Sample: 40e751c032c75d33c807219b2de6c584

P3pper Reports - **http://www.peppermalware.com**.

P3pper Twitter - **https://twitter.com/P3pperP0tts**.

This report has been generated automatically by a set of malware analysis tools.

Classification: **#TROJAN #OCCAMY** (based on p3pperp0tts rules)

Analysis date: 2019-04-12 07:11:35 (p3pperp0tts platform's analysis date)

Exe timestamp: 2018-06-10 10:14:01 (timestamp of the original sample)

Unpacked mods max timestamp: 2018-06-10 10:14:01 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2019-04-09 04:22:11 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: 40e751c032c75d33c807219b2de6c584

AV detections

- Microsoft: Trojan:Win32/Occamy.C
- Kaspersky: HEUR:Trojan.Win32.Generic
- Symantec:
- Malwarebytes: Trojan.Dropper.Generic

Source

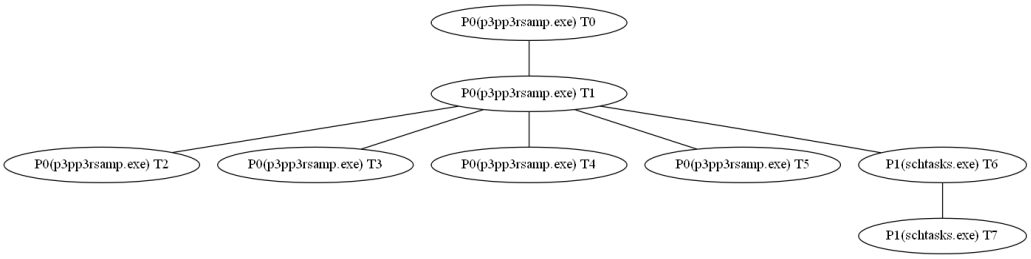
- hxxp://54.38.22.53/spike/svchost.exe

Virustotal

- https://virustotal.com/es/file/d15c5d86d4928052e085de35133520dec742c1b43a320603e46e5197e98ee881/analysis

Threads tree

The following tree represents sample's threads. T<index> is an alias for sample's threads (numeration is done in the order of threads creation). P<index> is an alias for processes owning sample's threads.



Most interesting behavior

The following list it's a collection of the most interesting events captured. This list is ordered by the score assigned to the event. In the section "Threads behavioural information" it's possible to find all the actions performed by each sample's thread ordered chronologically.

- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3rsamp.exe Type: REG_DWORD, Length: 4, Data: 8888)
- RegCreateKey (HKCU\\Software Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer\\Main Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl Desired Access: Maximum Allowed, Granted Access: None 0x0, Disposition: REG_CREATED_NEW_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION Desired Access: Read/Write, Disposition: REG_CREATED_NEW_KEY)
- RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3rsamp.exe Type: REG_DWORD, Length: 4, Data: 8888)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3rsamp.vshost.exe Type: REG_DWORD, Length: 4, Data: 8888)
- RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3rsamp.vshost.exe Type: REG_DWORD, Length: 4, Data: 8888)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.exe Type: REG_DWORD, Length: 4, Data: 8888)
- RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.exe Type: REG_DWORD, Length: 4, Data: 8888)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.vshost.exe Type: REG_DWORD, Length: 4, Data: 8888)
- RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.vshost.exe Type: REG_DWORD, Length: 4, Data: 8888)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.exe Type: REG_DWORD, Length: 4, Data: 8)
- RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.exe Type: REG_DWORD, Length: 4, Data: 8)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.vshost.exe Type: REG_DWORD, Length: 4, Data: 8)
- RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.vshost.exe Type: REG_DWORD, Length: 4, Data: 8)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32 Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)

• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
• RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\syscheck Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
• Process Create (C:\\Windows\\system32\\schtasks.exe PID: P1, Command line: "schtasks.exe" /create /sc minute /mo 1 /tn "Decp3pp3r" /tr "C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe")
• Thread Create (Thread ID: T1)
• Thread Create (Thread ID: TUNKALIAS)
• Thread Create (Thread ID: T2)
• Thread Create (Thread ID: T3)
• RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION Desired Access: Read/Write)
• Thread Create (Thread ID: T4)
• Thread Create (Thread ID: T5)
• Thread Create (Thread ID: T7)

Most interesting strings

The following list it's a collection of the most interesting strings found in the sample's modules (unpacked modules too) code or data.

- <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
- !This program cannot be run in DOS mode.
- <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/;q=0.8
- Accept-Encoding: gzip, deflate, br
- AssemblyBuilder
- set_Position
- System.IO.Compression
- GetCustomAttributes
- get_FieldHandle
- get_CurrentDomain
- System.Resources
- GetHostAddresses
- GetUnderlyingType
- System.Runtime.Serialization
- get_OriginalString
- IsAssignableFrom
- get_IsInterface
- StringFileInfo
- KeyValuePair`2
- System.CodeDom.Compiler
- IsInstanceOfType
- getElementsByTagName
- get_Assembly
- MakeByRefType
- DeflateStream
- GetConstructors
- AssemblyNameFlags
- get_IsValueType
- <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
- GetParameters
- LocalCertificateSelectionCallback
- add_AssemblyResolve
- AllocHGlobal
- set_ContentType
- Assembly Version
- set_ScriptErrorsSuppressed
- LocalBuilder
- get_ParameterType
- set_ContentLength
- VS_VERSION_INFO
- get_ReturnType
- GetDynamicILInfo
- get_TypeHandle
- OriginalFilename
- DeclareLocal
- AppendFormat
- CompressionMode

- get_ReadyState
- MakeGenericType
- get_ElapsedMilliseconds
- get_IsPointer
- DynamicILInfo
- </trustInfo>
- </requestedPrivileges>
- LocalMachine
- ResolveSignature
- ModuleBuilder
- HttpResponseHeader
- get_BaseType
- ParameterInfo
- GetValueOrDefault
- AssemblyName
- DebuggingModes
- oiTDMIW}^ln"o\\,pEA\\\\-\\,i5%6%.resources
- GetTargetType
- DefineDynamicAssembly
- GetManifestResourceStream
- GetAssemblies
- get_IsConstructor
- get_DeclaringType
- get_MethodHandle
- get_IsPrimitive
- SetLocalSignature
- GetRequestStream
- BindingFlags
- AssemblyBuilderAccess
- InvokeMember
- get_FieldType
- PropertyInfo
- <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
- get_CultureInfo
- ResourceManager
- get_IsVirtual
- GetOptionalCustomModifiers
- LegalCopyright
- get_Document
- CustomAttributeBuilder
- ResolveEventArgs
- get_MetadataToken
- GetFunctionPointer
- ResolveEventHandler
- get_HasValue
- FormatterServices
- get_IsStatic
- InternalName
- get_InnerException
- IsLittleEndian
- +j|Zf 'Tc!a}
- GetElementType
- ERROR_NO_MORE_ITEMS
- get_LocalPath
- RuntimeHelpers
- get_MainWindowTitle
- set_Arguments

- set_UserAgent
- SuspendThread
- AddressFamily
- get_OperationalStatus
- KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingleFileGenerator
- System.Net.Security
- PAGE_EXECUTE
- System.Windows.Forms
- System.Drawing
- System.Security.Cryptography.X509Certificates
- get_Position
- get_IsAbstract
- HttpWebResponse
- GCHandleType
- PAGE_READONLY
- PAGE_NOCACHE
- set_ServerCertificateValidationCallback
- set_ProtocolVersion
- IPGlobalProperties
- {0} /{1} HTTP/1.1
- G(G8GHGXGcGvG
- ExpandEnvironmentVariables
- GetIPGlobalProperties
- get_CurrentThread
- DWebBrowserEvents2_BeforeNavigate2EventHandler
- GetExecutingAssembly
- GetResponseStream
- L!L-L<LHLTLiL
- ApplicationSettingsBase
- get_BaseAddress
- ManagementObjectSearcher
- WebBrowserDocumentCompletedEventHandler
- set_DefaultConnectionLimit
- S@LT&KE4343242343Y;
- GetProcesses
- System.Net.Sockets
- FileIOPermissionAccess
- remove_DocumentCompleted
- SUSPEND_RESUME
- INTERNET_COOKIE_HTTPONLY
- ExecuteWriteCopy
- ReadAllBytes
- gzip, deflate, br
- StringBuilder
- DownloadString
- gzip, deflate, sdch, br
- System.Net.NetworkInformation
- GetAllNetworkInterfaces
- set_CreateNoWindow
- RtlSetProcessIsCritical
- get_CharacterSet
- get_BytesReceived
- NetworkStream
- set_UseShellExecute
- System.Security.Principal
- EnterDebugMode
- get_TickCount

- ResolveMember
- set_IsBackground
- sslPolicyErrors
- NetworkAccess
- HttpStatusCode
- OperationalStatus
- get_Location
- System.Security.Permissions.SecurityPermissionAttribute, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
- PasswordHash
- get_BytesSent
- IsWow64Process
- HttpWebRequest
- ReadAllLines
- WriteCombineModifierflag
- System.Runtime.CompilerServices
- MemoryStream
- CryptoStreamMode
- SpecialFolder
- WebBrowserBase
- GetProcessesByName
- NB2.Properties
- StreamWriter
- System.Runtime.InteropServices
- get_StatusCode
- NoCacheModifierflag
- get_LocalEndPoint
- get_ProcessName
- set_Expect100Continue
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- H&H.H6H;:HGHMHVHdHmH
- BinaryReader
- CryptoStream
- User-Agent: {0}
- get_PrimaryScreen
- WrapNonExceptionThrows
- SymmetricAlgorithm
- get_Connected
- _remoteStackTraceString
- IAsyncResult
- ScriptEngine
- get_FileName
- PAGE_WRITECOMBINE
- GetFolderPath
- get_FullyQualifiedName
- PAGE_EXECUTE_READWRITE
- set_FileName
- SettingsBase
- ConstructorInfo
- Upgrade-Insecure-Requests: 1
- get_ExecutablePath
- set_KeepAlive
- get_ThreadState
- AceQualifier
- PAGE_READWRITE
- get_UserName
- get_MainModule

- get_ActiveXInstance
- ZwSetInformationProcess
- get_RemoteEndPoint
- System.Runtime.ExceptionServices.ExceptionDispatchInfo
- get_NetworkInterfaceType
- SecurityIdentifier
- GetCurrentProcess
- INTERNET_COOKIE_THIRD_PARTY
- SET_THREAD_TOKEN
- INTERNET_FLAG_RESTRICTED_ZONE
- FromBase64String
- CookieContainer
- System.Threading
- GetValueNames
- lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- Connection: Keep-Alive
- ServicePointManager
- GetResourceString
- Cache-Control: no-cache
- get_ServerCertificateValidationCallback
- WebBrowserDocumentCompletedEventArgs
- get_IsAttached
- ProtocolType
- WellKnownSidType
- PAGE_NOACCESS
- set_UseNagleAlgorithm
- get_ModuleMemorySize
- StreamReader
- NetworkInterfaceType
- CreateRemoteThread
- System.Reflection.Emit
- RoaZ .PQua8g
- get_DiscretionaryAcl
- Rfc2898DeriveBytes
- GuardModifierflag
- Accept-Encoding
- ProcessStartInfo
- PAGE_WRITECOPY
- $88b6efb0-83b0-4cbd-a2d9-3a37200bd51b
- get_ProcessorCount
- GetEntryAssembly
- ProcessThread
- ReadOnlyCollectionBase
- ERROR_INSUFFICIENT_BUFFER
- PAGE_EXECUTE_READ
- BitConverter
- GetCommandLineArgs
- get_IsAbsoluteUri
- RemoteCertificateValidationCallback
- ERROR_INVALID_PARAMETER
- get_BinaryLength
- 3System.Resources.Tools.StronglyTypedResourceBuilder
- AsyncCallback
- SET_INFORMATION
- set_WindowStyle
- PAGE_EXECUTE_WRITECOPY

- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- ReadProcessMemory
- VirtualProtectEx
- IsDebuggerPresent
- CheckRemoteDebuggerPresent
- VirtualAllocEx
- WriteProcessMemory
- InternetGetCookieExW
- SetKernelObjectSecurity
- GetPhysicallyInstalledSystemMemory
- GetKernelObjectSecurity
- VirtualQueryEx
- NtUnmapViewOfSection

Hosts

- 192.168.149.142:49160
- 192.168.149.142:49161
- 54.38.92.92:80
- 80.82.64.205:1928

Dns queries

- isatap.localdomain ---> no answers
- 255.149.168.192.in-addr.arpa ---> no answers
- 2.149.168.192.in-addr.arpa ---> no answers
- 254.149.168.192.in-addr.arpa ---> no answers

Network traffic

This section contains the readable content of the captured network traffic classified by established connections.

- **tcp 192.168.149.142:49160 ---> 54.38.92.92:80**

GET /line/ HTTP/1.1[...]Connection: Keep-Alive[...]Host: ip-api.com[...]GET /line/ HTTP/1.1

- **tcp 54.38.92.92:80 ---> 192.168.149.142:49160**

Content-Type: text/plain; charset=UTF-8[...]HTTP/1.1 200 OK[...]Content-Length: 121[...]Date: Fri, 12 Apr 2019 04:58:54 GMT[...]Access-Control-Allow-Origin: *[...]HTTP/1.1 200 OK[...]AS9009 M247 Ltd[...]195.206.107.118[...]Europe/Madrid

- **tcp 192.168.149.142:49161 ---> 80.82.64.205:1928**

NICK [NEW][ES]p3pp3r|7239[...]USER [NEW][ES]p3pp3r|7239 0 * [NEW][ES]p3pp3r|7239[...]PONG :DA629672[...]JOIN #paradox

- **tcp 80.82.64.205:1928 ---> 192.168.149.142:49161**

:wee.wee.wee 254 [NEW][ES]p3pp3r|7239 4 :channels formed[...]:wee.wee.wee 366 [NEW][ES]p3pp3r|7239 #paradox :End of /NAMES list.[...]:[ID]KARINA|67816!~IDKARINA@F7505680.FD1D344D.85392EBA.IP JOIN :#paradox[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[ID]ASUS|87861 [TH]Administrator|1511 [JM]jay|96793 [MM]Best|68904 [VN]quoc|36846 [VN]USER|89682 [IN]india|20043 [VN]Nam|93466 [PH]User|37835 [VN]Admin|9390 [KH]long|83776 [PH]STI [RO]Parinti|48985 [PH]Pur[...]:[BR]Adm|51673!~BRAdm51@FBC0893E.B58149F7.DD2D601B.IP QUIT :Ping timeout: 380 seconds[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[IN]Vanita|87376 [ID]ADAMS [TZ]TPSC [TW]20141020|38668 [IN]admin|37672 [sai][7075]|F [DZ]TOSHIBA|37607 [PL]kulka|93154 [NP]User|19895 [IN]admin|25719 [PC][19597]|F [ID]user|22837 [IN]pc25|85633 [IN]rAHIl|4[...]:[IN]Green!~INGreen@12FE7B6A.548C640F.4EAB93A8.IP JOIN :#paradox[...]:[IN]intex|76708!~INintex@B09E8877.6150971D.AAEFEB35.IP JOIN :#paradox[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[DZ]Hinfo|69235 [US]Prudent|38179 [ID]USER|38110 [User][82509]|F [aqil][90189]|F [PK]GAMERX|28192 [VN]vu [PL]MAX|91456 [TR]CANNUR|47075 [VN]Administrator|98607 [IN]pankaj|75977 [JP]Administrator|69910 [BR][...]:[IN]Lenovo|81616!~INLenovo@482BEF13.73B13C3F.60D93FB2.IP JOIN :#paradox[...]:KiloAlpha!KiloAlpha@admin PRIVMSG #paradox :STOP https://da.tomatoes.host:2222/[...]:[toshiba][34539]|F!~toshiba@BE6EF9EF.A384C951.E4A7C77C.IP QUIT :Ping timeout: 380 seconds[...]:wee.wee.wee 253 [NEW][ES]p3pp3r|7239 15 :unknown connection(s)[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[PK]Fahad [LG][7565]|F [PK]My [BEG][14655]|F [PH]admin|14814 [EC]Satellite|22384 [IN]Koustubh|87598 [IN]Sanjayp|81084 [Kirti][10456]|F [3Starhospital][70748]|F [PK]HP|28976 [IN]shine|35678 [VN]osc4455|1961[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[NEW][VN]Administrator|82704 [NEW][TH]Administrator|42698 [MN]user|46084 [MX]usuario|86050 [ZA]Betxchange|50561 [ID]YULIPDL|24630 [ID]ASUS|42146 [MA]Student|66684 [CN]Administrator|138 [TH]Online|90268 [VE[...]:[US]EntirelyOiled|86045!~USEntire@he-C44A054A.zoominternet.net QUIT :Ping timeout: 380 seconds[...]:wee.wee.wee 422 [NEW][ES]p3pp3r|7239 :MOTD File is missing[...]:wee.wee.wee 002 [NEW][ES]p3pp3r|7239 :Your host is wee.wee.wee, running version UnrealIRCd-4.0.1[...]:[PK]psl4|59060!~PKpsl45@CBE13960.67B4FE4B.3C553E9B.IP QUIT :Ping timeout: 380 seconds[...]:[IN]Sanjay|775!~INSanjay@8EE88B62.12503622.98BB2DD0.IP QUIT :Ping timeout: 380 seconds[...]:[user][75530]|F!~user755@55C2DEA5.B1212B9.1E6EEEBF.IP JOIN :#paradox[...]:[VN]Administrator|93217!~VNAdmini@D849FDC2.A4BDDB7.A15E2393.IP JOIN :#paradox[...]:wee.wee.wee 255 [NEW][ES]p3pp3r|7239 :I have 898 clients and 0 servers[...]:[VN]Administrator|47610!~VNAdmini@D849FDC2.A4BDDB7.A15E2393.IP QUIT :Read error[...]:wee.wee.wee 003 [NEW][ES]p3pp3r|7239 :This server was created Sat Nov 25 2017 at 20:45:03 GMT[...]:wee.wee.wee 396 [NEW][ES]p3pp3r|7239 4B1B08F9.34FBA1A.5F843480.IP :is now your displayed host[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[PH]PC|88055 [User][1985]|F [ID]Pencegahan|39427 [HK]Administrator|10146 [PK]saaad|69284 [TH]TON|80203 [IN]ict|20122 [VN]Admin|28266 [ID]KikiJaya|3281 [US]Charles|65613 [ID]USER|52354

[PK]Muhammd|91040 [ID[...]:[IN]Lenovo|311!~INLenovo@482BEF13.73B13C3F.60D93FB2.IP QUIT :Read
error[...]:[NP]user|11880!~NPuser1@447F9FD7.4546FDE.36082E.IP JOIN
:#paradox[...]:[PK]AA|19375!~PKAA193@C24B1F32.856638C9.CEE73FBF.IP QUIT :Read
error[...]:[RO]Roby|52415!~RORoby5@he-86086178.residential.rdsnet.ro JOIN :#paradox[...]:wee.wee.wee 005
[NEW][ES]p3pp3r|7239 UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60 MAXNICKLEN=30
NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 :are supported by this server[...]:wee.wee.wee 353
[NEW][ES]p3pp3r|7239 = #paradox :[VN]MICRO|92153 [PH]pc|34040 [PK]iop|9808 [IN]zbe|25 [ID]WIN [ID]ARDYAN-IAN|90185
[IN]User|15549 [MY]apek|94671 [IN]pc-10|40813 [NEA][78970]|F [NP]Lawer|98489 [MY]Pre [IN]DEN [VN]TOSHIBA|88864
[IN]Admin|72[...]:[BEG][14655]|F!~BEG1465@4765A31D.22A79767.C1CCDF8.IP QUIT :Ping timeout: 380
seconds[...]:wee.wee.wee 266 [NEW][ES]p3pp3r|7239 898 1143 :Current global users 898, max
1143[...]:[VN]Administrator|93217!~VNAdmini@D849FDC2.A4BDDB7.A15E2393.IP QUIT :Read error[...]:wee.wee.wee 265
[NEW][ES]p3pp3r|7239 898 1564 :Current local users 898, max
1564[...]:[IN]Lenovo|311!~INLenovo@482BEF13.73B13C3F.60D93FB2.IP JOIN :#paradox[...]:wee.wee.wee 353
[NEW][ES]p3pp3r|7239 = #paradox :[PH]User|23754 [IN]co|9618 [PH]01|31065 [uesr][75718]|F [PK]Zeeshan|67377
[IN]Administrator|91968 [Ab-Basit][36102]|F [CL]casa|92428 [IN]Admin1|68728 [ID]Erlin-PC|5808 [AR]Personal|85426
[ID]USER|54416 [IN[...]:[IN]admin|80589!~INadmin@83D302A4.C1150588.767444AE.IP JOIN
:#paradox[...]:[sony][472]|F!~sony472@3059D2FB.2F4A76FF.9E448AF7.IP QUIT :Ping timeout: 380
seconds[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[ID]iqbal|19661 [BD]User|75040 [IN]Happy|94391
[NEW][VN]cpu|16246 [PE]Especial [DELL][14936]|F [MX]AMD [MX]PC|53178 [MX]netflix|50905 [EE]User|68397
[ID]user|92394 [DESIGNER][37286]|F [ID]airpaoh|12491 [IN[...]:wee.wee.wee NOTICE * :*** Couldn't resolve your
hostname; using your IP address instead[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[ID]User|48519
[ID]SALAM|40680 [ABC][73002]|F [US]Rahim [Dung][69676]|F [NEW][EG]Kasper|64130 [MX]EQUIPO|92947 [PH]pc-01|82440
[NEW][VN]Administrator|95369 [NEW][CN]Administrator|16610 [NEW][VN]Administrat[...]:wee.wee.wee 353
[NEW][ES]p3pp3r|7239 = #paradox :[ID]User|43381 [user][90045]|F [IN]SABARI|74855 [pc][27088]|F [IN]Acer|62911
[PH]lot [MY]Asus|45099 [VN]tuan|98023 [PH]Lala|78223 [IN]vijay1|32124 [PK]star|68066 [MY]user|74568
[Administrator][26365]|F [PK[...]:wee.wee.wee NOTICE * :*** Looking up your hostname...[...]:wee.wee.wee 001
[NEW][ES]p3pp3r|7239 :Welcome to the he IRC Network
[NEW][ES]p3pp3r|7239!~NEWESp@195.206.107.118[...]:[VN]User|46294!~VNUser4@2568ECD6.2CC4E9D8.EB20AEB8.IP QUIT :Ping
timeout: 380 seconds[...]:wee.wee.wee 005 [NEW][ES]p3pp3r|7239 MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A
SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=beI,kLf,l,psmntirzMQNRTOVKDdGPZSCc NETWORK=he
CASEMAPPING=ascii EXTBAN=~,SOcaRrnqj ELIST=MNUCT :are
supported[...]:[ID]KARINA|65812!~IDKARINA@F7505680.FD1D344D.85392EBA.IP QUIT :Read error[...]:wee.wee.wee 353
[NEW][ES]p3pp3r|7239 = #paradox :[PE]Mary|53777 [Thinkpad][92860]|F [VN]User|76600 [VN]DELL|71533 [ID]anroid|76131
[TH]SasithronT|443 [ID]zicko|18937 [VN]Kien [DZ]OMAR [PH]JENEW|62513 [VN]Printer|39314 [BR]Asus|81683 [CO]plan
[rahmanet][3[...]:wee.wee.wee 252 [NEW][ES]p3pp3r|7239 1 :operator(s) online[...]PING :DA629672[...]:wee.wee.wee
353 [NEW][ES]p3pp3r|7239 = #paradox :[TH]user|17003 [NP]Pharmacy|51317 [Flytechno][92925]|F [AC][60647]|F
[PH]computer|68833 [ID]Indra|15360 [IN]TCE|26726 [Admin][22317]|F [ID]acer|62995 [User][8726]|F [PH]NSO|31167
[ID]SPKT|96191 [ID]ACER|79[...]:[IN]admin|5748!~INadmin@C0625AF.1DB66F7.767444AE.IP QUIT :Ping timeout: 380
seconds[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[IN]smart|49315 [kasdas][58501]|F [VE]Lisbeth
[PK]hp|57042 [NEW][TH]hp|93817 [DCMS][86590]|F [VN]User|46294 [ID]asus|26359 [LB]Fater|34626 [NEW][IN]Ranjit|84312
[NEW][IN]Dell|43537 [mac][66106]|F [PK]MUHAM[...]:[VN]HP|71625!~VNHP716@D216BD57.1320D124.7A266DD1.IP JOIN
:#paradox[...]:[PL]Toshiba|68173!~PLToshib@he-6B8872DA.dynamic.mm.pl QUIT :Ping timeout: 380
seconds[...]:[VN]Administrator|86302!~VNAdmini@D849FDC2.A4BDDB7.A15E2393.IP QUIT :Read
error[...]:[sts][95131]|F!~sts9513@F20FDC18.A4901128.3396A5B4.IP QUIT :Read
error[...]:[PH]Pricomshop|94844!~PHPricom@9F15F628.92B72679.7FF3B2A3.IP QUIT :Ping timeout: 380
seconds[...]:[ID]COMPAQ|23479!~IDCOMPAQ@62281B5F.59D9467F.3F6B29CC.IP JOIN
:#paradox[...]:[NP]Admin|7475!~NPAdmin@9A0E12F5.9A4482A.598F1440.IP JOIN
:#paradox[...]:[MY]FooYuanMobile|82064!~MYFooYua@E9B8BB14.2A683964.573DC41E.IP QUIT :Ping timeout: 380
seconds[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[VN]tnc|43823 [RO]sami|23853 [PH]admin|92005
[ID]User|22364 [NEW][IN]sairam|90052 [MY]USER|10105 [IN]Hanumant|95505 [ENDRO][42612]|F [HR]ANTON|10059
[IN]acer|68512 [AR]master|21553 [LK]UESR|17493 [ID]user|[...]:[TR]user|95236!~TRuser9@E1E95544.684A79FC.A4054358.IP
JOIN :#paradox[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[NEW][TH]Microsoft|39628 [MY]cHuCk|16539
[ID]KARINA|65812 [AL]radio|45280 [ID]maitri|45951 [ID]PRP-GROUP02|74897 [VN]huy|66985 [CO]yorladys|73076
[DZ]amine|82587 [TWY-6][50488]|F [NEW][KR]hyochoul|56628
[I[...]:[IN]Asus|32290!~INAsus3@66585872.EE21CAFB.D31AFF89.IP JOIN :#paradox[...]:wee.wee.wee 353
[NEW][ES]p3pp3r|7239 = #paradox :[BD]Faruk|44362 [ID]7|2645 [HN]Oscar|87456 [User][89310]|F [MY]User|67327
[KE]Gidii|47713 [SD]safeena|58119 [user][78503]|F [SA]Bilal|40977 [user][32516]|F [TNNHNCDT][94253]|F

[IN]ACCOUNT|70629 [ID]User|39[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[ID]ARI|5665 [TH]Cyclip|36583 [CO]usuario|20733 [MY]user|55576 [LA]Binhtailor|95006 [K1][9766]|F [NEW][VN]vu [MY]FooYuanMobile|82064 [Usuario][5353]|F [MY]khairil|81612 [ID]HP|80754 [NG]HP|62225 [PH]kitkat[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[US]Matt|85010 [PH]Admin|27522 [GR]paok|94928 [BG]kubineca|89706 [ES]florin|86761 [NEW][KR]pc|57825 [MX]Alexpc|76316 [BR]BRASIL|20203 [VE]Mr [PR]CARLOS|55329 [KW]Pc|11682 [mario][6167]|F [PE]Usuario|33844 [...]:[NEW][ES]p3pp3r|7239 MODE [NEW][ES]p3pp3r|7239
:+iwx[...]:[VE]Niusyalis!~VENiusya@he-5E657354.dyn.dsl.cantv.net QUIT :Read error[...]:[AM]Raffy|81535!~AMRaffy@A530CDF3.A8350FEC.1CBABF4D.IP JOIN :#paradox[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[DE]Tommy|84485 [IL]Security1|63106 [VN]tuoins|95875 [SA]hp|90379 KiloAlpha[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[User][26283]|F [ID]USER|29269 [MX]user|60476 [GR]alexis|61847 [ID]user|99516 [ok][58263]|F [CI]GATEWAY|10985 [IN]Shiva [TR]win7|65957 [ID]PG [pc][43326]|F [RobertFabian][10584]|F [PK]DFAUA|33379 [PH]ertac[...]:[IN]Lenovo|2829!~INLenovo@482BEF13.73B13C3F.60D93FB2.IP JOIN :#paradox[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[NEW][ES]p3pp3r|7239 [ID]user|27819 [IN]orin|48923 [PH]PC1|83593 [NP]ABC|76177 [IN]admin|61726 [IN]Dell|52495 [BEG][58218]|F [VN]Administrator|86302 [IN]expert|34040 [IN]nitish|31580 [ID]Khafiardika|38362 [...]:[KE]Comp!~KEComp@F5EC0BB2.EA4CC72F.607F0F36.IP JOIN :#paradox[...]:[NEW][ES]p3pp3r|7239!~NEWESp@4B1B08F9.34FBA1A.5F843480.IP JOIN :#paradox[...]:[BD]Razzak|49911!~BDRazzak@1F2765CF.C7FA71FA.C53D97E.IP JOIN :#paradox[...]:[VN]Administrator|47610!~VNAdmini@D849FDC2.A4BDDB7.A15E2393.IP JOIN :#paradox[...]:wee.wee.wee 004 [NEW][ES]p3pp3r|7239 wee.wee.wee UnrealIRCd-4.0.1 iowrsxzdHtIRqpWGTSB lvhopsmntikraqbeIzMQNRTOVKDdGLPZSCcf[...]:[Future][3780]|F!~Future3@6B30BC3C.5471F8A0.FCE7E17F.IP JOIN :#paradox[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[kalibata][83433]|F [SYSTEM1][35129]|F [PE]cabina2|97020 [ID]Perpustakaan-WWF|19688 [CA]scott|63893 [Admin][92545]|F [PE]usuario|7551 [RO]claudia|24831 [ID]ABAH [MERRY][32704]|F [VN]Administrator|92141 [CN[...]:wee.wee.wee 251 [NEW][ES]p3pp3r|7239 :There are 1 users and 897 invisible on 1 servers[...]:wee.wee.wee NOTICE * :*** Looking up your hostname...[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[ID]ASUS|25871 [ID]USER|30297 [ID]FARL|92400 [ID]User|79912 [MY]user|39521 [AR]Leon|60290 [ID]ASUS|99612 [MY]tplww|789 [PH]kris|40668 [VN]GiaKhiem|95765 [LV]OsiX|61727 [VN]THC|24831 [PH]hqma_nks|21714 [ADM[...]:[ID]Hp|93901!~IDHp939@F324C68F.136EE767.4170A6DF.IP JOIN :#paradox[...]:wee.wee.wee 005 [NEW][ES]p3pp3r|7239 STATUSMSG=~&@%+ EXCEPTS INVEX CMDS=USERIP,STARTTLS,KNOCK,DCCALLOW,MAP :are supported by this server[...]:[IN]Lenovo|2829!~INLenovo@482BEF13.73B13C3F.60D93FB2.IP QUIT :Read error[...]:[PE]fer|29318!~PEfer29@B84D965E.2955139B.E6374A1F.IP JOIN :#paradox[...]:KiloAlpha!KiloAlpha@admin PRIVMSG #paradox :HTTP https://da.tomatoes.host:2222/ GET 3 2100 HTTP[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[BE]costelila|72418 [CR]Usuario|12943 [BG]OperatorClient|44019 [RO]toshiba|99393 [Minh [MX]alex|10284 [IN]Administrator|96349 [VN]USER|2972 [ZA]Smart|27584 [AR]Carrizo|74868 [SA]Administrator|6486 [Acer][4[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[IN]computer|35916 [PH]mismack|91370 [PH]kunat1|29269 [MX]Andrew|65321 [USER][49216]|F [VN]PC|55329 [DI][47660]|F [BR]Adm|51673 [IN]M|63815 [VN]Mr [VN]admin|14408 [PY]jcandia|84425 [US]Luke [ID]TOKO [IN]3D[...]:[IN]DILAWAR!~INDILAWA@24140E2B.7AFEDDF4.937E86F1.IP JOIN :#paradox[...]:[VN]User|71376!~VNUser7@2568ECD6.2CC4E9D8.EB20AEB8.IP JOIN :#paradox[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[HU]Win7|76378 [IN]HK [AR]MiNueva|21982 [Hazarika][72693]|F [IN]RBL [PH]pc|92116 [Server][41412]|F [long][8360]|F [ID]acer|29636 [SG]user|78674 [IN]Home|85486 [IT]UTENTE|37623 [ID]ASUS|23337 [EC]user|6286 [...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[ID]ATRX|23711 [rina][14636]|F [ID]budi [MX]ES11156|15046 [VN]Precision [ID]admin|5313 [GTE][76714]|F [ID]Suk [NEW][TW]USER|31814 [PC09][78480]|F [PH]Syland|85266 [ID]user|48490 [BH]VIP-DARKO|21237 [ID]SA|[...]:wee.wee.wee 353 [NEW][ES]p3pp3r|7239 = #paradox :[NEW][VN]Administrator|76350 [NL]Sewbalak|94132 [VN]bill|95258 [IN]EMAD|79556 [PH]WS5|4616 [PL]AJHmedia|22732 [TH]HP|87592 [VN]Administrator|4689 [PK]ARB|53025 [PL]Toshiba|68173 [IN]Shree [ID]ACER|10914 [P

Full strings list

The following list it's a collection of all the strings found in the sample's modules (unpacked modules too) code or data.

- <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
- !This program cannot be run in DOS mode.
- <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/;q=0.8
- Accept-Encoding: gzip, deflate, br
- AssemblyBuilder
- set_Position
- System.IO.Compression
- GetCustomAttributes
- get_FieldHandle
- get_CurrentDomain
- System.Resources
- GetHostAddresses
- GetUnderlyingType
- System.Runtime.Serialization
- get_OriginalString
- IsAssignableFrom
- get_IsInterface
- StringFileInfo
- KeyValuePair`2
- System.CodeDom.Compiler
- IsInstanceOfType
- getElementsByTagName
- get_Assembly
- MakeByRefType
- DeflateStream
- GetConstructors
- AssemblyNameFlags
- get_IsValueType
- <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
- GetParameters
- LocalCertificateSelectionCallback
- add_AssemblyResolve
- AllocHGlobal
- set_ContentType
- Assembly Version
- set_ScriptErrorsSuppressed
- LocalBuilder
- get_ParameterType
- set_ContentLength
- VS_VERSION_INFO
- get_ReturnType
- GetDynamicILInfo
- get_TypeHandle
- OriginalFilename
- DeclareLocal
- AppendFormat
- CompressionMode

- get_ReadyState
- MakeGenericType
- get_ElapsedMilliseconds
- get_IsPointer
- DynamicILInfo
- </trustInfo>
- </requestedPrivileges>
- LocalMachine
- ResolveSignature
- ModuleBuilder
- HttpResponseHeader
- get_BaseType
- ParameterInfo
- GetValueOrDefault
- AssemblyName
- DebuggingModes
- oiTDMIW}^ln"o\\,pEA\\\\-\\,i5%6%.resources
- GetTargetType
- DefineDynamicAssembly
- GetManifestResourceStream
- GetAssemblies
- get_IsConstructor
- get_DeclaringType
- get_MethodHandle
- get_IsPrimitive
- SetLocalSignature
- GetRequestStream
- BindingFlags
- AssemblyBuilderAccess
- InvokeMember
- get_FieldType
- PropertyInfo
- <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
- get_CultureInfo
- ResourceManager
- get_IsVirtual
- GetOptionalCustomModifiers
- LegalCopyright
- get_Document
- CustomAttributeBuilder
- ResolveEventArgs
- get_MetadataToken
- GetFunctionPointer
- ResolveEventHandler
- get_HasValue
- FormatterServices
- get_IsStatic
- InternalName
- get_InnerException
- IsLittleEndian
- +j|Zf 'Tc!a}
- GetElementType
- ERROR_NO_MORE_ITEMS
- get_LocalPath
- RuntimeHelpers
- get_MainWindowTitle
- set_Arguments

- set_UserAgent
- SuspendThread
- AddressFamily
- get_OperationalStatus
- KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingleFileGenerator
- System.Net.Security
- PAGE_EXECUTE
- System.Windows.Forms
- System.Drawing
- System.Security.Cryptography.X509Certificates
- get_Position
- get_IsAbstract
- HttpWebResponse
- GCHandleType
- PAGE_READONLY
- PAGE_NOCACHE
- set_ServerCertificateValidationCallback
- set_ProtocolVersion
- IPGlobalProperties
- {0} /{1} HTTP/1.1
- G(G8GHGXGcGvG
- ExpandEnvironmentVariables
- GetIPGlobalProperties
- get_CurrentThread
- DWebBrowserEvents2_BeforeNavigate2EventHandler
- GetExecutingAssembly
- GetResponseStream
- L!L-L<LHLTLiL
- ApplicationSettingsBase
- get_BaseAddress
- ManagementObjectSearcher
- WebBrowserDocumentCompletedEventHandler
- set_DefaultConnectionLimit
- S@LT&KE4343242343Y;
- GetProcesses
- System.Net.Sockets
- FileIOPermissionAccess
- remove_DocumentCompleted
- SUSPEND_RESUME
- INTERNET_COOKIE_HTTPONLY
- ExecuteWriteCopy
- ReadAllBytes
- gzip, deflate, br
- StringBuilder
- DownloadString
- gzip, deflate, sdch, br
- System.Net.NetworkInformation
- GetAllNetworkInterfaces
- set_CreateNoWindow
- RtlSetProcessIsCritical
- get_CharacterSet
- get_BytesReceived
- NetworkStream
- set_UseShellExecute
- System.Security.Principal
- EnterDebugMode
- get_TickCount

- ResolveMember
- set_IsBackground
- sslPolicyErrors
- NetworkAccess
- HttpStatusCode
- OperationalStatus
- get_Location
- System.Security.Permissions.SecurityPermissionAttribute, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
- PasswordHash
- get_BytesSent
- IsWow64Process
- HttpWebRequest
- ReadAllLines
- WriteCombineModifierflag
- System.Runtime.CompilerServices
- MemoryStream
- CryptoStreamMode
- SpecialFolder
- WebBrowserBase
- GetProcessesByName
- NB2.Properties
- StreamWriter
- System.Runtime.InteropServices
- get_StatusCode
- NoCacheModifierflag
- get_LocalEndPoint
- get_ProcessName
- set_Expect100Continue
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- H&H.H6H;:HGHMHVHdHmH
- BinaryReader
- CryptoStream
- User-Agent: {0}
- get_PrimaryScreen
- WrapNonExceptionThrows
- SymmetricAlgorithm
- get_Connected
- _remoteStackTraceString
- IAsyncResult
- ScriptEngine
- get_FileName
- PAGE_WRITECOMBINE
- GetFolderPath
- get_FullyQualifiedName
- PAGE_EXECUTE_READWRITE
- set_FileName
- SettingsBase
- ConstructorInfo
- Upgrade-Insecure-Requests: 1
- get_ExecutablePath
- set_KeepAlive
- get_ThreadState
- AceQualifier
- PAGE_READWRITE
- get_UserName
- get_MainModule

- get_ActiveXInstance
- ZwSetInformationProcess
- get_RemoteEndPoint
- System.Runtime.ExceptionServices.ExceptionDispatchInfo
- get_NetworkInterfaceType
- SecurityIdentifier
- GetCurrentProcess
- INTERNET_COOKIE_THIRD_PARTY
- SET_THREAD_TOKEN
- INTERNET_FLAG_RESTRICTED_ZONE
- FromBase64String
- CookieContainer
- System.Threading
- GetValueNames
- lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- Connection: Keep-Alive
- ServicePointManager
- GetResourceString
- Cache-Control: no-cache
- get_ServerCertificateValidationCallback
- WebBrowserDocumentCompletedEventArgs
- get_IsAttached
- ProtocolType
- WellKnownSidType
- PAGE_NOACCESS
- set_UseNagleAlgorithm
- get_ModuleMemorySize
- StreamReader
- NetworkInterfaceType
- CreateRemoteThread
- System.Reflection.Emit
- RoaZ .PQua8g
- get_DiscretionaryAcl
- Rfc2898DeriveBytes
- GuardModifierflag
- Accept-Encoding
- ProcessStartInfo
- PAGE_WRITECOPY
- $88b6efb0-83b0-4cbd-a2d9-3a37200bd51b
- get_ProcessorCount
- GetEntryAssembly
- ProcessThread
- ReadOnlyCollectionBase
- ERROR_INSUFFICIENT_BUFFER
- PAGE_EXECUTE_READ
- BitConverter
- GetCommandLineArgs
- get_IsAbsoluteUri
- RemoteCertificateValidationCallback
- ERROR_INVALID_PARAMETER
- get_BinaryLength
- 3System.Resources.Tools.StronglyTypedResourceBuilder
- AsyncCallback
- SET_INFORMATION
- set_WindowStyle
- PAGE_EXECUTE_WRITECOPY

- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- ReadProcessMemory
- VirtualProtectEx
- IsDebuggerPresent
- CheckRemoteDebuggerPresent
- VirtualAllocEx
- WriteProcessMemory
- InternetGetCookieExW
- HtmlDocument
- MatchCollection
- DebuggerBrowsableState
- AssemblyFileVersionAttribute
- GeneratedCodeAttribute
- GuidAttribute
- DebuggableAttribute
- SecurityCriticalAttribute
- FileDescription
- GetBaseDefinition
- costura.jurassic.dll.compressed
- FlagsAttribute
- AssemblyCompanyAttribute
- CompilerGeneratedAttribute
- HtmlElementCollection
- GetILGenerator
- GetGetMethod
- System.Collections.Generic
- WebBrowserReadyState
- AssemblyDescriptionAttribute
- ExecutionEngineException
- ParamArrayAttribute
- ResolveMethod
- AssemblyProductAttribute
- GetFieldFromHandle
- TargetInvocationException
- ThreadStaticAttribute
- RuntimeCompatibilityAttribute
- CreateDelegate
- EditorBrowsableAttribute
- StackOverflowException
- InternalsVisibleToAttribute
- AssemblyCopyrightAttribute
- LegalTrademarks
- Synchronized
- InitializeArray
- UserScopedSettingAttribute
- InvalidProgramException
- TypedReference
- AssemblyTitleAttribute
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- GetUninitializedObject
- SecurityPermi
- DebuggerBrowsableAttribute
- AuthenticateAsClient
- DebuggerNonUserCodeAttribute
- AssemblyConfigurationAttribute

- EditorBrowsableState
- ArithmeticException
- ProductVersion
- IEnumerator`1
- PointToScreen
- NotSupportedException
- ExtensionAttribute
- UnverifiableCodeAttribute
- NullReferenceException
- ManagementObject
- STAThreadAttribute
- ComVisibleAttribute
- System.Globalization
- ToLowerInvariant
- InvalidCastException
- CompilationRelaxationsAttribute
- StringComparison
- AssemblyTrademarkAttribute
- SetValueDirect
- DefaultSettingValueAttribute
- OverflowException
- costura.interop.shdocvw.dll.compressed
- DefineDynamicModule
- SetKernelObjectSecurity
- GetPhysicallyInstalledSystemMemory
- GetKernelObjectSecurity
- VirtualQueryEx
- NtUnmapViewOfSection
- Cache-control
- TcpConnectionInformation
- System.Security.AccessControl
- GetFileNameWithoutExtension
- Dictionary`2
- ManagementObjectEnumerator
- System.Diagnostics
- DWebBrowserEvents2_Event
- GetIsNetworkAvailable
- @1B2c3D4e5F6g7H8
- oiTDMIW}^ln"o,pEA\\-,i5%6%
- ManagementObjectCollection
- System.ComponentModel
- System.Collections
- System.Security.Permissions
- 2:O;O<G=O>W?G@
- GetActiveTcpConnections
- SystemException
- IEnumerable`1
- CodeAccessPermission
- QUERY_INFORMATION
- IPv4InterfaceStatistics
- RuntimeMethodHandle
- ParameterizedThreadStart
- ProcessThreadCollection
- System.Management
- ProcessWindowStyle
- DownloadFile
- GetMethodDescriptor

- WindowsIdentity
- MulticastDelegate
- ConfuserEx v1.0.0
- GroupCollection
- WebPermission
- application/x-www-form-urlencoded
- CreateSubKey
- GetIPv4Statistics
- NameValueCollection
- X509Certificate
- kernel32.dll
- CreateDecryptor
- DynamicMethod
- WriteAllText
- ApartmentState
- DIRECT_IMPERSONATION
- SkipVerification
- System.Configuration
- GetBinaryForm
- GetEnumerator
- GetTypeFromHandle
- SetApartmentState
- RijndaelManaged
- Microsoft.Win32
- System.Collections.Specialized
- System.Security.Cryptography
- ProcessModule
- NetworkInterface
- op_Inequality
- ICryptoTransform
- P@@Sw0rd54690fj48743843789eey3
- Interop.SHDocVw
- GenericSecurityDescriptor
- add_BeforeNavigate2
- GetConstructor
- GetLastWin32Error
- GetHINSTANCE
- WebHeaderCollection
- ExecuteReadWrite
- PlatformNotSupportedException
- Win32Exception
- DeleteSubKey
- SecurityAction
- advapi32.dll
- System.Text.RegularExpressions
- System.Security
- RuntimeFieldHandle
- IsNullOrEmpty
- H6jZ dDfba8`
- SecurityPermissionAttribute
- ArgumentNullException
- RuntimeTypeHandle
- System.Reflection
- FileIOPermission
- ManagementBaseObject
- GetObjectValue
- GetGlobalValue

- UriComponents
- GetComponents
- ConfusedByAttribute
- RawSecurityDescriptor
- InternalPreserveStackTrace
- add_DocumentCompleted
- SetCustomAttribute
- @"@3@>@O@V@_@f@l@v@}@
- <!<9<B<G<U<z<

Threads behaviour

In this section it's possible to find information about sample's threads, such as the actions performed by each sample's thread ordered chronologically.

- **Thread T0 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T1 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T1)
- **Thread T1 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T2 (in process P0, p3pp3rsamp.exe)
    - Thread T3 (in process P0, p3pp3rsamp.exe)
    - Thread T4 (in process P0, p3pp3rsamp.exe)
    - Thread T5 (in process P0, p3pp3rsamp.exe)
    - Thread T6 (in process P1, schtasks.exe)
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)
    - Thread Create (Thread ID: TUNKALIAS)
    - Thread Create (Thread ID: T2)
    - Thread Create (Thread ID: TUNKALIAS)
    - Thread Create (Thread ID: T3)
    - Thread Create (Thread ID: TUNKALIAS)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - Thread Create (Thread ID: TUNKALIAS)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3rsamp.exe Type: REG_DWORD, Length: 4, Data: 8888)
    - RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION Desired Access: Read/Write)
    - RegCreateKey (HKCU\\Software Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKCU\\Software\\Microsoft Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer\\Main Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl Desired Access: Maximum Allowed, Granted Access: None 0x0, Disposition: REG_CREATED_NEW_KEY)
    - RegCreateKey (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION Desired Access: Read/Write, Disposition: REG_CREATED_NEW_KEY)

• RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3rsamp.exe Type: REG_DWORD, Length: 4, Data: 8888)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3rsamp.vshost.exe Type: REG_DWORD, Length: 4, Data: 8888)
• RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3rsamp.vshost.exe Type: REG_DWORD, Length: 4, Data: 8888)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.exe Type: REG_DWORD, Length: 4, Data: 8888)
• RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.exe Type: REG_DWORD, Length: 4, Data: 8888)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.vshost.exe Type: REG_DWORD, Length: 4, Data: 8888)
• RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.vshost.exe Type: REG_DWORD, Length: 4, Data: 8888)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.exe Type: REG_DWORD, Length: 4, Data: 8)
• RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.exe Type: REG_DWORD, Length: 4, Data: 8)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Internet Explorer\\MAIN\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.vshost.exe Type: REG_DWORD, Length: 4, Data: 8)
• RegSetValue (HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl\\FEATURE_BROWSER_EMULATION\\p3pp3r.vshost.exe Type: REG_DWORD, Length: 4, Data: 8)
• RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32 Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
• RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)

- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
- Thread Create (Thread ID: TUNKALIAS)
- Thread Create (Thread ID: T4)
- Thread Create (Thread ID: TUNKALIAS)
- Thread Create (Thread ID: T5)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\syscheck Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- Thread Create (Thread ID: TUNKALIAS)
- Process Create (C:\\Windows\\system32\\schtasks.exe PID: P1, Command line: "schtasks.exe" /create /sc minute /mo 1 /tn "Decp3pp3r" /tr "C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe")

- **Thread T2 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)
- **Thread T3 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)
- **Thread T4 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)
- **Thread T5 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)

- **Thread T6 (in process P1, schtasks.exe) description**
  - **Thread's childs**
    - Thread T7 (in process P1, schtasks.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T7)
- **Thread T7 (in process P1, schtasks.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)

Network by processes

The analysis environment tries to capture and collect network actions performed by sample's threads.

- No processes with network events found

Unpacked or injected modules

In this section it's possible to find information about sample's modules, such as the rich signatures and strings

- **Module 1 (probably unpacked / injected by the sample)**
  - **Module 1 rich signatures**
    - No rich signatures found
  - **Module 1 strings**
    - **Module 1 most interesting strings**
      - <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
      - !This program cannot be run in DOS mode.
      - <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
      - <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
      - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
      - AssemblyBuilder
      - set_Position
      - System.IO.Compression
      - GetCustomAttributes
      - get_FieldHandle
      - get_CurrentDomain
      - System.Resources
      - GetHostAddresses
      - GetUnderlyingType
      - System.Runtime.Serialization
      - get_OriginalString
      - IsAssignableFrom
      - get_IsInterface
      - StringFileInfo
      - KeyValuePair`2
      - System.CodeDom.Compiler
      - IsInstanceOfType
      - getElementsByTagName
      - get_Assembly
      - MakeByRefType
      - DeflateStream
      - GetConstructors
      - AssemblyNameFlags
      - get_IsValueType
      - <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
      - GetParameters
      - LocalCertificateSelectionCallback
      - add_AssemblyResolve
      - AllocHGlobal
      - set_ContentType
      - Assembly Version
      - set_ScriptErrorsSuppressed
      - LocalBuilder
      - get_ParameterType
      - set_ContentLength
      - VS_VERSION_INFO

- get_ReturnType
- GetDynamicILInfo
- get_TypeHandle
- OriginalFilename
- DeclareLocal
- AppendFormat
- CompressionMode
- get_ReadyState
- MakeGenericType
- get_ElapsedMilliseconds
- get_IsPointer
- DynamicILInfo
- </trustInfo>
- </requestedPrivileges>
- LocalMachine
- ResolveSignature
- ModuleBuilder
- HttpResponseHeader
- get_BaseType
- ParameterInfo
- GetValueOrDefault
- AssemblyName
- DebuggingModes
- oiTDMIW}^ln"o\\,pEA\\\\-\\,i5%6%.resources
- GetTargetType
- DefineDynamicAssembly
- GetManifestResourceStream
- GetAssemblies
- get_IsConstructor
- get_DeclaringType
- get_MethodHandle
- get_IsPrimitive
- SetLocalSignature
- GetRequestStream
- BindingFlags
- AssemblyBuilderAccess
- InvokeMember
- get_FieldType
- PropertyInfo
- <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
- get_CultureInfo
- ResourceManager
- get_IsVirtual
- GetOptionalCustomModifiers
- LegalCopyright
- get_Document
- CustomAttributeBuilder
- ResolveEventArgs
- get_MetadataToken
- GetFunctionPointer
- ResolveEventHandler
- get_HasValue
- FormatterServices
- get_IsStatic
- InternalName
- get_InnerException
- IsLittleEndian

- +j|Zf 'Tc!a}
- GetElementType

- **Module 1 other strings**

- HtmlDocument
- MatchCollection
- DebuggerBrowsableState
- AssemblyFileVersionAttribute
- GeneratedCodeAttribute
- GuidAttribute
- DebuggableAttribute
- SecurityCriticalAttribute
- FileDescription
- GetBaseDefinition
- costura.jurassic.dll.compressed
- FlagsAttribute
- AssemblyCompanyAttribute
- CompilerGeneratedAttribute
- HtmlElementCollection
- GetILGenerator
- GetGetMethod
- System.Collections.Generic
- WebBrowserReadyState
- AssemblyDescriptionAttribute
- ExecutionEngineException
- ParamArrayAttribute
- ResolveMethod
- AssemblyProductAttribute
- GetFieldFromHandle
- TargetInvocationException
- ThreadStaticAttribute
- RuntimeCompatibilityAttribute
- CreateDelegate
- EditorBrowsableAttribute
- StackOverflowException
- InternalsVisibleToAttribute
- AssemblyCopyrightAttribute
- LegalTrademarks
- Synchronized
- InitializeArray
- UserScopedSettingAttribute
- InvalidProgramException
- TypedReference
- AssemblyTitleAttribute
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- GetUninitializedObject
- SecurityPermi
- DebuggerBrowsableAttribute
- AuthenticateAsClient
- DebuggerNonUserCodeAttribute
- AssemblyConfigurationAttribute
- EditorBrowsableState
- ArithmeticException

- ProductVersion
- IEnumerator`1
- PointToScreen
- NotSupportedException
- ExtensionAttribute
- UnverifiableCodeAttribute
- NullReferenceException
- ManagementObject
- STAThreadAttribute
- ComVisibleAttribute
- System.Globalization
- ToLowerInvariant
- InvalidCastException
- CompilationRelaxationsAttribute
- StringComparison
- AssemblyTrademarkAttribute
- SetValueDirect
- DefaultSettingValueAttribute
- OverflowException
- costura.interop.shdocvw.dll.compressed
- DefineDynamicModule
- No strings found

Module 2 (probably unpacked / injected by the sample)

Module 2 rich signatures

- No rich signatures found

Module 2 strings

Module 2 most interesting strings

- <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
- !This program cannot be run in DOS mode.
- <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
- AssemblyBuilder
- set_Position
- System.IO.Compression
- GetCustomAttributes
- get_FieldHandle
- get_CurrentDomain
- System.Resources
- GetHostAddresses
- GetUnderlyingType
- System.Runtime.Serialization
- get_OriginalString
- IsAssignableFrom
- get_IsInterface
- StringFileInfo
- KeyValuePair`2
- System.CodeDom.Compiler
- IsInstanceOfType

- getElementsByTagName
- get_Assembly
- MakeByRefType
- DeflateStream
- GetConstructors
- AssemblyNameFlags
- get_IsValueType
- <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
- GetParameters
- LocalCertificateSelectionCallback
- add_AssemblyResolve
- AllocHGlobal
- set_ContentType
- Assembly Version
- set_ScriptErrorsSuppressed
- LocalBuilder
- get_ParameterType
- set_ContentLength
- VS_VERSION_INFO
- get_ReturnType
- GetDynamicILInfo
- get_TypeHandle
- OriginalFilename
- DeclareLocal
- AppendFormat
- CompressionMode
- get_ReadyState
- MakeGenericType
- get_ElapsedMilliseconds
- get_IsPointer
- DynamicILInfo
- </trustInfo>
- </requestedPrivileges>
- LocalMachine
- ResolveSignature
- ModuleBuilder
- HttpResponseHeader
- get_BaseType
- ParameterInfo
- GetValueOrDefault
- AssemblyName
- DebuggingModes
- oiTDMIW}^ln"o\\,pEA\\\\-\\,i5%6%.resources
- GetTargetType
- DefineDynamicAssembly
- GetManifestResourceStream
- GetAssemblies
- get_IsConstructor
- get_DeclaringType
- get_MethodHandle
- get_IsPrimitive
- SetLocalSignature
- GetRequestStream
- BindingFlags
- AssemblyBuilderAccess
- InvokeMember
- get_FieldType

- PropertyInfo
- <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
- get_CultureInfo
- ResourceManager
- get_IsVirtual
- GetOptionalCustomModifiers
- LegalCopyright
- get_Document
- CustomAttributeBuilder
- ResolveEventArgs
- get_MetadataToken
- GetFunctionPointer
- ResolveEventHandler
- get_HasValue
- FormatterServices
- get_IsStatic
- InternalName
- get_InnerException
- IsLittleEndian
- +j|Zf 'Tc!a}
- GetElementType

- **Module 2 other strings**

- HtmlDocument
- MatchCollection
- DebuggerBrowsableState
- AssemblyFileVersionAttribute
- GeneratedCodeAttribute
- GuidAttribute
- DebuggableAttribute
- SecurityCriticalAttribute
- FileDescription
- GetBaseDefinition
- costura.jurassic.dll.compressed
- FlagsAttribute
- AssemblyCompanyAttribute
- CompilerGeneratedAttribute
- HtmlElementCollection
- GetILGenerator
- GetGetMethod
- System.Collections.Generic
- WebBrowserReadyState
- AssemblyDescriptionAttribute
- ExecutionEngineException
- ParamArrayAttribute
- ResolveMethod
- AssemblyProductAttribute
- GetFieldFromHandle
- TargetInvocationException
- ThreadStaticAttribute
- RuntimeCompatibilityAttribute
- CreateDelegate
- EditorBrowsableAttribute
- StackOverflowException
- InternalsVisibleToAttribute

- AssemblyCopyrightAttribute
- LegalTrademarks
- Synchronized
- InitializeArray
- UserScopedSettingAttribute
- InvalidProgramException
- TypedReference
- AssemblyTitleAttribute
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- GetUninitializedObject
- SecurityPermi
- DebuggerBrowsableAttribute
- AuthenticateAsClient
- DebuggerNonUserCodeAttribute
- AssemblyConfigurationAttribute
- EditorBrowsableState
- ArithmeticException
- ProductVersion
- IEnumerator`1
- PointToScreen
- NotSupportedException
- ExtensionAttribute
- UnverifiableCodeAttribute
- NullReferenceException
- ManagementObject
- STAThreadAttribute
- ComVisibleAttribute
- System.Globalization
- ToLowerInvariant
- InvalidCastException
- CompilationRelaxationsAttribute
- StringComparison
- AssemblyTrademarkAttribute
- SetValueDirect
- DefaultSettingValueAttribute
- OverflowException
- costura.interop.shdocvw.dll.compressed
- DefineDynamicModule
- No strings found

Module 3 (probably unpacked / injected by the sample)

Module 3 rich signatures

- No rich signatures found

Module 3 strings

Module 3 most interesting strings

- <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
- !This program cannot be run in DOS mode.

- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
- <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/;q=0.8
- Accept-Encoding: gzip, deflate, br
- ERROR_NO_MORE_ITEMS
- AssemblyBuilder
- get_FieldHandle
- get_LocalPath
- RuntimeHelpers
- CustomAttributeBuilder
- get_MainWindowTitle
- set_Arguments
- set_UserAgent
- SuspendThread
- AddressFamily
- StringFileInfo
- get_OperationalStatus
- KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingleFileGenerator
- System.Net.Security
- PAGE_EXECUTE
- LocalCertificateSelectionCallback
- add_AssemblyResolve
- System.Windows.Forms
- System.Drawing
- System.Security.Cryptography.X509Certificates
- get_Position
- Assembly Version
- get_IsAbstract
- HttpWebResponse
- GCHandleType
- PAGE_READONLY
- PAGE_NOCACHE
- set_ServerCertificateValidationCallback
- set_ProtocolVersion
- LocalMachine
- IPGlobalProperties
- DebuggingModes
- {0} /{1} HTTP/1.1
- G(G8GHGXGcGvG
- ExpandEnvironmentVariables
- AssemblyBuilderAccess
- GetIPGlobalProperties
- get_CurrentThread
- DWebBrowserEvents2_BeforeNavigate2EventHandler
- GetExecutingAssembly
- ResourceManager
- LocalBuilder
- GetResponseStream
- <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
- get_HasValue
- L!L-L<LHLTLiL
- get_IsStatic
- ApplicationSettingsBase
- get_BaseAddress
- ManagementObjectSearcher
- WebBrowserDocumentCompletedEventHandler

- GetElementType
- set_DefaultConnectionLimit
- S@LT&KE4343242343Y;
- get_IsPointer
- GetHostAddresses
- GetCustomAttributes
- GetProcesses
- System.Net.Sockets
- System.Resources
- FileIOPermissionAccess
- remove_DocumentCompleted
- getElementsByTagName
- get_Assembly
- MakeByRefType
- DeflateStream
- SUSPEND_RESUME
- AssemblyNameFlags
- get_IsValueType
- INTERNET_COOKIE_HTTPONLY
- ExecuteWriteCopy
- ReadAllBytes
- gzip, deflate, br
- get_ParameterType
- StringBuilder
- get_ReturnType
- DownloadString
- gzip, deflate, sdch, br
- System.Net.NetworkInformation
- GetAllNetworkInterfaces
- set_CreateNoWindow
- RtlSetProcessIsCritical
- DeclareLocal
- get_FieldType
- get_CharacterSet
- get_ReadyState
- get_BytesReceived
- get_ElapsedMilliseconds
- NetworkStream
- set_UseShellExecute
- ResolveSignature
- System.Security.Principal
- EnterDebugMode
- GetTargetType
- get_TickCount
- ResolveMember
- set_IsBackground
- sslPolicyErrors
- NetworkAccess
- HttpStatusCode
- DefineDynamicAssembly
- OperationalStatus
- get_Location
- GetRequestStream
- <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
- IsLittleEndian
- System.Security.Permissions.SecurityPermissionAttribute, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089

- PasswordHash
- get_BytesSent
- IsWow64Process
- FormatterServices
- get_Document
- HttpWebRequest
- ResolveEventArgs
- ReadAllLines
- WriteCombineModifierflag
- System.Runtime.CompilerServices
- MemoryStream
- CryptoStreamMode
- SpecialFolder
- WebBrowserBase
- GetProcessesByName
- NB2.Properties
- StreamWriter
- System.Runtime.InteropServices
- get_StatusCode
- NoCacheModifierflag
- get_LocalEndPoint
- set_Position
- get_ProcessName
- set_Expect100Continue
- System.Runtime.Serialization
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- H&H.H6H;:HGHMHVHdHmH
- BinaryReader
- CryptoStream
- User-Agent: {0}
- VS_VERSION_INFO
- get_PrimaryScreen
- GetConstructors
- WrapNonExceptionThrows
- SymmetricAlgorithm
- get_Connected
- GetParameters
- _remoteStackTraceString
- IAsyncResult
- ScriptEngine
- PropertyInfo
- get_FileName
- PAGE_WRITECOMBINE
- set_ContentLength
- GetFolderPath
- get_FullyQualifiedName
- get_TypeHandle
- PAGE_EXECUTE_READWRITE
- set_FileName
- SettingsBase
- ConstructorInfo
- Upgrade-Insecure-Requests: 1
- DynamicILInfo
- </trustInfo>
- </requestedPrivileges>
- get_ExecutablePath
- get_BaseType

- set_KeepAlive
- get_ThreadState
- GetValueOrDefault
- MakeGenericType
- AceQualifier
- GetManifestResourceStream
- PAGE_READWRITE
- get_IsConstructor
- get_DeclaringType
- get_UserName
- get_MainModule
- BindingFlags
- get_ActiveXInstance
- AppendFormat
- InvokeMember
- get_IsPrimitive
- ZwSetInformationProcess
- get_CultureInfo
- get_RemoteEndPoint
- System.Runtime.ExceptionServices.ExceptionDispatchInfo
- get_NetworkInterfaceType
- ModuleBuilder
- SecurityIdentifier
- GetCurrentProcess
- INTERNET_COOKIE_THIRD_PARTY
- SET_THREAD_TOKEN
- INTERNET_FLAG_RESTRICTED_ZONE
- FromBase64String
- GetFunctionPointer
- CookieContainer
- System.IO.Compression
- get_MetadataToken
- get_CurrentDomain
- OriginalFilename
- GetUnderlyingType
- get_OriginalString
- System.Threading
- IsAssignableFrom
- GetValueNames
- lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- get_IsInterface
- Connection: Keep-Alive
- System.CodeDom.Compiler
- ServicePointManager
- GetResourceString
- Cache-Control: no-cache
- get_ServerCertificateValidationCallback
- AllocHGlobal
- WebBrowserDocumentCompletedEventArgs
- get_IsAttached
- ProtocolType
- set_ContentType
- WellKnownSidType
- set_ScriptErrorsSuppressed
- PAGE_NOACCESS
- set_UseNagleAlgorithm

- GetDynamicILInfo
- get_ModuleMemorySize
- StreamReader
- NetworkInterfaceType
- CreateRemoteThread
- System.Reflection.Emit
- RoaZ .PQua8g
- get_DiscretionaryAcl
- Rfc2898DeriveBytes
- GuardModifierflag
- Accept-Encoding
- ProcessStartInfo
- PAGE_WRITECOPY
- HttpResponseHeader
- $88b6efb0-83b0-4cbd-a2d9-3a37200bd51b
- get_ProcessorCount
- GetEntryAssembly
- ParameterInfo
- ProcessThread
- AssemblyName
- oiTDMIW}^ln"o\\,pEA\\\\-\\,i5%6%.resources
- SetLocalSignature
- GetAssemblies
- get_MethodHandle
- ReadOnlyCollectionBase
- KeyValuePair`2
- ERROR_INSUFFICIENT_BUFFER
- PAGE_EXECUTE_READ
- BitConverter
- get_InnerException
- get_IsVirtual
- GetCommandLineArgs
- GetOptionalCustomModifiers
- LegalCopyright
- IsInstanceOfType
- get_IsAbsoluteUri
- RemoteCertificateValidationCallback
- ERROR_INVALID_PARAMETER
- get_BinaryLength
- ResolveEventHandler
- 3System.Resources.Tools.StronglyTypedResourceBuilder
- CompressionMode
- AsyncCallback
- InternalName
- SET_INFORMATION
- set_WindowStyle
- PAGE_EXECUTE_WRITECOPY
- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- +j|Zf 'Tc!a}
- ReadProcessMemory
- VirtualProtectEx
- IsDebuggerPresent
- CheckRemoteDebuggerPresent
- VirtualAllocEx
- WriteProcessMemory
- InternetGetCookieExW
- SetKernelObjectSecurity

- GetPhysicallyInstalledSystemMemory
- GetKernelObjectSecurity
- VirtualQueryEx
- NtUnmapViewOfSection

- **Module 3 other strings**

- Cache-control
- GeneratedCodeAttribute
- TcpConnectionInformation
- DebuggableAttribute
- GetBaseDefinition
- costura.jurassic.dll.compressed
- System.Security.AccessControl
- GetFileNameWithoutExtension
- Dictionary`2
- GetGetMethod
- ThreadStaticAttribute
- ManagementObjectEnumerator
- System.Diagnostics
- DWebBrowserEvents2_Event
- GetIsNetworkAvailable
- System.Collections.Generic
- ExecutionEngineException
- @1B2c3D4e5F6g7H8
- oiTDMIW}^ln"o,pEA\\-,i5%6%
- EditorBrowsableAttribute
- ManagementObjectCollection
- AssemblyCopyrightAttribute
- System.ComponentModel
- System.Collections
- InitializeArray
- UserScopedSettingAttribute
- System.Security.Permissions
- TypedReference
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- GetUninitializedObject
- DebuggerNonUserCodeAttribute
- O;O<G=O>W?G@
- GetActiveTcpConnections
- SystemException
- IEnumerable`1
- CodeAccessPermission
- ExtensionAttribute
- System.Globalization
- QUERY_INFORMATION
- STAThreadAttribute
- StackOverflowException
- InvalidCastException
- IPv4InterfaceStatistics
- RuntimeMethodHandle
- FileDescription
- ParameterizedThreadStart
- ProcessThreadCollection

- AssemblyFileVersionAttribute
- System.Management
- ProcessWindowStyle
- DownloadFile
- CompilerGeneratedAttribute
- GetMethodDescriptor
- WindowsIdentity
- MulticastDelegate
- ConfuserEx v1.0.0
- GroupCollection
- WebPermission
- application/x-www-form-urlencoded
- AssemblyProductAttribute
- RuntimeCompatibilityAttribute
- NullReferenceException
- CreateSubKey
- InternalsVisibleToAttribute
- GetIPv4Statistics
- LegalTrademarks
- Synchronized
- NameValueCollection
- X509Certificate
- kernel32.dll
- ArithmeticException
- CreateDecryptor
- DynamicMethod
- PointToScreen
- WriteAllText
- CompilationRelaxationsAttribute
- StringComparison
- ApartmentState
- OverflowException
- costura.interop.shdocvw.dll.compressed
- DIRECT_IMPERSONATION
- SkipVerification
- FlagsAttribute
- HtmlDocument
- System.Configuration
- SecurityCriticalAttribute
- GetBinaryForm
- GetEnumerator
- GetTypeFromHandle
- AssemblyConfigurationAttribute
- SetApartmentState
- RijndaelManaged
- ResolveMethod
- Microsoft.Win32
- CreateDelegate
- System.Collections.Specialized
- System.Security.Cryptography
- ProcessModule
- NetworkInterface
- AssemblyTitleAttribute
- op_Inequality
- ICryptoTransform
- DebuggerBrowsableAttribute
- MatchCollection

- TargetInvocationException
- NotSupportedException
- P@@Sw0rd54690fj48743843789eey3
- ToLowerInvariant
- Interop.SHDocVw
- AssemblyTrademarkAttribute
- SetValueDirect
- DefineDynamicModule
- GenericSecurityDescriptor
- add_BeforeNavigate2
- GetConstructor
- ManagementObject
- ProductVersion
- DebuggerBrowsableState
- GetLastWin32Error
- GetHINSTANCE
- GuidAttribute
- WebHeaderCollection
- ExecuteReadWrite
- AssemblyCompanyAttribute
- PlatformNotSupportedException
- HtmlElementCollection
- Win32Exception
- DeleteSubKey
- SecurityAction
- WebBrowserReadyState
- advapi32.dll
- AssemblyDescriptionAttribute
- ParamArrayAttribute
- GetFieldFromHandle
- System.Text.RegularExpressions
- GetILGenerator
- System.Security
- RuntimeFieldHandle
- IsNullOrEmpty
- H6jZ dDfba8`
- SecurityPermissionAttribute
- InvalidProgramException
- ArgumentNullException
- RuntimeTypeHandle
- AuthenticateAsClient
- System.Reflection
- FileIOPermission
- ManagementBaseObject
- EditorBrowsableState
- IEnumerator`1
- UnverifiableCodeAttribute
- GetObjectValue
- GetGlobalValue
- ComVisibleAttribute
- UriComponents
- GetComponents
- ConfusedByAttribute
- RawSecurityDescriptor
- InternalPreserveStackTrace
- DefaultSettingValueAttribute
- add_DocumentCompleted

- SetCustomAttribute
- @"@3@>@O@V@_@f@l@v@}@
- <!<9<B<G<U<z<

- **Module 4 (probably unpacked / injected by the sample)**

  - **Module 4 rich signatures**

    - No rich signatures found

  - **Module 4 strings**

    - **Module 4 most interesting strings**

    - <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
    - text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
    - !This program cannot be run in DOS mode.
    - <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
    - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    - <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
    - text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/;q=0.8
    - Accept-Encoding: gzip, deflate, br
    - ERROR_NO_MORE_ITEMS
    - AssemblyBuilder
    - get_FieldHandle
    - get_LocalPath
    - RuntimeHelpers
    - CustomAttributeBuilder
    - get_MainWindowTitle
    - set_Arguments
    - set_UserAgent
    - SuspendThread
    - AddressFamily
    - StringFileInfo
    - get_OperationalStatus
    - KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingleFileGenerator
    - System.Net.Security
    - PAGE_EXECUTE
    - LocalCertificateSelectionCallback
    - add_AssemblyResolve
    - System.Windows.Forms
    - System.Drawing
    - System.Security.Cryptography.X509Certificates
    - get_Position
    - Assembly Version
    - get_IsAbstract
    - HttpWebResponse
    - GCHandleType
    - PAGE_READONLY
    - PAGE_NOCACHE
    - set_ServerCertificateValidationCallback
    - set_ProtocolVersion
    - LocalMachine
    - IPGlobalProperties
    - DebuggingModes

- {0} /{1} HTTP/1.1
- G(G8GHGXGcGvG
- ExpandEnvironmentVariables
- AssemblyBuilderAccess
- GetIPGlobalProperties
- get_CurrentThread
- DWebBrowserEvents2_BeforeNavigate2EventHandler
- GetExecutingAssembly
- ResourceManager
- LocalBuilder
- GetResponseStream
- <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
- get_HasValue
- L!L-L<LHLTLiL
- get_IsStatic
- ApplicationSettingsBase
- get_BaseAddress
- ManagementObjectSearcher
- WebBrowserDocumentCompletedEventHandler
- GetElementType
- set_DefaultConnectionLimit
- S@LT&KE4343242343Y;
- get_IsPointer
- GetHostAddresses
- GetCustomAttributes
- GetProcesses
- System.Net.Sockets
- System.Resources
- FileIOPermissionAccess
- remove_DocumentCompleted
- getElementsByTagName
- get_Assembly
- MakeByRefType
- DeflateStream
- SUSPEND_RESUME
- AssemblyNameFlags
- get_IsValueType
- INTERNET_COOKIE_HTTPONLY
- ExecuteWriteCopy
- ReadAllBytes
- gzip, deflate, br
- get_ParameterType
- StringBuilder
- get_ReturnType
- DownloadString
- gzip, deflate, sdch, br
- System.Net.NetworkInformation
- GetAllNetworkInterfaces
- set_CreateNoWindow
- RtlSetProcessIsCritical
- DeclareLocal
- get_FieldType
- get_CharacterSet
- get_ReadyState
- get_BytesReceived
- get_ElapsedMilliseconds
- NetworkStream

- set_UseShellExecute
- ResolveSignature
- System.Security.Principal
- EnterDebugMode
- GetTargetType
- get_TickCount
- ResolveMember
- set_IsBackground
- sslPolicyErrors
- NetworkAccess
- HttpStatusCode
- DefineDynamicAssembly
- OperationalStatus
- get_Location
- GetRequestStream
- <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
- IsLittleEndian
- System.Security.Permissions.SecurityPermissionAttribute, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
- PasswordHash
- get_BytesSent
- IsWow64Process
- FormatterServices
- get_Document
- HttpWebRequest
- ResolveEventArgs
- ReadAllLines
- WriteCombineModifierflag
- System.Runtime.CompilerServices
- MemoryStream
- CryptoStreamMode
- SpecialFolder
- WebBrowserBase
- GetProcessesByName
- NB2.Properties
- StreamWriter
- System.Runtime.InteropServices
- get_StatusCode
- NoCacheModifierflag
- get_LocalEndPoint
- set_Position
- get_ProcessName
- set_Expect100Continue
- System.Runtime.Serialization
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- H&H.H6H;:HGHMHVHdHmH
- BinaryReader
- CryptoStream
- User-Agent: {0}
- VS_VERSION_INFO
- get_PrimaryScreen
- GetConstructors
- WrapNonExceptionThrows
- SymmetricAlgorithm
- get_Connected
- GetParameters
- _remoteStackTraceString

- IAsyncResult
- ScriptEngine
- PropertyInfo
- get_FileName
- PAGE_WRITECOMBINE
- set_ContentLength
- GetFolderPath
- get_FullyQualifiedName
- get_TypeHandle
- PAGE_EXECUTE_READWRITE
- set_FileName
- SettingsBase
- ConstructorInfo
- Upgrade-Insecure-Requests: 1
- DynamicILInfo
- </trustInfo>
- </requestedPrivileges>
- get_ExecutablePath
- get_BaseType
- set_KeepAlive
- get_ThreadState
- GetValueOrDefault
- MakeGenericType
- AceQualifier
- GetManifestResourceStream
- PAGE_READWRITE
- get_IsConstructor
- get_DeclaringType
- get_UserName
- get_MainModule
- BindingFlags
- get_ActiveXInstance
- AppendFormat
- InvokeMember
- get_IsPrimitive
- ZwSetInformationProcess
- get_CultureInfo
- get_RemoteEndPoint
- System.Runtime.ExceptionServices.ExceptionDispatchInfo
- get_NetworkInterfaceType
- ModuleBuilder
- SecurityIdentifier
- GetCurrentProcess
- INTERNET_COOKIE_THIRD_PARTY
- SET_THREAD_TOKEN
- INTERNET_FLAG_RESTRICTED_ZONE
- FromBase64String
- GetFunctionPointer
- CookieContainer
- System.IO.Compression
- get_MetadataToken
- get_CurrentDomain
- OriginalFilename
- GetUnderlyingType
- get_OriginalString
- System.Threading
- IsAssignableFrom

- GetValueNames
- lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- get_IsInterface
- Connection: Keep-Alive
- System.CodeDom.Compiler
- ServicePointManager
- GetResourceString
- Cache-Control: no-cache
- get_ServerCertificateValidationCallback
- AllocHGlobal
- WebBrowserDocumentCompletedEventArgs
- get_IsAttached
- ProtocolType
- set_ContentType
- WellKnownSidType
- set_ScriptErrorsSuppressed
- PAGE_NOACCESS
- set_UseNagleAlgorithm
- GetDynamicILInfo
- get_ModuleMemorySize
- StreamReader
- NetworkInterfaceType
- CreateRemoteThread
- System.Reflection.Emit
- RoaZ .PQua8g
- get_DiscretionaryAcl
- Rfc2898DeriveBytes
- GuardModifierflag
- Accept-Encoding
- ProcessStartInfo
- PAGE_WRITECOPY
- HttpResponseHeader
- $88b6efb0-83b0-4cbd-a2d9-3a37200bd51b
- get_ProcessorCount
- GetEntryAssembly
- ParameterInfo
- ProcessThread
- AssemblyName
- oiTDMIW}^ln"o\\,pEA\\\\-\\,i5%6%.resources
- SetLocalSignature
- GetAssemblies
- get_MethodHandle
- ReadOnlyCollectionBase
- KeyValuePair`2
- ERROR_INSUFFICIENT_BUFFER
- PAGE_EXECUTE_READ
- BitConverter
- get_InnerException
- get_IsVirtual
- GetCommandLineArgs
- GetOptionalCustomModifiers
- LegalCopyright
- IsInstanceOfType
- get_IsAbsoluteUri
- RemoteCertificateValidationCallback
- ERROR_INVALID_PARAMETER

- get_BinaryLength
- ResolveEventHandler
- 3System.Resources.Tools.StronglyTypedResourceBuilder
- CompressionMode
- AsyncCallback
- InternalName
- SET_INFORMATION
- set_WindowStyle
- PAGE_EXECUTE_WRITECOPY
- text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- +j|Zf 'Tc!a}
- ReadProcessMemory
- VirtualProtectEx
- IsDebuggerPresent
- CheckRemoteDebuggerPresent
- VirtualAllocEx
- WriteProcessMemory
- InternetGetCookieExW
- SetKernelObjectSecurity
- GetPhysicallyInstalledSystemMemory
- GetKernelObjectSecurity
- VirtualQueryEx
- NtUnmapViewOfSection

- **Module 4 other strings**

- Cache-control
- GeneratedCodeAttribute
- TcpConnectionInformation
- DebuggableAttribute
- GetBaseDefinition
- costura.jurassic.dll.compressed
- System.Security.AccessControl
- GetFileNameWithoutExtension
- Dictionary`2
- GetGetMethod
- ThreadStaticAttribute
- ManagementObjectEnumerator
- System.Diagnostics
- DWebBrowserEvents2_Event
- GetIsNetworkAvailable
- System.Collections.Generic
- ExecutionEngineException
- @1B2c3D4e5F6g7H8
- oiTDMIW}^ln"o,pEA\\-,i5%6%
- EditorBrowsableAttribute
- ManagementObjectCollection
- AssemblyCopyrightAttribute
- System.ComponentModel
- System.Collections
- InitializeArray
- UserScopedSettingAttribute
- System.Security.Permissions
- TypedReference
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute

- AddrOfPinnedObject
- GetUninitializedObject
- DebuggerNonUserCodeAttribute
- O;O<G=O>W?G@
- GetActiveTcpConnections
- SystemException
- IEnumerable`1
- CodeAccessPermission
- ExtensionAttribute
- System.Globalization
- QUERY_INFORMATION
- STAThreadAttribute
- StackOverflowException
- InvalidCastException
- IPv4InterfaceStatistics
- RuntimeMethodHandle
- FileDescription
- ParameterizedThreadStart
- ProcessThreadCollection
- AssemblyFileVersionAttribute
- System.Management
- ProcessWindowStyle
- DownloadFile
- CompilerGeneratedAttribute
- GetMethodDescriptor
- WindowsIdentity
- MulticastDelegate
- ConfuserEx v1.0.0
- GroupCollection
- WebPermission
- application/x-www-form-urlencoded
- AssemblyProductAttribute
- RuntimeCompatibilityAttribute
- NullReferenceException
- CreateSubKey
- InternalsVisibleToAttribute
- GetIPv4Statistics
- LegalTrademarks
- Synchronized
- NameValueCollection
- X509Certificate
- kernel32.dll
- ArithmeticException
- CreateDecryptor
- DynamicMethod
- PointToScreen
- WriteAllText
- CompilationRelaxationsAttribute
- StringComparison
- ApartmentState
- OverflowException
- costura.interop.shdocvw.dll.compressed
- DIRECT_IMPERSONATION
- SkipVerification
- FlagsAttribute
- HtmlDocument
- System.Configuration

- SecurityCriticalAttribute
- GetBinaryForm
- GetEnumerator
- GetTypeFromHandle
- AssemblyConfigurationAttribute
- SetApartmentState
- RijndaelManaged
- ResolveMethod
- Microsoft.Win32
- CreateDelegate
- System.Collections.Specialized
- System.Security.Cryptography
- ProcessModule
- NetworkInterface
- AssemblyTitleAttribute
- op_Inequality
- ICryptoTransform
- DebuggerBrowsableAttribute
- MatchCollection
- TargetInvocationException
- NotSupportedException
- P@@Sw0rd54690fj48743843789eey3
- ToLowerInvariant
- Interop.SHDocVw
- AssemblyTrademarkAttribute
- SetValueDirect
- DefineDynamicModule
- GenericSecurityDescriptor
- add_BeforeNavigate2
- GetConstructor
- ManagementObject
- ProductVersion
- DebuggerBrowsableState
- GetLastWin32Error
- GetHINSTANCE
- GuidAttribute
- WebHeaderCollection
- ExecuteReadWrite
- AssemblyCompanyAttribute
- PlatformNotSupportedException
- HtmlElementCollection
- Win32Exception
- DeleteSubKey
- SecurityAction
- WebBrowserReadyState
- advapi32.dll
- AssemblyDescriptionAttribute
- ParamArrayAttribute
- GetFieldFromHandle
- System.Text.RegularExpressions
- GetILGenerator
- System.Security
- RuntimeFieldHandle
- IsNullOrEmpty
- H6jZ dDfba8`
- SecurityPermissionAttribute
- InvalidProgramException

- ArgumentNullException
- RuntimeTypeHandle
- AuthenticateAsClient
- System.Reflection
- FileIOPermission
- ManagementBaseObject
- EditorBrowsableState
- IEnumerator`1
- UnverifiableCodeAttribute
- GetObjectValue
- GetGlobalValue
- ComVisibleAttribute
- UriComponents
- GetComponents
- ConfusedByAttribute
- RawSecurityDescriptor
- InternalPreserveStackTrace
- DefaultSettingValueAttribute
- add_DocumentCompleted
- SetCustomAttribute
- @"@3@>@O@V@_@f@l@v@}@
- <!<9<B<G<U<z<

Extra Information Recovered

In this section there is additional information recovered by platform plugins

Configs Recovered

In this section there are malware configs recovered by platform plugins