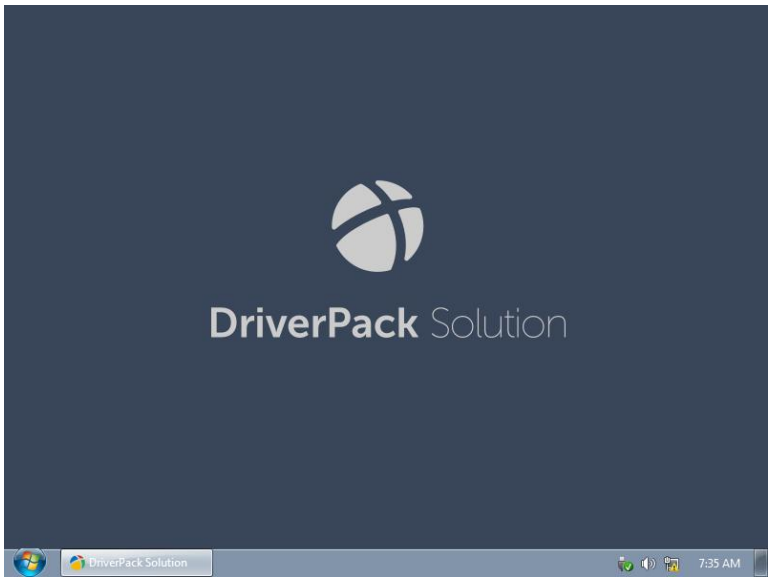
[+] Kuzyakov Artur Vyacheslavovich IP	
Status	NoError ✔
Start Date	2016-02-01 00:00:00
End Date	2018-04-01 23:59:59
Sha256	d5a7a8a629505595f4ff315e705c9bea4493d82cdcdfe1ae6a5e28fad34c6cca
Serial	158377DA2BD81EDC1F1DF9B7E343B3CB
Subject Key Identifier	8f 27 88 37 bb 1d 73 ad cd 15 7f c7 53 f2 87 7e c2 49 49 66
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)"}

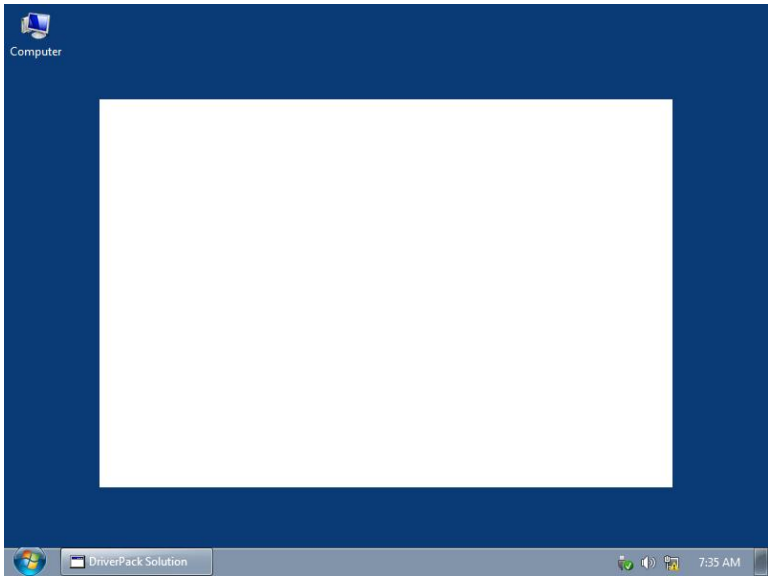
SCREENSHOTS

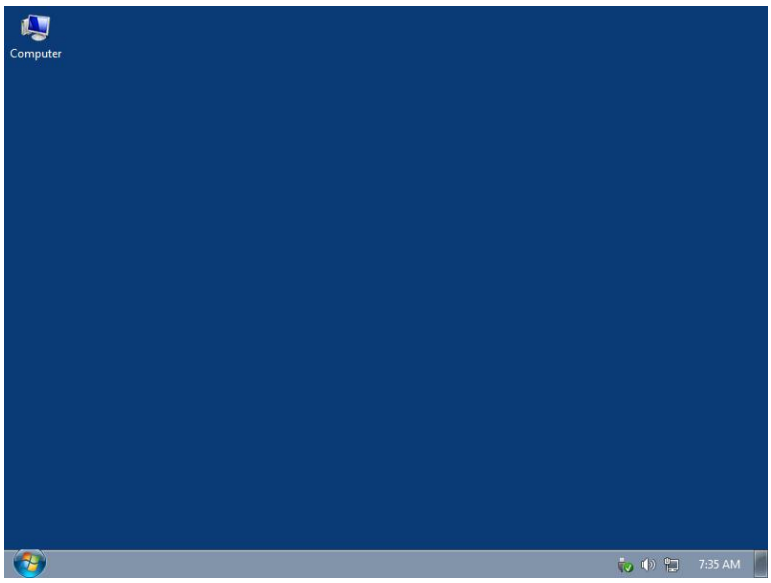

DriverPack Solution
DriverPack Solution ...
7:35 AM

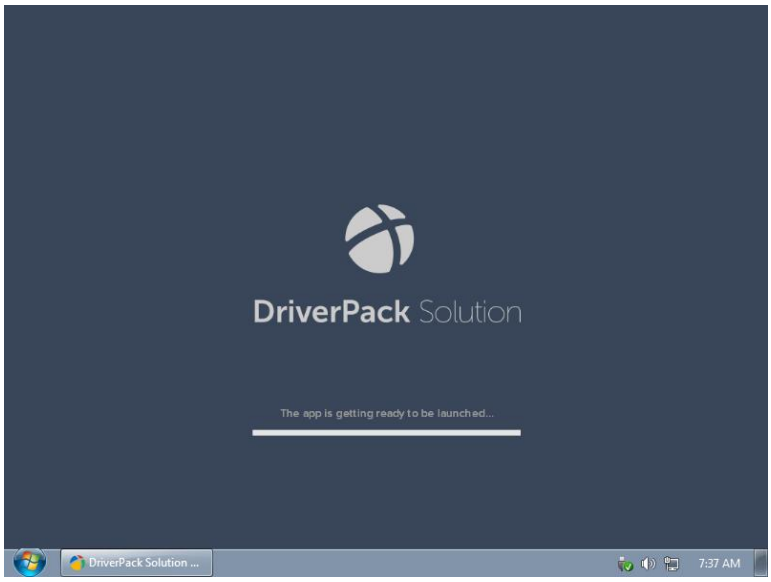

DriverPack Solution
7:35 AM

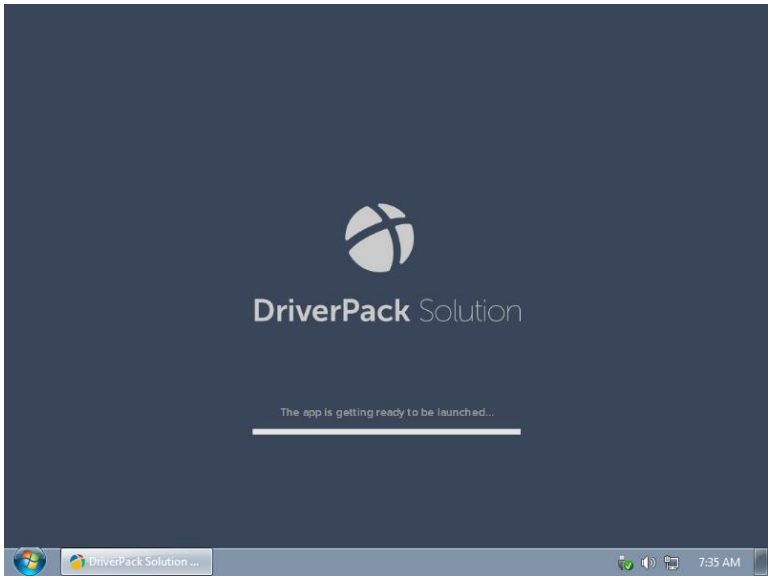

DriverPack Solution
DriverPack Solution
7:35 AM

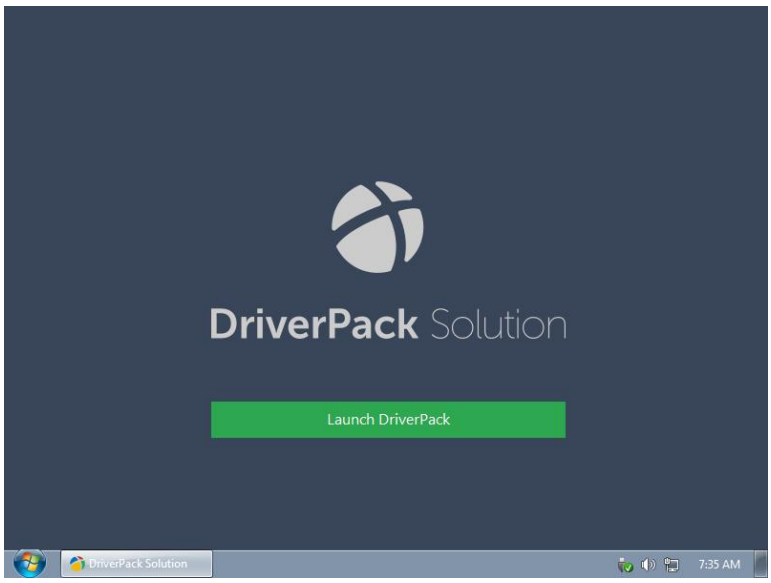

DriverPack Solution
DriverPack Solution
7:35 AM

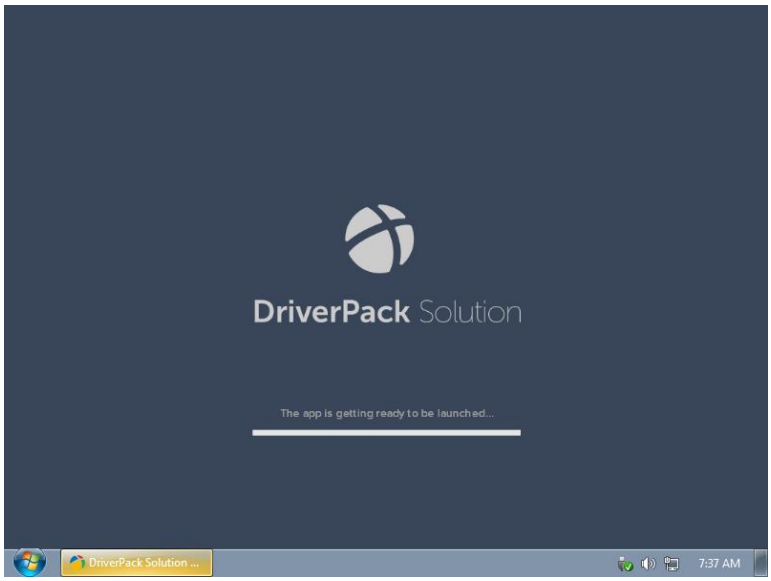

Computer
DriverPack Solution
7:35 AM

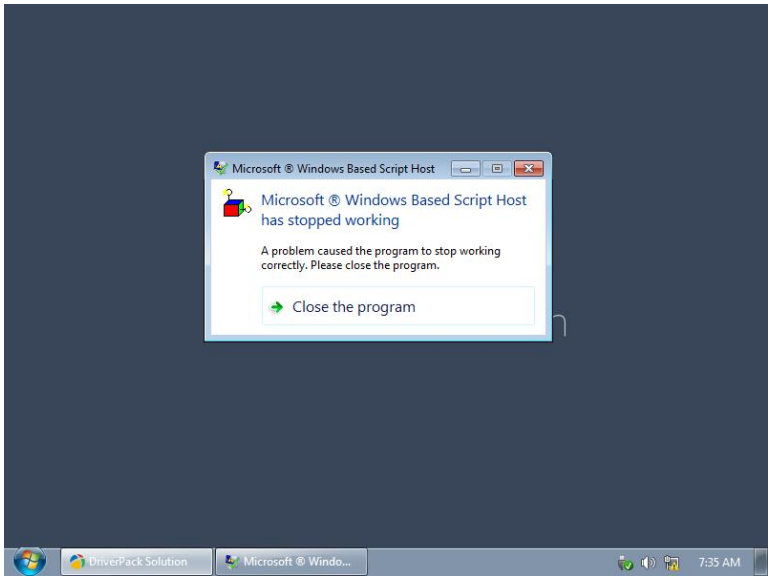

Computer
7:35 AM


DriverPack Solution
The app is getting ready to be launched...
DriverPack Solution ...
7:37 AM


DriverPack Solution
The app is getting ready to be launched...
DriverPack Solution ...
7:35 AM


DriverPack Solution
Launch DriverPack
DriverPack Solution
7:35 AM


DriverPack Solution
The app is getting ready to be launched...
DriverPack Solution ...
7:37 AM


Microsoft ® Windows Based Script Host
Microsoft ® Windows Based Script Host has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
DriverPack Solution
Microsoft ® Windo...
7:35 AM