Sample: ae4d420c05281acf9696e558b02a42f8

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: **#PWS #AGENTTESLA** (based on p3pperp0tts rules)

Analysis date: 2019-06-18 14:42:31 (p3pperp0tts platform's analysis date)

Exe timestamp: 2019-05-05 22:12:38 (timestamp of the original sample)

Unpacked mods max timestamp: 2019-05-05 22:12:38 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2019-05-08 20:31:00 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: ae4d420c05281acf9696e558b02a42f8

AV detections

- Microsoft: PWS:Win32/AgentTesla.YB!MTB
- Kaspersky: HEUR:Trojan.MSIL.Scarsi.gen
- Symantec: ML.Attribute.HighConfidence
- Malwarebytes: Spyware.AgentTesla.Generic

Source

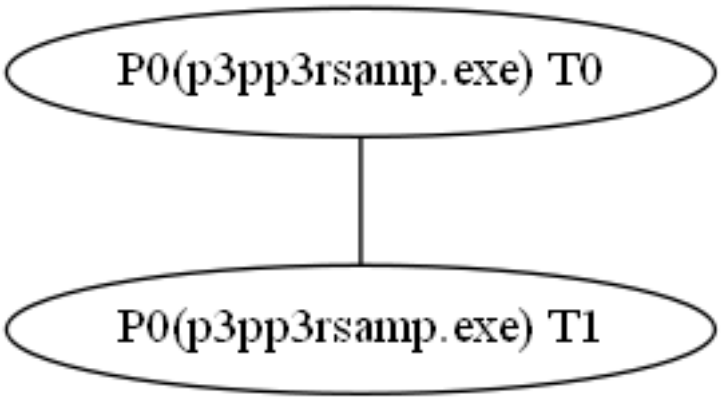
-

Virustotal

- https://virustotal.com/es/file/5c741edbd2de663b174758bde17b7f4b7179d55473c9b6a9b67d21eb33766ebd/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.

- Process Create (C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe PID: PUNKALIAS, Command line: "C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe")
- Thread Create (Thread ID: TUNKALIAS)
- Thread Create (Thread ID: T1)

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.

- get_PasswordHash
- !This program cannot be run in DOS mode.
- ALG_CLASS_HASH
- set_Password
- STATURL_QUERYFLAGS
- StringFileInfo
- Dispose__Instance__
- GetLastInputInfo
- get_OSVersion
- SortFileTimeAscending
- set_AllowAutoRedirect
- _urlHistoryList
- InternetExplorer
- System.Windows.Forms
- System.Drawing
- STATURL_QUERYFLAG_NOTITLE
- ConditionalCompareObjectLess
- Assembly Version
- astable_name
- VaultCloseVault
- set_Attributes
- CryptCreateHash
- AppendFormat
- szDisplayName
- GetImageEncoders
- LocalMachine
- GetWindowTextLength
- set_Credentials
- IEAutoCompleteSecretHeader
- DoesURLMatchWithHash
- STATURLFLAG_ISCACHED
- DebuggingModes
- STATURLFLAGS
- ALG_SID_SHA1
- ManagementClass
- remove_KeyDown
- EncoderParameters
- SHGFI_EXETYPE
- dwAttributes
- VaultOpenVault
- SHA1CryptoServiceProvider
- System.Collections.IComparer.Compare
- CreateParams
- GetDirectories
- ConditionalCompareObjectEqual
- SetAttributes
- FileVersionInfo
- get_CurrentThread
- set_EnableSsl
- FileTimeToDateTime
- GetExecutingAssembly

- FtpWebRequest
- ResourceManager
- DelegateAsyncResult
- GetInstances
- Microsoft.VisualBasic.Devices
- GetResponseStream
- EscapeDataString
- SHGFI_TYPENAME
- SHGFI_ATTRIBUTES
- ILC_COLORDDB
- URL_ESCAPE_PERCENT
- set_MaximumAutomaticRedirections
- SHGFI_ATTR_SPECIFIED
- ManagementObjectSearcher
- STATURL_QUERYFLAG_TOPLEVEL
- ProcessStartInfo
- GetSubKeyNames
- Auto-vacuum capable database is not supported
- m_ComputerObjectProvider
- get_StartInfo
- $3C374A41-BAE4-11CF-BF7D-00AA006946EE
- System.Net.Mail
- get_Registry
- GetProcesses
- VideocardName
- System.Resources
- My.WebServices
- get_ProductName
- get_EnumUrls
- ImageCodecInfo
- ChangeClipboardChain
- get_BigEndianUnicode
- remove_Click
- get_DriveType
- SortFileTimeAscendingHelper
- ConditionalCompareObjectGreaterEqual
- remove_KeyUp
- get_DefaultCredentials
- get_LastVisited
- lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- ReadAllBytes
- GetVersionInfo
- pszContainer
- VaultEnumerateItems
- StringBuilder
- get_ComputerName
- DownloadString
- get_IsInvalid
- GetURLHashString
- pszCredentialFriendlyName
- set_CreateNoWindow
- SetClipboardViewer
- m_MyWebServicesObjectProvider
- $3C374A40-BAE4-11CF-BF7D-00AA006946EE
- set_UseShellExecute
- System.Security.Principal

- ElapsedEventHandler
- HashParameters
- get_InvariantCulture
- get_TickCount
- punkISFolder
- get_CapsLock
- set_IsBackground
- get_AltKeyDown
- SHGFI_DISPLAYNAME
- CRYPT_VERIFYCONTEXT
- remove_Wheel
- get_Location
- Not a valid SQLite 3 Database File
- GetRequestStream
- FromBase64String
- NumberStyles
- NewLateBinding
- $3C374A42-BAE4-11CF-BF7D-00AA006946EE
- ComInterfaceType
- get_EndOfStream
- HttpWebRequest
- OperatingSystemName
- URL_UNESCAPE
- DataProtectionScope
- System.Runtime.CompilerServices
- GetCallingAssembly
- MemoryStream
- ComputerInfo
- get_WebServices
- GetProcessesByName
- get_Capacity
- Microsoft.VisualBasic.MyServices
- ServerComputer
- get_FormatID
- remove_DoubleClick
- System.Runtime.InteropServices
- get_ProcessName
- ObjectIdentifier
- GetProcessById
- lpSystemTime
- SHGetFileInfo
- 4System.Web.Services.Protocols.SoapHttpClientProtocol
- UnescapeDataString
- get_StandardOutput
- vaultcli.dll
- SHGFI_SHELLICONSIZE
- EnumProcessModules
- get_ShiftKeyDown
- dwFileAttributes
- GetDirectoryName
- VS_VERSION_INFO
- WindowsPrincipal
- System.Timers
- WrapNonExceptionThrows
- SymmetricAlgorithm
- FileAttributes
- ConditionalCompareObjectNotEqual

- IAsyncResult
- ConditionalCompareObjectGreater
- PtrToStringUni
- IESecretInfoHeader
- get_FileName
- GetSavedCookies
- ToBase64String
- get_Properties
- set_ContentLength
- GetFolderPath
- get_FullyQualifiedName
- <Username>k__BackingField
- set_FileName
- UrlHistoryClass
- HashAlgorithm
- TransformFinalBlock
- set_UseDefaultCredentials
- get_ExecutablePath
- set_KeepAlive
- IUrlHistoryStg
- AceQualifier
- ElapsedEventArgs
- IFormatProvider
- STATURL_QUERYFLAG_NOURL
- ProcessorName
- get_MainModule
- get_CtrlKeyDown
- SHGFI_LARGEICON
- System.Drawing.Imaging
- SHGFI_SMALLICON
- get_Millisecond
- Microsoft.VisualBasic.ApplicationServices
- System.Runtime.InteropServices.ComTypes
- CompareObjectEqual
- URL_ESCAPE_SPACES_ONLY
- get_GetInstance
- set_IsBodyHtml
- DateTimeToFileTime
- URL_ESCAPE_UNSAFE
- +-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
- UTF8Encoding
- LateIndexGet
- Unknow database format
- SecurityIdentifier
- GetCurrentProcess
- ByteArrayToStructure
- CompareObjectGreater
- get_Application
- FileTimeToSystemTime
- Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2
- set_Username
- get_TotalFreeSpace
- DelegateCallback
- ReadAllLines
- get_Clipboard
- STATURL_QUERYFLAG_ISCACHED
- IESecretHeader

- OriginalFilename
- SHGFI_SYSICONINDEX
- CompareString
- get_TotalPhysicalMemory
- System.Threading
- GetValueNames
- get_FileSystem
- GetWindowThreadProcessId
- System.Runtime.ConstrainedExecution
- PROV_RSA_FULL
- Microsoft.VisualBasic.CompilerServices
- System.CodeDom.Compiler
- CompareFileTime
- get_Computer
- STATURLFLAG_ISTOPLEVEL
- SystemTimeToFileTime
- C:\\Users\\Admin\\Desktop\\IELibrary\\IELibrary\\obj\\Debug\\IELibrary.pdb
- CompareObjectNotEqual
- get_IsAttached
- get_UrlString
- CryptGetHashParam
- set_ContentType
- WellKnownSidType
- m_AppObjectProvider
- SpecialFolder
- NetworkCredential
- cbSizeFileInfo
- get_Attachments
- StreamReader
- GCHandleType
- <Browser>k__BackingField
- ApplicationBase
- get_Keyboard
- get_DiscretionaryAcl
- BinaryReader
- PtrToStructure
- GetPrivateProfileString
- KeyValuePair`2
- get_Password
- FILE_ATTRIBUTRE_NORMAL
- System.ComponentModel.Design
- SHGFI_USEFILEATTRIBUTES
- ICredentialsByHost
- TripleDESCryptoServiceProvider
- BitConverter
- add_DoubleClick
- m_UserObjectProvider
- set_Capacity
- get_OSFullName
- LegalCopyright
- SQLite format 3
- get_BinaryLength
- get_UserName
- remove_Changed
- set_RedirectStandardOutput
- SchemaElementId
- CryptDestroyHash

- FileSystemInfo
- AsyncCallback
- InternalName
- set_WindowStyle
- EncoderParameter
- get_LastUpdated
- 1.85 (Hash, version 2, native byte-order)
- TB International
- yW{uOkygCi[]aSu^
- (c) 1998 Ziegler Group
- RuntimeHelpers
- (r?wjrh__Gs}ei^A
- FGS - Fluid Global Solutions
- Ziegler Group
- lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- QSystem.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
- hSystem.Drawing.Bitmap, System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3aPADPADwe
- xHd.resources
- System.Drawing.Bitmap
- LateIndexSet
- GetEnvironmentVariable
- GetWindowText
- MapVirtualKey
- CreateDirectory
- SetWindowsHookEx
- CryptAcquireContext
- GetForegroundWindow
- CallNextHookEx
- VirtualProtect
- SetKernelObjectSecurity
- CryptHashData
- SetWindowsHookExA
- GetDiskFreeSpaceExA
- GetKernelObjectSecurity
- UnhookWindowsHookEx
- GetKeyboardState
- GetKeyboardLayout
- GetModuleFileNameA
- CryptReleaseContext
- VirtualAlloc

Hosts

- 192.168.149.199:49184
- 52.202.139.131:80 (checkip.amazonaws.com)

Dns queries

- 2.149.168.192.in-addr.arpa ---> no answers
- 255.149.168.192.in-addr.arpa ---> no answers
- 254.149.168.192.in-addr.arpa ---> no answers
- checkip.amazonaws.com ---> 52.202.139.131, 18.211.215.84, 52.206.161.133, 52.200.125.74, 34.233.102.38, 52.6.79.229
- 131.139.202.52.in-addr.arpa ---> no answers

Network traffic

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

- **tcp 192.168.149.199:49184 ---> 52.202.139.131 (checkip.amazonaws.com) :80**

  Connection: Keep-Alive[...]Host: checkip.amazonaws.com[...]GET / HTTP/1.1

- **tcp 52.202.139.131 (checkip.amazonaws.com) :80 ---> 192.168.149.199:49184**

  Server: lighttpd/1.4.41[...]HTTP/1.1 200 OK[...]HTTP/1.1 200 OK[...]Connection: Keep-Alive[...]Date: Tue, 18 Jun 2019 12:30:26 GMT[...]Content-Length: 11

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.

- get_PasswordHash
- !This program cannot be run in DOS mode.
- ALG_CLASS_HASH
- set_Password
- STATURL_QUERYFLAGS
- StringFileInfo
- Dispose__Instance__
- GetLastInputInfo
- get_OSVersion
- SortFileTimeAscending
- set_AllowAutoRedirect
- _urlHistoryList
- InternetExplorer
- System.Windows.Forms
- System.Drawing
- STATURL_QUERYFLAG_NOTITLE
- ConditionalCompareObjectLess
- Assembly Version
- astable_name
- VaultCloseVault
- set_Attributes
- CryptCreateHash
- AppendFormat
- szDisplayName
- GetImageEncoders
- LocalMachine
- GetWindowTextLength
- set_Credentials
- IEAutoCompleteSecretHeader
- DoesURLMatchWithHash
- STATURLFLAG_ISCACHED
- DebuggingModes
- STATURLFLAGS
- ALG_SID_SHA1
- ManagementClass
- remove_KeyDown
- EncoderParameters
- SHGFI_EXETYPE
- dwAttributes
- VaultOpenVault
- SHA1CryptoServiceProvider
- System.Collections.IComparer.Compare
- CreateParams
- GetDirectories
- ConditionalCompareObjectEqual
- SetAttributes
- FileVersionInfo
- get_CurrentThread
- set_EnableSsl
- FileTimeToDateTime
- GetExecutingAssembly

- FtpWebRequest
- ResourceManager
- DelegateAsyncResult
- GetInstances
- Microsoft.VisualBasic.Devices
- GetResponseStream
- EscapeDataString
- SHGFI_TYPENAME
- SHGFI_ATTRIBUTES
- ILC_COLORDDB
- URL_ESCAPE_PERCENT
- set_MaximumAutomaticRedirections
- SHGFI_ATTR_SPECIFIED
- ManagementObjectSearcher
- STATURL_QUERYFLAG_TOPLEVEL
- ProcessStartInfo
- GetSubKeyNames
- Auto-vacuum capable database is not supported
- m_ComputerObjectProvider
- get_StartInfo
- $3C374A41-BAE4-11CF-BF7D-00AA006946EE
- System.Net.Mail
- get_Registry
- GetProcesses
- VideocardName
- System.Resources
- My.WebServices
- get_ProductName
- get_EnumUrls
- ImageCodecInfo
- ChangeClipboardChain
- get_BigEndianUnicode
- remove_Click
- get_DriveType
- SortFileTimeAscendingHelper
- ConditionalCompareObjectGreaterEqual
- remove_KeyUp
- get_DefaultCredentials
- get_LastVisited
- lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- ReadAllBytes
- GetVersionInfo
- pszContainer
- VaultEnumerateItems
- StringBuilder
- get_ComputerName
- DownloadString
- get_IsInvalid
- GetURLHashString
- pszCredentialFriendlyName
- set_CreateNoWindow
- SetClipboardViewer
- m_MyWebServicesObjectProvider
- $3C374A40-BAE4-11CF-BF7D-00AA006946EE
- set_UseShellExecute
- System.Security.Principal

- ElapsedEventHandler
- HashParameters
- get_InvariantCulture
- get_TickCount
- punkISFolder
- get_CapsLock
- set_IsBackground
- get_AltKeyDown
- SHGFI_DISPLAYNAME
- CRYPT_VERIFYCONTEXT
- remove_Wheel
- get_Location
- Not a valid SQLite 3 Database File
- GetRequestStream
- FromBase64String
- NumberStyles
- NewLateBinding
- $3C374A42-BAE4-11CF-BF7D-00AA006946EE
- ComInterfaceType
- get_EndOfStream
- HttpWebRequest
- OperatingSystemName
- URL_UNESCAPE
- DataProtectionScope
- System.Runtime.CompilerServices
- GetCallingAssembly
- MemoryStream
- ComputerInfo
- get_WebServices
- GetProcessesByName
- get_Capacity
- Microsoft.VisualBasic.MyServices
- ServerComputer
- get_FormatID
- remove_DoubleClick
- System.Runtime.InteropServices
- get_ProcessName
- ObjectIdentifier
- GetProcessById
- lpSystemTime
- SHGetFileInfo
- 4System.Web.Services.Protocols.SoapHttpClientProtocol
- UnescapeDataString
- get_StandardOutput
- vaultcli.dll
- SHGFI_SHELLICONSIZE
- EnumProcessModules
- get_ShiftKeyDown
- dwFileAttributes
- GetDirectoryName
- VS_VERSION_INFO
- WindowsPrincipal
- System.Timers
- WrapNonExceptionThrows
- SymmetricAlgorithm
- FileAttributes
- ConditionalCompareObjectNotEqual

- IAsyncResult
- ConditionalCompareObjectGreater
- PtrToStringUni
- IESecretInfoHeader
- get_FileName
- GetSavedCookies
- ToBase64String
- get_Properties
- set_ContentLength
- GetFolderPath
- get_FullyQualifiedName
- <Username>k__BackingField
- set_FileName
- UrlHistoryClass
- HashAlgorithm
- TransformFinalBlock
- set_UseDefaultCredentials
- get_ExecutablePath
- set_KeepAlive
- IUrlHistoryStg
- AceQualifier
- ElapsedEventArgs
- IFormatProvider
- STATURL_QUERYFLAG_NOURL
- ProcessorName
- get_MainModule
- get_CtrlKeyDown
- SHGFI_LARGEICON
- System.Drawing.Imaging
- SHGFI_SMALLICON
- get_Millisecond
- Microsoft.VisualBasic.ApplicationServices
- System.Runtime.InteropServices.ComTypes
- CompareObjectEqual
- URL_ESCAPE_SPACES_ONLY
- get_GetInstance
- set_IsBodyHtml
- DateTimeToFileTime
- URL_ESCAPE_UNSAFE
- +-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
- UTF8Encoding
- LateIndexGet
- Unknow database format
- SecurityIdentifier
- GetCurrentProcess
- ByteArrayToStructure
- CompareObjectGreater
- get_Application
- FileTimeToSystemTime
- Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2
- set_Username
- get_TotalFreeSpace
- DelegateCallback
- ReadAllLines
- get_Clipboard
- STATURL_QUERYFLAG_ISCACHED
- IESecretHeader

- OriginalFilename
- SHGFI_SYSICONINDEX
- CompareString
- get_TotalPhysicalMemory
- System.Threading
- GetValueNames
- get_FileSystem
- GetWindowThreadProcessId
- System.Runtime.ConstrainedExecution
- PROV_RSA_FULL
- Microsoft.VisualBasic.CompilerServices
- System.CodeDom.Compiler
- CompareFileTime
- get_Computer
- STATURLFLAG_ISTOPLEVEL
- SystemTimeToFileTime
- C:\\Users\\Admin\\Desktop\\IELibrary\\IELibrary\\obj\\Debug\\IELibrary.pdb
- CompareObjectNotEqual
- get_IsAttached
- get_UrlString
- CryptGetHashParam
- set_ContentType
- WellKnownSidType
- m_AppObjectProvider
- SpecialFolder
- NetworkCredential
- cbSizeFileInfo
- get_Attachments
- StreamReader
- GCHandleType
- <Browser>k__BackingField
- ApplicationBase
- get_Keyboard
- get_DiscretionaryAcl
- BinaryReader
- PtrToStructure
- GetPrivateProfileString
- KeyValuePair`2
- get_Password
- FILE_ATTRIBUTRE_NORMAL
- System.ComponentModel.Design
- SHGFI_USEFILEATTRIBUTES
- ICredentialsByHost
- TripleDESCryptoServiceProvider
- BitConverter
- add_DoubleClick
- m_UserObjectProvider
- set_Capacity
- get_OSFullName
- LegalCopyright
- SQLite format 3
- get_BinaryLength
- get_UserName
- remove_Changed
- set_RedirectStandardOutput
- SchemaElementId
- CryptDestroyHash

- FileSystemInfo
- AsyncCallback
- InternalName
- set_WindowStyle
- EncoderParameter
- get_LastUpdated
- 1.85 (Hash, version 2, native byte-order)
- TB International
- yW{uOkygCi[]aSu^
- (c) 1998 Ziegler Group
- RuntimeHelpers
- (r?wjrh__Gs}ei^A
- FGS - Fluid Global Solutions
- Ziegler Group
- lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- QSystem.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
- hSystem.Drawing.Bitmap, System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3aPADPADwe
- xHd.resources
- System.Drawing.Bitmap
- LateIndexSet
- GetEnvironmentVariable
- GetWindowText
- MapVirtualKey
- CreateDirectory
- SetWindowsHookEx
- CryptAcquireContext
- GetForegroundWindow
- CallNextHookEx
- VirtualProtect
- SetKernelObjectSecurity
- CryptHashData
- SetWindowsHookExA
- GetDiskFreeSpaceExA
- GetKernelObjectSecurity
- UnhookWindowsHookEx
- GetKeyboardState
- GetKeyboardLayout
- GetModuleFileNameA
- CryptReleaseContext
- ADDURL_ADDTOCACHE
- $AFA0DC11-C313-11D0-831A-00C04FD5AE38
- DebuggableAttribute
- IUrlHistoryStg2
- milliseconds
- System.Security.AccessControl
- dwSecretInfoSize
- GetFileNameWithoutExtension
- Dictionary`2
- $83018595-3f8a-4e71-94b2-8e41a61ed763
- ThreadStaticAttribute
- ManagementObjectEnumerator
- GetUrlHistory
- System.Diagnostics
- System.Collections.Generic
- FileNotFoundException
- pcchCanonicalized

- URL_PLUGGABLE_PROTOCOL
- RegQueryValueEx
- fWriteHistory
- EditorBrowsableAttribute
- ManagementObjectCollection
- m_ThreadStaticValue
- AssemblyTrademarkAttribute
- AssemblyCopyrightAttribute
- System.ComponentModel
- System.Collections
- ReleaseHandle
- InitializeArray
- GetExtension
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- CreateProjectError
- AddUrlAndNotify
- PropertyDataCollection
- MyGroupCollectionAttribute
- ExplorerUrlHistory
- IEnumerable`1
- System.Globalization
- STAThreadAttribute
- ArgumentOutOfRangeException
- MouseButtons
- DefaultMemberAttribute
- FileAttribute
- FileDescription
- ParameterizedThreadStart
- TargetMethod
- System.Management
- ProtectedData
- "!#!$!%!&!,+10203240506087 97:7;7<7>=?=@=BACBDB
- ProcessWindowStyle
- CreateEncryptor
- DefaultValueAttribute
- PropertyData
- WindowsBuiltInRole
- LastModified
- CompilerGeneratedAttribute
- ILD_TRANSPARENT
- WindowsIdentity
- MulticastDelegate
- AddHistoryEntry
- ClipboardProxy
- GroupCollection
- DelegateAsyncState
- <Password>k__BackingField
- AssemblyProductAttribute
- Collection`1
- My.Application
- RuntimeCompatibilityAttribute
- CreateSubKey
- ADDURL_ADDTOHISTORYANDCACHE
- SystemInformation
- LegalTrademarks

- CopyFromScreen
- Microsoft.VisualBasic
- AppendAllText
- HideModuleNameAttribute
- sql_statement
- dwPropertiesCount
- CreateDecryptor
- TargetObject
- WH_KEYBOARD_LL
- UrlCanonicalize
- RegOpenKeyEx
- SuppressIldasmAttribute
- pceltFetched
- advapi32.dll
- WriteAllText
- pResourceElement
- CompilationRelaxationsAttribute
- StringComparison
- IEnumSTATURL
- WithEventsValue
- ConcatenateObject
- pPropertyElements
- FileSystemProxy
- dwSecretSize
- ClearHistory
- CreateObject
- GetBinaryForm
- GetEnumerator
- AmountOfMemory
- GetTypeFromHandle
- StandardModuleAttribute
- IndexOutOfRangeException
- AssemblyConfigurationAttribute
- RecoveredBrowserAccount
- GetCharCount
- Microsoft.Win32
- Create__Instance__
- System.Security.Cryptography
- ProcessModule
- GetModuleFileNameEx
- AssemblyTitleAttribute
- FrameworkVersion
- HelpKeywordAttribute
- ICryptoTransform
- DebuggerBrowsableAttribute
- MatchCollection
- DebuggerHiddenAttribute
- SetProjectError
- ClearProjectError
- AssemblyFileVersionAttribute
- DeleteHistoryEntry
- pszCanonicalized
- LateSetComplex
- RegistryProxy
- AttachmentCollection
- ReliabilityContractAttribute
- GetPropertyValue

- GenericSecurityDescriptor
- <Url>k__BackingField
- GetSavedPasswords
- pIdentityElement
- VaultEnumerateVaults
- ProductVersion
- DebuggerBrowsableState
- GetLastWin32Error
- GetHINSTANCE
- GuidAttribute
- KeyCollection
- OperatingSystem
- ReleaseComObject
- AssemblyCompanyAttribute
- InterfaceTypeAttribute
- Win32Exception
- ProtectedArray
- CreateHandle
- DeleteSubKey
- ftLastVisited
- AssemblyDescriptionAttribute
- pAuthenticatorElement
- BindToObject
- System.Text.RegularExpressions
- Authenticator
- ftLastUpdated
- System.Security
- RuntimeFieldHandle
- AccessedThroughPropertyAttribute
- IsNullOrEmpty
- System.Collections.ObjectModel
- FlagsAttribute
- STATURLEnumerator
- unsignedShort
- NativeWindow
- URL_DONT_SIMPLIFY
- RuntimeTypeHandle
- System.Reflection
- ManagementBaseObject
- EditorBrowsableState
- kernel32.dll
- IELibrary.dll
- op_Inequality
- SearchOption
- DivideObject
- dwTotalSecrets
- GetObjectValue
- ManagementObject
- ComVisibleAttribute
- CompareMethod
- RegistryValueKind
- SubtractObject
- RawSecurityDescriptor
- CredentialCache
- CannonializeURL
- VirtualAlloc
- s#]z<Py2:=96dNH

- MultiplyObject
- LeftShiftObject
- GeneratedCodeAttribute
- CallWindowProc
- mebcfxwgjmsq
- LLKHF_INJECTED
- WM_SYSKEYDOWN
- LLKHF_EXTENDED
- LLKHF_ALTDOWN
- 5g]QFSeN{Cqg[

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**
    - Process Create (C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe PID: PUNKALIAS, Command line: "C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe")
    - Thread Create (Thread ID: TUNKALIAS)
    - Thread Create (Thread ID: TUNKALIAS)
    - Thread Create (Thread ID: T1)
    - Thread Create (Thread ID: TUNKALIAS)
- **Thread T1 (in process P0, p3pp3rsamp.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**

- get_PasswordHash
- !This program cannot be run in DOS mode.
- ALG_CLASS_HASH
- set_Password
- STATURL_QUERYFLAGS
- StringFileInfo
- Dispose__Instance__
- GetLastInputInfo
- get_OSVersion
- SortFileTimeAscending
- set_AllowAutoRedirect
- _urlHistoryList
- InternetExplorer
- System.Windows.Forms
- System.Drawing
- STATURL_QUERYFLAG_NOTITLE
- ConditionalCompareObjectLess
- Assembly Version
- astable_name
- VaultCloseVault
- set_Attributes
- CryptCreateHash
- AppendFormat
- szDisplayName
- GetImageEncoders
- LocalMachine
- GetWindowTextLength
- set_Credentials
- IEAutoCompleteSecretHeader
- DoesURLMatchWithHash
- STATURLFLAG_ISCACHED
- DebuggingModes
- STATURLFLAGS
- ALG_SID_SHA1
- ManagementClass
- remove_KeyDown
- EncoderParameters
- SHGFI_EXETYPE
- dwAttributes
- VaultOpenVault
- SHA1CryptoServiceProvider

- System.Collections.IComparer.Compare
- CreateParams
- GetDirectories
- ConditionalCompareObjectEqual
- SetAttributes
- FileVersionInfo
- get_CurrentThread
- set_EnableSsl
- FileTimeToDateTime
- GetExecutingAssembly
- FtpWebRequest
- ResourceManager
- DelegateAsyncResult
- GetInstances
- Microsoft.VisualBasic.Devices
- GetResponseStream
- EscapeDataString
- SHGFI_TYPENAME
- SHGFI_ATTRIBUTES
- ILC_COLORDDB
- URL_ESCAPE_PERCENT
- set_MaximumAutomaticRedirections
- SHGFI_ATTR_SPECIFIED
- ManagementObjectSearcher
- STATURL_QUERYFLAG_TOPLEVEL
- ProcessStartInfo
- GetSubKeyNames
- Auto-vacuum capable database is not supported
- m_ComputerObjectProvider
- get_StartInfo
- $3C374A41-BAE4-11CF-BF7D-00AA006946EE
- System.Net.Mail
- get_Registry
- GetProcesses
- VideocardName
- System.Resources
- My.WebServices
- get_ProductName
- get_EnumUrls
- ImageCodecInfo
- ChangeClipboardChain
- get_BigEndianUnicode
- remove_Click
- get_DriveType
- SortFileTimeAscendingHelper
- ConditionalCompareObjectGreaterEqual
- remove_KeyUp
- get_DefaultCredentials
- get_LastVisited
- lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- ReadAllBytes
- GetVersionInfo
- pszContainer
- VaultEnumerateItems
- StringBuilder
- get_ComputerName

- DownloadString
- get_IsInvalid
- GetURLHashString
- pszCredentialFriendlyName
- set_CreateNoWindow
- SetClipboardViewer
- m_MyWebServicesObjectProvider
- $3C374A40-BAE4-11CF-BF7D-00AA006946EE
- set_UseShellExecute
- System.Security.Principal
- ElapsedEventHandler
- HashParameters
- get_InvariantCulture
- get_TickCount
- punkISFolder
- get_CapsLock
- set_IsBackground
- get_AltKeyDown
- SHGFI_DISPLAYNAME
- CRYPT_VERIFYCONTEXT
- remove_Wheel
- get_Location
- Not a valid SQLite 3 Database File
- GetRequestStream
- FromBase64String
- NumberStyles
- NewLateBinding
- $3C374A42-BAE4-11CF-BF7D-00AA006946EE
- ComInterfaceType
- get_EndOfStream
- HttpWebRequest
- OperatingSystemName
- URL_UNESCAPE
- DataProtectionScope
- System.Runtime.CompilerServices
- GetCallingAssembly
- MemoryStream
- ComputerInfo
- get_WebServices
- GetProcessesByName
- get_Capacity
- Microsoft.VisualBasic.MyServices
- ServerComputer
- get_FormatID
- remove_DoubleClick
- System.Runtime.InteropServices
- get_ProcessName
- ObjectIdentifier
- GetProcessById
- lpSystemTime
- SHGetFileInfo
- 4System.Web.Services.Protocols.SoapHttpClientProtocol
- UnescapeDataString
- get_StandardOutput
- vaultcli.dll
- SHGFI_SHELLICONSIZE
- EnumProcessModules

- get_ShiftKeyDown
- dwFileAttributes
- GetDirectoryName
- VS_VERSION_INFO
- WindowsPrincipal
- System.Timers
- WrapNonExceptionThrows
- SymmetricAlgorithm
- FileAttributes
- ConditionalCompareObjectNotEqual
- IAsyncResult
- ConditionalCompareObjectGreater
- PtrToStringUni
- IESecretInfoHeader
- get_FileName
- GetSavedCookies
- ToBase64String
- get_Properties
- set_ContentLength
- GetFolderPath
- get_FullyQualifiedName
- <Username>k__BackingField
- set_FileName
- UrlHistoryClass
- HashAlgorithm
- TransformFinalBlock
- set_UseDefaultCredentials
- get_ExecutablePath
- set_KeepAlive
- IUrlHistoryStg
- AceQualifier
- ElapsedEventArgs
- IFormatProvider
- STATURL_QUERYFLAG_NOURL
- ProcessorName
- get_MainModule
- get_CtrlKeyDown
- SHGFI_LARGEICON
- System.Drawing.Imaging
- SHGFI_SMALLICON
- get_Millisecond
- Microsoft.VisualBasic.ApplicationServices
- System.Runtime.InteropServices.ComTypes
- CompareObjectEqual
- URL_ESCAPE_SPACES_ONLY
- get_GetInstance
- set_IsBodyHtml
- DateTimeToFileTime
- URL_ESCAPE_UNSAFE
- +-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
- UTF8Encoding
- LateIndexGet
- Unknow database format
- SecurityIdentifier
- GetCurrentProcess
- ByteArrayToStructure
- CompareObjectGreater

- get_Application
- FileTimeToSystemTime
- Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2
- set_Username
- get_TotalFreeSpace
- DelegateCallback
- ReadAllLines
- get_Clipboard
- STATURL_QUERYFLAG_ISCACHED
- IESecretHeader
- OriginalFilename
- SHGFI_SYSICONINDEX
- CompareString
- get_TotalPhysicalMemory
- System.Threading
- GetValueNames
- get_FileSystem
- GetWindowThreadProcessId
- System.Runtime.ConstrainedExecution
- PROV_RSA_FULL
- Microsoft.VisualBasic.CompilerServices
- System.CodeDom.Compiler
- CompareFileTime
- get_Computer
- STATURLFLAG_ISTOPLEVEL
- SystemTimeToFileTime
- C:\\Users\\Admin\\Desktop\\IELibrary\\IELibrary\\obj\\Debug\\IELibrary.pdb
- CompareObjectNotEqual
- get_IsAttached
- get_UrlString
- CryptGetHashParam
- set_ContentType
- WellKnownSidType
- m_AppObjectProvider
- SpecialFolder
- NetworkCredential
- cbSizeFileInfo
- get_Attachments
- StreamReader
- GCHandleType
- <Browser>k__BackingField
- ApplicationBase
- get_Keyboard
- get_DiscretionaryAcl
- BinaryReader
- PtrToStructure
- GetPrivateProfileString
- KeyValuePair`2
- get_Password
- FILE_ATTRIBUTRE_NORMAL
- System.ComponentModel.Design
- SHGFI_USEFILEATTRIBUTES
- ICredentialsByHost
- TripleDESCryptoServiceProvider
- BitConverter
- add_DoubleClick
- m_UserObjectProvider

- set_Capacity
- get_OSFullName
- LegalCopyright
- SQLite format 3
- get_BinaryLength
- get_UserName
- remove_Changed
- set_RedirectStandardOutput
- SchemaElementId
- CryptDestroyHash
- FileSystemInfo
- AsyncCallback
- InternalName
- set_WindowStyle
- EncoderParameter
- get_LastUpdated
- 1.85 (Hash, version 2, native byte-order)
- GetEnvironmentVariable
- GetWindowText
- MapVirtualKey
- CreateDirectory
- SetWindowsHookEx
- CryptAcquireContext
- GetForegroundWindow
- CallNextHookEx
- VirtualProtect
- SetKernelObjectSecurity
- CryptHashData
- SetWindowsHookExA
- GetDiskFreeSpaceExA
- GetKernelObjectSecurity
- UnhookWindowsHookEx
- GetKeyboardState
- GetKeyboardLayout
- GetModuleFileNameA
- CryptReleaseContext

- **Module 1 other strings**

- ADDURL_ADDTOCACHE
- $AFA0DC11-C313-11D0-831A-00C04FD5AE38
- DebuggableAttribute
- IUrlHistoryStg2
- milliseconds
- System.Security.AccessControl
- dwSecretInfoSize
- GetFileNameWithoutExtension
- Dictionary`2
- $83018595-3f8a-4e71-94b2-8e41a61ed763
- ThreadStaticAttribute
- ManagementObjectEnumerator
- GetUrlHistory
- System.Diagnostics
- System.Collections.Generic
- FileNotFoundException
- pcchCanonicalized

- URL_PLUGGABLE_PROTOCOL
- RegQueryValueEx
- fWriteHistory
- EditorBrowsableAttribute
- ManagementObjectCollection
- m_ThreadStaticValue
- AssemblyTrademarkAttribute
- AssemblyCopyrightAttribute
- System.ComponentModel
- System.Collections
- ReleaseHandle
- InitializeArray
- GetExtension
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- CreateProjectError
- AddUrlAndNotify
- PropertyDataCollection
- MyGroupCollectionAttribute
- ExplorerUrlHistory
- IEnumerable`1
- System.Globalization
- STAThreadAttribute
- ArgumentOutOfRangeException
- MouseButtons
- DefaultMemberAttribute
- FileAttribute
- FileDescription
- ParameterizedThreadStart
- TargetMethod
- System.Management
- ProtectedData
- 7;7<7>=?=@=BACBDB
- ProcessWindowStyle
- CreateEncryptor
- DefaultValueAttribute
- PropertyData
- WindowsBuiltInRole
- LastModified
- CompilerGeneratedAttribute
- ILD_TRANSPARENT
- WindowsIdentity
- MulticastDelegate
- AddHistoryEntry
- ClipboardProxy
- GroupCollection
- DelegateAsyncState
- <Password>k__BackingField
- AssemblyProductAttribute
- Collection`1
- My.Application
- RuntimeCompatibilityAttribute
- CreateSubKey
- ADDURL_ADDTOHISTORYANDCACHE
- SystemInformation
- LegalTrademarks

- CopyFromScreen
- Microsoft.VisualBasic
- AppendAllText
- HideModuleNameAttribute
- sql_statement
- dwPropertiesCount
- CreateDecryptor
- TargetObject
- WH_KEYBOARD_LL
- UrlCanonicalize
- RegOpenKeyEx
- SuppressIldasmAttribute
- pceltFetched
- advapi32.dll
- WriteAllText
- pResourceElement
- CompilationRelaxationsAttribute
- StringComparison
- IEnumSTATURL
- WithEventsValue
- ConcatenateObject
- pPropertyElements
- FileSystemProxy
- dwSecretSize
- ClearHistory
- CreateObject
- GetBinaryForm
- GetEnumerator
- AmountOfMemory
- GetTypeFromHandle
- StandardModuleAttribute
- IndexOutOfRangeException
- AssemblyConfigurationAttribute
- RecoveredBrowserAccount
- GetCharCount
- Microsoft.Win32
- Create__Instance__
- System.Security.Cryptography
- ProcessModule
- GetModuleFileNameEx
- AssemblyTitleAttribute
- FrameworkVersion
- HelpKeywordAttribute
- ICryptoTransform
- DebuggerBrowsableAttribute
- MatchCollection
- DebuggerHiddenAttribute
- SetProjectError
- ClearProjectError
- AssemblyFileVersionAttribute
- DeleteHistoryEntry
- pszCanonicalized
- LateSetComplex
- RegistryProxy
- AttachmentCollection
- ReliabilityContractAttribute
- GetPropertyValue

- GenericSecurityDescriptor
- <Url>k__BackingField
- GetSavedPasswords
- pIdentityElement
- VaultEnumerateVaults
- ProductVersion
- DebuggerBrowsableState
- GetLastWin32Error
- GetHINSTANCE
- GuidAttribute
- KeyCollection
- OperatingSystem
- ReleaseComObject
- AssemblyCompanyAttribute
- InterfaceTypeAttribute
- Win32Exception
- ProtectedArray
- CreateHandle
- DeleteSubKey
- ftLastVisited
- AssemblyDescriptionAttribute
- pAuthenticatorElement
- BindToObject
- System.Text.RegularExpressions
- Authenticator
- ftLastUpdated
- System.Security
- RuntimeFieldHandle
- AccessedThroughPropertyAttribute
- IsNullOrEmpty
- System.Collections.ObjectModel
- FlagsAttribute
- STATURLEnumerator
- unsignedShort
- NativeWindow
- URL_DONT_SIMPLIFY
- RuntimeTypeHandle
- System.Reflection
- ManagementBaseObject
- EditorBrowsableState
- kernel32.dll
- IELibrary.dll
- op_Inequality
- SearchOption
- DivideObject
- dwTotalSecrets
- GetObjectValue
- ManagementObject
- ComVisibleAttribute
- CompareMethod
- RegistryValueKind
- SubtractObject
- RawSecurityDescriptor
- CredentialCache
- CannonializeURL
- mebcfxwgjmsq
- LLKHF_INJECTED

- WM_SYSKEYDOWN
- LLKHF_EXTENDED
- LLKHF_ALTDOWN

Module 2 (probably unpacked / injected by the sample)

Module 2 rich signatures

- No rich signatures found

Module 2 strings

Module 2 most interesting strings

- get_PasswordHash
- !This program cannot be run in DOS mode.
- ALG_CLASS_HASH
- set_Password
- STATURL_QUERYFLAGS
- StringFileInfo
- Dispose__Instance__
- GetLastInputInfo
- get_OSVersion
- SortFileTimeAscending
- set_AllowAutoRedirect
- _urlHistoryList
- InternetExplorer
- System.Windows.Forms
- System.Drawing
- STATURL_QUERYFLAG_NOTITLE
- ConditionalCompareObjectLess
- Assembly Version
- astable_name
- VaultCloseVault
- set_Attributes
- CryptCreateHash
- AppendFormat
- szDisplayName
- GetImageEncoders
- LocalMachine
- GetWindowTextLength
- set_Credentials
- IEAutoCompleteSecretHeader
- DoesURLMatchWithHash
- STATURLFLAG_ISCACHED
- DebuggingModes
- STATURLFLAGS
- ALG_SID_SHA1
- ManagementClass
- remove_KeyDown
- EncoderParameters
- SHGFI_EXETYPE
- dwAttributes
- VaultOpenVault
- SHA1CryptoServiceProvider

- System.Collections.IComparer.Compare
- CreateParams
- GetDirectories
- ConditionalCompareObjectEqual
- SetAttributes
- FileVersionInfo
- get_CurrentThread
- set_EnableSsl
- FileTimeToDateTime
- GetExecutingAssembly
- FtpWebRequest
- ResourceManager
- DelegateAsyncResult
- GetInstances
- Microsoft.VisualBasic.Devices
- GetResponseStream
- EscapeDataString
- SHGFI_TYPENAME
- SHGFI_ATTRIBUTES
- ILC_COLORDDB
- URL_ESCAPE_PERCENT
- set_MaximumAutomaticRedirections
- SHGFI_ATTR_SPECIFIED
- ManagementObjectSearcher
- STATURL_QUERYFLAG_TOPLEVEL
- ProcessStartInfo
- GetSubKeyNames
- Auto-vacuum capable database is not supported
- m_ComputerObjectProvider
- get_StartInfo
- $3C374A41-BAE4-11CF-BF7D-00AA006946EE
- System.Net.Mail
- get_Registry
- GetProcesses
- VideocardName
- System.Resources
- My.WebServices
- get_ProductName
- get_EnumUrls
- ImageCodecInfo
- ChangeClipboardChain
- get_BigEndianUnicode
- remove_Click
- get_DriveType
- SortFileTimeAscendingHelper
- ConditionalCompareObjectGreaterEqual
- remove_KeyUp
- get_DefaultCredentials
- get_LastVisited
- lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- ReadAllBytes
- GetVersionInfo
- pszContainer
- VaultEnumerateItems
- StringBuilder
- get_ComputerName

- DownloadString
- get_IsInvalid
- GetURLHashString
- pszCredentialFriendlyName
- set_CreateNoWindow
- SetClipboardViewer
- m_MyWebServicesObjectProvider
- $3C374A40-BAE4-11CF-BF7D-00AA006946EE
- set_UseShellExecute
- System.Security.Principal
- ElapsedEventHandler
- HashParameters
- get_InvariantCulture
- get_TickCount
- punkISFolder
- get_CapsLock
- set_IsBackground
- get_AltKeyDown
- SHGFI_DISPLAYNAME
- CRYPT_VERIFYCONTEXT
- remove_Wheel
- get_Location
- Not a valid SQLite 3 Database File
- GetRequestStream
- FromBase64String
- NumberStyles
- NewLateBinding
- $3C374A42-BAE4-11CF-BF7D-00AA006946EE
- ComInterfaceType
- get_EndOfStream
- HttpWebRequest
- OperatingSystemName
- URL_UNESCAPE
- DataProtectionScope
- System.Runtime.CompilerServices
- GetCallingAssembly
- MemoryStream
- ComputerInfo
- get_WebServices
- GetProcessesByName
- get_Capacity
- Microsoft.VisualBasic.MyServices
- ServerComputer
- get_FormatID
- remove_DoubleClick
- System.Runtime.InteropServices
- get_ProcessName
- ObjectIdentifier
- GetProcessById
- lpSystemTime
- SHGetFileInfo
- 4System.Web.Services.Protocols.SoapHttpClientProtocol
- UnescapeDataString
- get_StandardOutput
- vaultcli.dll
- SHGFI_SHELLICONSIZE
- EnumProcessModules

- get_ShiftKeyDown
- dwFileAttributes
- GetDirectoryName
- VS_VERSION_INFO
- WindowsPrincipal
- System.Timers
- WrapNonExceptionThrows
- SymmetricAlgorithm
- FileAttributes
- ConditionalCompareObjectNotEqual
- IAsyncResult
- ConditionalCompareObjectGreater
- PtrToStringUni
- IESecretInfoHeader
- get_FileName
- GetSavedCookies
- ToBase64String
- get_Properties
- set_ContentLength
- GetFolderPath
- get_FullyQualifiedName
- <Username>k__BackingField
- set_FileName
- UrlHistoryClass
- HashAlgorithm
- TransformFinalBlock
- set_UseDefaultCredentials
- get_ExecutablePath
- set_KeepAlive
- IUrlHistoryStg
- AceQualifier
- ElapsedEventArgs
- IFormatProvider
- STATURL_QUERYFLAG_NOURL
- ProcessorName
- get_MainModule
- get_CtrlKeyDown
- SHGFI_LARGEICON
- System.Drawing.Imaging
- SHGFI_SMALLICON
- get_Millisecond
- Microsoft.VisualBasic.ApplicationServices
- System.Runtime.InteropServices.ComTypes
- CompareObjectEqual
- URL_ESCAPE_SPACES_ONLY
- get_GetInstance
- set_IsBodyHtml
- DateTimeToFileTime
- URL_ESCAPE_UNSAFE
- +-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
- UTF8Encoding
- LateIndexGet
- Unknow database format
- SecurityIdentifier
- GetCurrentProcess
- ByteArrayToStructure
- CompareObjectGreater

- get_Application
- FileTimeToSystemTime
- Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2
- set_Username
- get_TotalFreeSpace
- DelegateCallback
- ReadAllLines
- get_Clipboard
- STATURL_QUERYFLAG_ISCACHED
- IESecretHeader
- OriginalFilename
- SHGFI_SYSICONINDEX
- CompareString
- get_TotalPhysicalMemory
- System.Threading
- GetValueNames
- get_FileSystem
- GetWindowThreadProcessId
- System.Runtime.ConstrainedExecution
- PROV_RSA_FULL
- Microsoft.VisualBasic.CompilerServices
- System.CodeDom.Compiler
- CompareFileTime
- get_Computer
- STATURLFLAG_ISTOPLEVEL
- SystemTimeToFileTime
- C:\\Users\\Admin\\Desktop\\IELibrary\\IELibrary\\obj\\Debug\\IELibrary.pdb
- CompareObjectNotEqual
- get_IsAttached
- get_UrlString
- CryptGetHashParam
- set_ContentType
- WellKnownSidType
- m_AppObjectProvider
- SpecialFolder
- NetworkCredential
- cbSizeFileInfo
- get_Attachments
- StreamReader
- GCHandleType
- <Browser>k__BackingField
- ApplicationBase
- get_Keyboard
- get_DiscretionaryAcl
- BinaryReader
- PtrToStructure
- GetPrivateProfileString
- KeyValuePair`2
- get_Password
- FILE_ATTRIBUTRE_NORMAL
- System.ComponentModel.Design
- SHGFI_USEFILEATTRIBUTES
- ICredentialsByHost
- TripleDESCryptoServiceProvider
- BitConverter
- add_DoubleClick
- m_UserObjectProvider

- set_Capacity
- get_OSFullName
- LegalCopyright
- SQLite format 3
- get_BinaryLength
- get_UserName
- remove_Changed
- set_RedirectStandardOutput
- SchemaElementId
- CryptDestroyHash
- FileSystemInfo
- AsyncCallback
- InternalName
- set_WindowStyle
- EncoderParameter
- get_LastUpdated
- 1.85 (Hash, version 2, native byte-order)
- GetEnvironmentVariable
- GetWindowText
- MapVirtualKey
- CreateDirectory
- SetWindowsHookEx
- CryptAcquireContext
- GetForegroundWindow
- CallNextHookEx
- VirtualProtect
- SetKernelObjectSecurity
- CryptHashData
- SetWindowsHookExA
- GetDiskFreeSpaceExA
- GetKernelObjectSecurity
- UnhookWindowsHookEx
- GetKeyboardState
- GetKeyboardLayout
- GetModuleFileNameA
- CryptReleaseContext

- **Module 2 other strings**

- ADDURL_ADDTOCACHE
- $AFA0DC11-C313-11D0-831A-00C04FD5AE38
- DebuggableAttribute
- IUrlHistoryStg2
- milliseconds
- System.Security.AccessControl
- dwSecretInfoSize
- GetFileNameWithoutExtension
- Dictionary`2
- $83018595-3f8a-4e71-94b2-8e41a61ed763
- ThreadStaticAttribute
- ManagementObjectEnumerator
- GetUrlHistory
- System.Diagnostics
- System.Collections.Generic
- FileNotFoundException
- pcchCanonicalized

- URL_PLUGGABLE_PROTOCOL
- RegQueryValueEx
- fWriteHistory
- EditorBrowsableAttribute
- ManagementObjectCollection
- m_ThreadStaticValue
- AssemblyTrademarkAttribute
- AssemblyCopyrightAttribute
- System.ComponentModel
- System.Collections
- ReleaseHandle
- InitializeArray
- GetExtension
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- CreateProjectError
- AddUrlAndNotify
- PropertyDataCollection
- MyGroupCollectionAttribute
- ExplorerUrlHistory
- IEnumerable`1
- System.Globalization
- STAThreadAttribute
- ArgumentOutOfRangeException
- MouseButtons
- DefaultMemberAttribute
- FileAttribute
- FileDescription
- ParameterizedThreadStart
- TargetMethod
- System.Management
- ProtectedData
- 7;7<7>=?=@=BACBDB
- ProcessWindowStyle
- CreateEncryptor
- DefaultValueAttribute
- PropertyData
- WindowsBuiltInRole
- LastModified
- CompilerGeneratedAttribute
- ILD_TRANSPARENT
- WindowsIdentity
- MulticastDelegate
- AddHistoryEntry
- ClipboardProxy
- GroupCollection
- DelegateAsyncState
- <Password>k__BackingField
- AssemblyProductAttribute
- Collection`1
- My.Application
- RuntimeCompatibilityAttribute
- CreateSubKey
- ADDURL_ADDTOHISTORYANDCACHE
- SystemInformation
- LegalTrademarks

- CopyFromScreen
- Microsoft.VisualBasic
- AppendAllText
- HideModuleNameAttribute
- sql_statement
- dwPropertiesCount
- CreateDecryptor
- TargetObject
- WH_KEYBOARD_LL
- UrlCanonicalize
- RegOpenKeyEx
- SuppressIldasmAttribute
- pceltFetched
- advapi32.dll
- WriteAllText
- pResourceElement
- CompilationRelaxationsAttribute
- StringComparison
- IEnumSTATURL
- WithEventsValue
- ConcatenateObject
- pPropertyElements
- FileSystemProxy
- dwSecretSize
- ClearHistory
- CreateObject
- GetBinaryForm
- GetEnumerator
- AmountOfMemory
- GetTypeFromHandle
- StandardModuleAttribute
- IndexOutOfRangeException
- AssemblyConfigurationAttribute
- RecoveredBrowserAccount
- GetCharCount
- Microsoft.Win32
- Create__Instance__
- System.Security.Cryptography
- ProcessModule
- GetModuleFileNameEx
- AssemblyTitleAttribute
- FrameworkVersion
- HelpKeywordAttribute
- ICryptoTransform
- DebuggerBrowsableAttribute
- MatchCollection
- DebuggerHiddenAttribute
- SetProjectError
- ClearProjectError
- AssemblyFileVersionAttribute
- DeleteHistoryEntry
- pszCanonicalized
- LateSetComplex
- RegistryProxy
- AttachmentCollection
- ReliabilityContractAttribute
- GetPropertyValue

- GenericSecurityDescriptor
- <Url>k__BackingField
- GetSavedPasswords
- pIdentityElement
- VaultEnumerateVaults
- ProductVersion
- DebuggerBrowsableState
- GetLastWin32Error
- GetHINSTANCE
- GuidAttribute
- KeyCollection
- OperatingSystem
- ReleaseComObject
- AssemblyCompanyAttribute
- InterfaceTypeAttribute
- Win32Exception
- ProtectedArray
- CreateHandle
- DeleteSubKey
- ftLastVisited
- AssemblyDescriptionAttribute
- pAuthenticatorElement
- BindToObject
- System.Text.RegularExpressions
- Authenticator
- ftLastUpdated
- System.Security
- RuntimeFieldHandle
- AccessedThroughPropertyAttribute
- IsNullOrEmpty
- System.Collections.ObjectModel
- FlagsAttribute
- STATURLEnumerator
- unsignedShort
- NativeWindow
- URL_DONT_SIMPLIFY
- RuntimeTypeHandle
- System.Reflection
- ManagementBaseObject
- EditorBrowsableState
- kernel32.dll
- IELibrary.dll
- op_Inequality
- SearchOption
- DivideObject
- dwTotalSecrets
- GetObjectValue
- ManagementObject
- ComVisibleAttribute
- CompareMethod
- RegistryValueKind
- SubtractObject
- RawSecurityDescriptor
- CredentialCache
- CannonializeURL
- mebcfxwgjmsq
- LLKHF_INJECTED

- WM_SYSKEYDOWN
- LLKHF_EXTENDED
- LLKHF_ALTDOWN

Module 3 (probably unpacked / injected by the sample)

Module 3 rich signatures

- No rich signatures found

Module 3 strings

Module 3 most interesting strings

- !This program cannot be run in DOS mode.
- System.Drawing
- TB International
- Microsoft.VisualBasic.ApplicationServices
- CompareObjectEqual
- NewLateBinding
- yW{uOkygCi[]aSu^
- (c) 1998 Ziegler Group
- RuntimeHelpers
- (r?wjrh__Gs}ei^A
- Dispose__Instance__
- OriginalFilename
- My.WebServices
- FGS - Fluid Global Solutions
- Ziegler Group
- Microsoft.VisualBasic.Devices
- System.Runtime.CompilerServices
- VS_VERSION_INFO
- 4System.Web.Services.Protocols.SoapHttpClientProtocol
- lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- LegalCopyright
- LateIndexGet
- BitConverter
- WrapNonExceptionThrows
- QSystem.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
- hSystem.Drawing.Bitmap, System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3aPADPADwe
- Microsoft.VisualBasic.CompilerServices
- xHd.resources
- InternalName
- ApplicationBase
- System.Drawing.Bitmap
- System.CodeDom.Compiler
- System.Runtime.InteropServices
- StringFileInfo
- System.ComponentModel.Design
- LateIndexSet
- Assembly Version
- VirtualAlloc

Module 3 other strings

- System.Security.Cryptography
- GetTypeFromHandle
- AssemblyCopyrightAttribute
- System.ComponentModel
- =96dNH
- StandardModuleAttribute
- MultiplyObject
- System.Diagnostics
- HelpKeywordAttribute
- FileDescription
- GetObjectValue
- AssemblyTitleAttribute
- CreateInstance
- LeftShiftObject
- Microsoft.VisualBasic
- STAThreadAttribute
- AssemblyFileVersionAttribute
- GeneratedCodeAttribute
- Create__Instance__
- RuntimeTypeHandle
- LateSetComplex
- CompilationRelaxationsAttribute
- HideModuleNameAttribute
- MyGroupCollectionAttribute
- DebuggerHiddenAttribute
- SubtractObject
- System.Reflection
- AssemblyProductAttribute
- CallWindowProc
- My.Application
- ThreadStaticAttribute
- RuntimeCompatibilityAttribute
- EditorBrowsableState
- ComVisibleAttribute
- EditorBrowsableAttribute
- ProductVersion
- AssemblyCompanyAttribute
- CompilerGeneratedAttribute
- 5g]QFSeN{Cqg[

Module 4 (probably unpacked / injected by the sample)

Module 4 rich signatures

- No rich signatures found

Module 4 strings

Module 4 most interesting strings

- !This program cannot be run in DOS mode.
- System.Drawing
- TB International
- Microsoft.VisualBasic.ApplicationServices

- CompareObjectEqual
- NewLateBinding
- yW{uOkygCi[]aSu^
- (c) 1998 Ziegler Group
- RuntimeHelpers
- (r?wjrh__Gs}ei^A
- Dispose__Instance__
- OriginalFilename
- My.WebServices
- FGS - Fluid Global Solutions
- Ziegler Group
- Microsoft.VisualBasic.Devices
- System.Runtime.CompilerServices
- VS_VERSION_INFO
- 4System.Web.Services.Protocols.SoapHttpClientProtocol
- lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- LegalCopyright
- LateIndexGet
- BitConverter
- WrapNonExceptionThrows
- QSystem.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
- hSystem.Drawing.Bitmap, System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3aPADPADwe
- Microsoft.VisualBasic.CompilerServices
- xHd.resources
- InternalName
- ApplicationBase
- System.Drawing.Bitmap
- System.CodeDom.Compiler
- System.Runtime.InteropServices
- StringFileInfo
- System.ComponentModel.Design
- LateIndexSet
- Assembly Version
- VirtualAlloc

- **Module 4 other strings**

- System.Security.Cryptography
- GetTypeFromHandle
- AssemblyCopyrightAttribute
- System.ComponentModel
- =96dNH
- StandardModuleAttribute
- MultiplyObject
- System.Diagnostics
- HelpKeywordAttribute
- FileDescription
- GetObjectValue
- AssemblyTitleAttribute
- CreateInstance
- LeftShiftObject
- Microsoft.VisualBasic
- STAThreadAttribute
- AssemblyFileVersionAttribute
- GeneratedCodeAttribute

- Create__Instance__
- RuntimeTypeHandle
- LateSetComplex
- CompilationRelaxationsAttribute
- HideModuleNameAttribute
- MyGroupCollectionAttribute
- DebuggerHiddenAttribute
- SubtractObject
- System.Reflection
- AssemblyProductAttribute
- CallWindowProc
- My.Application
- ThreadStaticAttribute
- RuntimeCompatibilityAttribute
- EditorBrowsableState
- ComVisibleAttribute
- EditorBrowsableAttribute
- ProductVersion
- AssemblyCompanyAttribute
- CompilerGeneratedAttribute
- 5g]QFSeN{Cqg[

Module 5 (probably unpacked / injected by the sample)

Module 5 rich signatures

- No rich signatures found

Module 5 strings

Module 5 most interesting strings

- get_PasswordHash
- !This program cannot be run in DOS mode.
- ALG_CLASS_HASH
- set_Password
- STATURL_QUERYFLAGS
- StringFileInfo
- Dispose__Instance__
- GetLastInputInfo
- get_OSVersion
- SortFileTimeAscending
- set_AllowAutoRedirect
- _urlHistoryList
- InternetExplorer
- System.Windows.Forms
- System.Drawing
- STATURL_QUERYFLAG_NOTITLE
- ConditionalCompareObjectLess
- Assembly Version
- astable_name
- VaultCloseVault
- set_Attributes
- CryptCreateHash
- AppendFormat

- szDisplayName
- GetImageEncoders
- LocalMachine
- GetWindowTextLength
- set_Credentials
- IEAutoCompleteSecretHeader
- DoesURLMatchWithHash
- STATURLFLAG_ISCACHED
- DebuggingModes
- STATURLFLAGS
- ALG_SID_SHA1
- ManagementClass
- remove_KeyDown
- EncoderParameters
- SHGFI_EXETYPE
- dwAttributes
- VaultOpenVault
- SHA1CryptoServiceProvider
- System.Collections.IComparer.Compare
- CreateParams
- GetDirectories
- ConditionalCompareObjectEqual
- SetAttributes
- FileVersionInfo
- get_CurrentThread
- set_EnableSsl
- FileTimeToDateTime
- GetExecutingAssembly
- FtpWebRequest
- ResourceManager
- DelegateAsyncResult
- GetInstances
- Microsoft.VisualBasic.Devices
- GetResponseStream
- EscapeDataString
- SHGFI_TYPENAME
- SHGFI_ATTRIBUTES
- ILC_COLORDDB
- URL_ESCAPE_PERCENT
- set_MaximumAutomaticRedirections
- SHGFI_ATTR_SPECIFIED
- ManagementObjectSearcher
- STATURL_QUERYFLAG_TOPLEVEL
- ProcessStartInfo
- GetSubKeyNames
- Auto-vacuum capable database is not supported
- m_ComputerObjectProvider
- get_StartInfo
- $3C374A41-BAE4-11CF-BF7D-00AA006946EE
- System.Net.Mail
- get_Registry
- GetProcesses
- VideocardName
- System.Resources
- My.WebServices
- get_ProductName
- get_EnumUrls

- ImageCodecInfo
- ChangeClipboardChain
- get_BigEndianUnicode
- remove_Click
- get_DriveType
- SortFileTimeAscendingHelper
- ConditionalCompareObjectGreaterEqual
- remove_KeyUp
- get_DefaultCredentials
- get_LastVisited
- lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- ReadAllBytes
- GetVersionInfo
- pszContainer
- VaultEnumerateItems
- StringBuilder
- get_ComputerName
- DownloadString
- get_IsInvalid
- GetURLHashString
- pszCredentialFriendlyName
- set_CreateNoWindow
- SetClipboardViewer
- m_MyWebServicesObjectProvider
- $3C374A40-BAE4-11CF-BF7D-00AA006946EE
- set_UseShellExecute
- System.Security.Principal
- ElapsedEventHandler
- HashParameters
- get_InvariantCulture
- get_TickCount
- punkISFolder
- get_CapsLock
- set_IsBackground
- get_AltKeyDown
- SHGFI_DISPLAYNAME
- CRYPT_VERIFYCONTEXT
- remove_Wheel
- get_Location
- Not a valid SQLite 3 Database File
- GetRequestStream
- FromBase64String
- NumberStyles
- NewLateBinding
- $3C374A42-BAE4-11CF-BF7D-00AA006946EE
- ComInterfaceType
- get_EndOfStream
- HttpWebRequest
- OperatingSystemName
- URL_UNESCAPE
- DataProtectionScope
- System.Runtime.CompilerServices
- GetCallingAssembly
- MemoryStream
- ComputerInfo
- get_WebServices

- GetProcessesByName
- get_Capacity
- Microsoft.VisualBasic.MyServices
- ServerComputer
- get_FormatID
- remove_DoubleClick
- System.Runtime.InteropServices
- get_ProcessName
- ObjectIdentifier
- GetProcessById
- lpSystemTime
- SHGetFileInfo
- 4System.Web.Services.Protocols.SoapHttpClientProtocol
- UnescapeDataString
- get_StandardOutput
- vaultcli.dll
- SHGFI_SHELLICONSIZE
- EnumProcessModules
- get_ShiftKeyDown
- dwFileAttributes
- GetDirectoryName
- VS_VERSION_INFO
- WindowsPrincipal
- System.Timers
- WrapNonExceptionThrows
- SymmetricAlgorithm
- FileAttributes
- ConditionalCompareObjectNotEqual
- IAsyncResult
- ConditionalCompareObjectGreater
- PtrToStringUni
- IESecretInfoHeader
- get_FileName
- GetSavedCookies
- ToBase64String
- get_Properties
- set_ContentLength
- GetFolderPath
- get_FullyQualifiedName
- <Username>k__BackingField
- set_FileName
- UrlHistoryClass
- HashAlgorithm
- TransformFinalBlock
- set_UseDefaultCredentials
- get_ExecutablePath
- set_KeepAlive
- IUrlHistoryStg
- AceQualifier
- ElapsedEventArgs
- IFormatProvider
- STATURL_QUERYFLAG_NOURL
- ProcessorName
- get_MainModule
- get_CtrlKeyDown
- SHGFI_LARGEICON
- System.Drawing.Imaging

- SHGFI_SMALLICON
- get_Millisecond
- Microsoft.VisualBasic.ApplicationServices
- System.Runtime.InteropServices.ComTypes
- CompareObjectEqual
- URL_ESCAPE_SPACES_ONLY
- get_GetInstance
- set_IsBodyHtml
- DateTimeToFileTime
- URL_ESCAPE_UNSAFE
- +-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
- UTF8Encoding
- LateIndexGet
- Unknow database format
- SecurityIdentifier
- GetCurrentProcess
- ByteArrayToStructure
- CompareObjectGreater
- get_Application
- FileTimeToSystemTime
- Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2
- set_Username
- get_TotalFreeSpace
- DelegateCallback
- ReadAllLines
- get_Clipboard
- STATURL_QUERYFLAG_ISCACHED
- IESecretHeader
- OriginalFilename
- SHGFI_SYSICONINDEX
- CompareString
- get_TotalPhysicalMemory
- System.Threading
- GetValueNames
- get_FileSystem
- GetWindowThreadProcessId
- System.Runtime.ConstrainedExecution
- PROV_RSA_FULL
- Microsoft.VisualBasic.CompilerServices
- System.CodeDom.Compiler
- CompareFileTime
- get_Computer
- STATURLFLAG_ISTOPLEVEL
- SystemTimeToFileTime
- C:\\Users\\Admin\\Desktop\\IELibrary\\IELibrary\\obj\\Debug\\IELibrary.pdb
- CompareObjectNotEqual
- get_IsAttached
- get_UrlString
- CryptGetHashParam
- set_ContentType
- WellKnownSidType
- m_AppObjectProvider
- SpecialFolder
- NetworkCredential
- cbSizeFileInfo
- get_Attachments
- StreamReader

- GCHandleType
- <Browser>k__BackingField
- ApplicationBase
- get_Keyboard
- get_DiscretionaryAcl
- BinaryReader
- PtrToStructure
- GetPrivateProfileString
- KeyValuePair`2
- get_Password
- FILE_ATTRIBUTRE_NORMAL
- System.ComponentModel.Design
- SHGFI_USEFILEATTRIBUTES
- ICredentialsByHost
- TripleDESCryptoServiceProvider
- BitConverter
- add_DoubleClick
- m_UserObjectProvider
- set_Capacity
- get_OSFullName
- LegalCopyright
- SQLite format 3
- get_BinaryLength
- get_UserName
- remove_Changed
- set_RedirectStandardOutput
- SchemaElementId
- CryptDestroyHash
- FileSystemInfo
- AsyncCallback
- InternalName
- set_WindowStyle
- EncoderParameter
- get_LastUpdated
- 1.85 (Hash, version 2, native byte-order)
- GetEnvironmentVariable
- GetWindowText
- MapVirtualKey
- CreateDirectory
- SetWindowsHookEx
- CryptAcquireContext
- GetForegroundWindow
- CallNextHookEx
- VirtualProtect
- SetKernelObjectSecurity
- CryptHashData
- SetWindowsHookExA
- GetDiskFreeSpaceExA
- GetKernelObjectSecurity
- UnhookWindowsHookEx
- GetKeyboardState
- GetKeyboardLayout
- GetModuleFileNameA
- CryptReleaseContext

- **Module 5 other strings**

- ADDURL_ADDTOCACHE
- $AFA0DC11-C313-11D0-831A-00C04FD5AE38
- DebuggableAttribute
- IUrlHistoryStg2
- milliseconds
- System.Security.AccessControl
- dwSecretInfoSize
- GetFileNameWithoutExtension
- Dictionary`2
- $83018595-3f8a-4e71-94b2-8e41a61ed763
- ThreadStaticAttribute
- ManagementObjectEnumerator
- GetUrlHistory
- System.Diagnostics
- System.Collections.Generic
- FileNotFoundException
- pcchCanonicalized
- URL_PLUGGABLE_PROTOCOL
- RegQueryValueEx
- fWriteHistory
- EditorBrowsableAttribute
- ManagementObjectCollection
- m_ThreadStaticValue
- AssemblyTrademarkAttribute
- AssemblyCopyrightAttribute
- System.ComponentModel
- System.Collections
- ReleaseHandle
- InitializeArray
- GetExtension
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- CreateProjectError
- AddUrlAndNotify
- PropertyDataCollection
- MyGroupCollectionAttribute
- ExplorerUrlHistory
- IEnumerable`1
- System.Globalization
- STAThreadAttribute
- ArgumentOutOfRangeException
- MouseButtons
- DefaultMemberAttribute
- FileAttribute
- FileDescription
- ParameterizedThreadStart
- TargetMethod
- System.Management
- ProtectedData
- 7;7<7>=?=@=BACBDB
- ProcessWindowStyle
- CreateEncryptor
- DefaultValueAttribute
- PropertyData

- WindowsBuiltInRole
- LastModified
- CompilerGeneratedAttribute
- ILD_TRANSPARENT
- WindowsIdentity
- MulticastDelegate
- AddHistoryEntry
- ClipboardProxy
- GroupCollection
- DelegateAsyncState
- <Password>k__BackingField
- AssemblyProductAttribute
- Collection`1
- My.Application
- RuntimeCompatibilityAttribute
- CreateSubKey
- ADDURL_ADDTOHISTORYANDCACHE
- SystemInformation
- LegalTrademarks
- CopyFromScreen
- Microsoft.VisualBasic
- AppendAllText
- HideModuleNameAttribute
- sql_statement
- dwPropertiesCount
- CreateDecryptor
- TargetObject
- WH_KEYBOARD_LL
- UrlCanonicalize
- RegOpenKeyEx
- SuppressIldasmAttribute
- pceltFetched
- advapi32.dll
- WriteAllText
- pResourceElement
- CompilationRelaxationsAttribute
- StringComparison
- IEnumSTATURL
- WithEventsValue
- ConcatenateObject
- pPropertyElements
- FileSystemProxy
- dwSecretSize
- ClearHistory
- CreateObject
- GetBinaryForm
- GetEnumerator
- AmountOfMemory
- GetTypeFromHandle
- StandardModuleAttribute
- IndexOutOfRangeException
- AssemblyConfigurationAttribute
- RecoveredBrowserAccount
- GetCharCount
- Microsoft.Win32
- Create__Instance__
- System.Security.Cryptography

- ProcessModule
- GetModuleFileNameEx
- AssemblyTitleAttribute
- FrameworkVersion
- HelpKeywordAttribute
- ICryptoTransform
- DebuggerBrowsableAttribute
- MatchCollection
- DebuggerHiddenAttribute
- SetProjectError
- ClearProjectError
- AssemblyFileVersionAttribute
- DeleteHistoryEntry
- pszCanonicalized
- LateSetComplex
- RegistryProxy
- AttachmentCollection
- ReliabilityContractAttribute
- GetPropertyValue
- GenericSecurityDescriptor
- <Url>k__BackingField
- GetSavedPasswords
- pIdentityElement
- VaultEnumerateVaults
- ProductVersion
- DebuggerBrowsableState
- GetLastWin32Error
- GetHINSTANCE
- GuidAttribute
- KeyCollection
- OperatingSystem
- ReleaseComObject
- AssemblyCompanyAttribute
- InterfaceTypeAttribute
- Win32Exception
- ProtectedArray
- CreateHandle
- DeleteSubKey
- ftLastVisited
- AssemblyDescriptionAttribute
- pAuthenticatorElement
- BindToObject
- System.Text.RegularExpressions
- Authenticator
- ftLastUpdated
- System.Security
- RuntimeFieldHandle
- AccessedThroughPropertyAttribute
- IsNullOrEmpty
- System.Collections.ObjectModel
- FlagsAttribute
- STATURLEnumerator
- unsignedShort
- NativeWindow
- URL_DONT_SIMPLIFY
- RuntimeTypeHandle
- System.Reflection

- ManagementBaseObject
- EditorBrowsableState
- kernel32.dll
- IELibrary.dll
- op_Inequality
- SearchOption
- DivideObject
- dwTotalSecrets
- GetObjectValue
- ManagementObject
- ComVisibleAttribute
- CompareMethod
- RegistryValueKind
- SubtractObject
- RawSecurityDescriptor
- CredentialCache
- CannonializeURL
- mebcfxwgjmsq
- LLKHF_INJECTED
- WM_SYSKEYDOWN
- LLKHF_EXTENDED
- LLKHF_ALTDOWN

Module 6 (probably unpacked / injected by the sample)

Module 6 rich signatures

- No rich signatures found

Module 6 strings

Module 6 most interesting strings

- get_PasswordHash
- !This program cannot be run in DOS mode.
- ALG_CLASS_HASH
- set_Password
- STATURL_QUERYFLAGS
- StringFileInfo
- Dispose__Instance__
- GetLastInputInfo
- get_OSVersion
- SortFileTimeAscending
- set_AllowAutoRedirect
- _urlHistoryList
- InternetExplorer
- System.Windows.Forms
- System.Drawing
- STATURL_QUERYFLAG_NOTITLE
- ConditionalCompareObjectLess
- Assembly Version
- astable_name
- VaultCloseVault
- set_Attributes
- CryptCreateHash

- AppendFormat
- szDisplayName
- GetImageEncoders
- LocalMachine
- GetWindowTextLength
- set_Credentials
- IEAutoCompleteSecretHeader
- DoesURLMatchWithHash
- STATURLFLAG_ISCACHED
- DebuggingModes
- STATURLFLAGS
- ALG_SID_SHA1
- ManagementClass
- remove_KeyDown
- EncoderParameters
- SHGFI_EXETYPE
- dwAttributes
- VaultOpenVault
- SHA1CryptoServiceProvider
- System.Collections.IComparer.Compare
- CreateParams
- GetDirectories
- ConditionalCompareObjectEqual
- SetAttributes
- FileVersionInfo
- get_CurrentThread
- set_EnableSsl
- FileTimeToDateTime
- GetExecutingAssembly
- FtpWebRequest
- ResourceManager
- DelegateAsyncResult
- GetInstances
- Microsoft.VisualBasic.Devices
- GetResponseStream
- EscapeDataString
- SHGFI_TYPENAME
- SHGFI_ATTRIBUTES
- ILC_COLORDDB
- URL_ESCAPE_PERCENT
- set_MaximumAutomaticRedirections
- SHGFI_ATTR_SPECIFIED
- ManagementObjectSearcher
- STATURL_QUERYFLAG_TOPLEVEL
- ProcessStartInfo
- GetSubKeyNames
- Auto-vacuum capable database is not supported
- m_ComputerObjectProvider
- get_StartInfo
- $3C374A41-BAE4-11CF-BF7D-00AA006946EE
- System.Net.Mail
- get_Registry
- GetProcesses
- VideocardName
- System.Resources
- My.WebServices
- get_ProductName

- get_EnumUrls
- ImageCodecInfo
- ChangeClipboardChain
- get_BigEndianUnicode
- remove_Click
- get_DriveType
- SortFileTimeAscendingHelper
- ConditionalCompareObjectGreaterEqual
- remove_KeyUp
- get_DefaultCredentials
- get_LastVisited
- lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
- ReadAllBytes
- GetVersionInfo
- pszContainer
- VaultEnumerateItems
- StringBuilder
- get_ComputerName
- DownloadString
- get_IsInvalid
- GetURLHashString
- pszCredentialFriendlyName
- set_CreateNoWindow
- SetClipboardViewer
- m_MyWebServicesObjectProvider
- $3C374A40-BAE4-11CF-BF7D-00AA006946EE
- set_UseShellExecute
- System.Security.Principal
- ElapsedEventHandler
- HashParameters
- get_InvariantCulture
- get_TickCount
- punkISFolder
- get_CapsLock
- set_IsBackground
- get_AltKeyDown
- SHGFI_DISPLAYNAME
- CRYPT_VERIFYCONTEXT
- remove_Wheel
- get_Location
- Not a valid SQLite 3 Database File
- GetRequestStream
- FromBase64String
- NumberStyles
- NewLateBinding
- $3C374A42-BAE4-11CF-BF7D-00AA006946EE
- ComInterfaceType
- get_EndOfStream
- HttpWebRequest
- OperatingSystemName
- URL_UNESCAPE
- DataProtectionScope
- System.Runtime.CompilerServices
- GetCallingAssembly
- MemoryStream
- ComputerInfo

- get_WebServices
- GetProcessesByName
- get_Capacity
- Microsoft.VisualBasic.MyServices
- ServerComputer
- get_FormatID
- remove_DoubleClick
- System.Runtime.InteropServices
- get_ProcessName
- ObjectIdentifier
- GetProcessById
- lpSystemTime
- SHGetFileInfo
- 4System.Web.Services.Protocols.SoapHttpClientProtocol
- UnescapeDataString
- get_StandardOutput
- vaultcli.dll
- SHGFI_SHELLICONSIZE
- EnumProcessModules
- get_ShiftKeyDown
- dwFileAttributes
- GetDirectoryName
- VS_VERSION_INFO
- WindowsPrincipal
- System.Timers
- WrapNonExceptionThrows
- SymmetricAlgorithm
- FileAttributes
- ConditionalCompareObjectNotEqual
- IAsyncResult
- ConditionalCompareObjectGreater
- PtrToStringUni
- IESecretInfoHeader
- get_FileName
- GetSavedCookies
- ToBase64String
- get_Properties
- set_ContentLength
- GetFolderPath
- get_FullyQualifiedName
- <Username>k__BackingField
- set_FileName
- UrlHistoryClass
- HashAlgorithm
- TransformFinalBlock
- set_UseDefaultCredentials
- get_ExecutablePath
- set_KeepAlive
- IUrlHistoryStg
- AceQualifier
- ElapsedEventArgs
- IFormatProvider
- STATURL_QUERYFLAG_NOURL
- ProcessorName
- get_MainModule
- get_CtrlKeyDown
- SHGFI_LARGEICON

- System.Drawing.Imaging
- SHGFI_SMALLICON
- get_Millisecond
- Microsoft.VisualBasic.ApplicationServices
- System.Runtime.InteropServices.ComTypes
- CompareObjectEqual
- URL_ESCAPE_SPACES_ONLY
- get_GetInstance
- set_IsBodyHtml
- DateTimeToFileTime
- URL_ESCAPE_UNSAFE
- +-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
- UTF8Encoding
- LateIndexGet
- Unknow database format
- SecurityIdentifier
- GetCurrentProcess
- ByteArrayToStructure
- CompareObjectGreater
- get_Application
- FileTimeToSystemTime
- Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2
- set_Username
- get_TotalFreeSpace
- DelegateCallback
- ReadAllLines
- get_Clipboard
- STATURL_QUERYFLAG_ISCACHED
- IESecretHeader
- OriginalFilename
- SHGFI_SYSICONINDEX
- CompareString
- get_TotalPhysicalMemory
- System.Threading
- GetValueNames
- get_FileSystem
- GetWindowThreadProcessId
- System.Runtime.ConstrainedExecution
- PROV_RSA_FULL
- Microsoft.VisualBasic.CompilerServices
- System.CodeDom.Compiler
- CompareFileTime
- get_Computer
- STATURLFLAG_ISTOPLEVEL
- SystemTimeToFileTime
- C:\\Users\\Admin\\Desktop\\IELibrary\\IELibrary\\obj\\Debug\\IELibrary.pdb
- CompareObjectNotEqual
- get_IsAttached
- get_UrlString
- CryptGetHashParam
- set_ContentType
- WellKnownSidType
- m_AppObjectProvider
- SpecialFolder
- NetworkCredential
- cbSizeFileInfo
- get_Attachments

- StreamReader
- GCHandleType
- <Browser>k__BackingField
- ApplicationBase
- get_Keyboard
- get_DiscretionaryAcl
- BinaryReader
- PtrToStructure
- GetPrivateProfileString
- KeyValuePair`2
- get_Password
- FILE_ATTRIBUTRE_NORMAL
- System.ComponentModel.Design
- SHGFI_USEFILEATTRIBUTES
- ICredentialsByHost
- TripleDESCryptoServiceProvider
- BitConverter
- add_DoubleClick
- m_UserObjectProvider
- set_Capacity
- get_OSFullName
- LegalCopyright
- SQLite format 3
- get_BinaryLength
- get_UserName
- remove_Changed
- set_RedirectStandardOutput
- SchemaElementId
- CryptDestroyHash
- FileSystemInfo
- AsyncCallback
- InternalName
- set_WindowStyle
- EncoderParameter
- get_LastUpdated
- 1.85 (Hash, version 2, native byte-order)
- GetEnvironmentVariable
- GetWindowText
- MapVirtualKey
- CreateDirectory
- SetWindowsHookEx
- CryptAcquireContext
- GetForegroundWindow
- CallNextHookEx
- VirtualProtect
- SetKernelObjectSecurity
- CryptHashData
- SetWindowsHookExA
- GetDiskFreeSpaceExA
- GetKernelObjectSecurity
- UnhookWindowsHookEx
- GetKeyboardState
- GetKeyboardLayout
- GetModuleFileNameA
- CryptReleaseContext

- **Module 6 other strings**

- ADDURL_ADDTOCACHE
- $AFA0DC11-C313-11D0-831A-00C04FD5AE38
- DebuggableAttribute
- IUrlHistoryStg2
- milliseconds
- System.Security.AccessControl
- dwSecretInfoSize
- GetFileNameWithoutExtension
- Dictionary`2
- $83018595-3f8a-4e71-94b2-8e41a61ed763
- ThreadStaticAttribute
- ManagementObjectEnumerator
- GetUrlHistory
- System.Diagnostics
- System.Collections.Generic
- FileNotFoundException
- pcchCanonicalized
- URL_PLUGGABLE_PROTOCOL
- RegQueryValueEx
- fWriteHistory
- EditorBrowsableAttribute
- ManagementObjectCollection
- m_ThreadStaticValue
- AssemblyTrademarkAttribute
- AssemblyCopyrightAttribute
- System.ComponentModel
- System.Collections
- ReleaseHandle
- InitializeArray
- GetExtension
- CreateInstance
- SuppressUnmanagedCodeSecurityAttribute
- AddrOfPinnedObject
- CreateProjectError
- AddUrlAndNotify
- PropertyDataCollection
- MyGroupCollectionAttribute
- ExplorerUrlHistory
- IEnumerable`1
- System.Globalization
- STAThreadAttribute
- ArgumentOutOfRangeException
- MouseButtons
- DefaultMemberAttribute
- FileAttribute
- FileDescription
- ParameterizedThreadStart
- TargetMethod
- System.Management
- ProtectedData
- 7;7<7>=?=@=BACBDB
- ProcessWindowStyle
- CreateEncryptor
- DefaultValueAttribute

- PropertyData
- WindowsBuiltInRole
- LastModified
- CompilerGeneratedAttribute
- ILD_TRANSPARENT
- WindowsIdentity
- MulticastDelegate
- AddHistoryEntry
- ClipboardProxy
- GroupCollection
- DelegateAsyncState
- <Password>k__BackingField
- AssemblyProductAttribute
- Collection`1
- My.Application
- RuntimeCompatibilityAttribute
- CreateSubKey
- ADDURL_ADDTOHISTORYANDCACHE
- SystemInformation
- LegalTrademarks
- CopyFromScreen
- Microsoft.VisualBasic
- AppendAllText
- HideModuleNameAttribute
- sql_statement
- dwPropertiesCount
- CreateDecryptor
- TargetObject
- WH_KEYBOARD_LL
- UrlCanonicalize
- RegOpenKeyEx
- SuppressIldasmAttribute
- pceltFetched
- advapi32.dll
- WriteAllText
- pResourceElement
- CompilationRelaxationsAttribute
- StringComparison
- IEnumSTATURL
- WithEventsValue
- ConcatenateObject
- pPropertyElements
- FileSystemProxy
- dwSecretSize
- ClearHistory
- CreateObject
- GetBinaryForm
- GetEnumerator
- AmountOfMemory
- GetTypeFromHandle
- StandardModuleAttribute
- IndexOutOfRangeException
- AssemblyConfigurationAttribute
- RecoveredBrowserAccount
- GetCharCount
- Microsoft.Win32
- Create__Instance__

- System.Security.Cryptography
- ProcessModule
- GetModuleFileNameEx
- AssemblyTitleAttribute
- FrameworkVersion
- HelpKeywordAttribute
- ICryptoTransform
- DebuggerBrowsableAttribute
- MatchCollection
- DebuggerHiddenAttribute
- SetProjectError
- ClearProjectError
- AssemblyFileVersionAttribute
- DeleteHistoryEntry
- pszCanonicalized
- LateSetComplex
- RegistryProxy
- AttachmentCollection
- ReliabilityContractAttribute
- GetPropertyValue
- GenericSecurityDescriptor
- <Url>k__BackingField
- GetSavedPasswords
- pIdentityElement
- VaultEnumerateVaults
- ProductVersion
- DebuggerBrowsableState
- GetLastWin32Error
- GetHINSTANCE
- GuidAttribute
- KeyCollection
- OperatingSystem
- ReleaseComObject
- AssemblyCompanyAttribute
- InterfaceTypeAttribute
- Win32Exception
- ProtectedArray
- CreateHandle
- DeleteSubKey
- ftLastVisited
- AssemblyDescriptionAttribute
- pAuthenticatorElement
- BindToObject
- System.Text.RegularExpressions
- Authenticator
- ftLastUpdated
- System.Security
- RuntimeFieldHandle
- AccessedThroughPropertyAttribute
- IsNullOrEmpty
- System.Collections.ObjectModel
- FlagsAttribute
- STATURLEnumerator
- unsignedShort
- NativeWindow
- URL_DONT_SIMPLIFY
- RuntimeTypeHandle

- System.Reflection
- ManagementBaseObject
- EditorBrowsableState
- kernel32.dll
- IELibrary.dll
- op_Inequality
- SearchOption
- DivideObject
- dwTotalSecrets
- GetObjectValue
- ManagementObject
- ComVisibleAttribute
- CompareMethod
- RegistryValueKind
- SubtractObject
- RawSecurityDescriptor
- CredentialCache
- CannonializeURL
- mebcfxwgjmsq
- LLKHF_INJECTED
- WM_SYSKEYDOWN
- LLKHF_EXTENDED
- LLKHF_ALTDOWN

Extra Information Recovered

In this section there is additional information recovered by platform plugins

- **DecryptedStringConsistent**

Mysd7x

8tAOQ.F

wQpX_BNw

WScript.Shell

CreateShortcut

TargetPath

cmd.exe

WorkingDirectory

7X:5Kow

Do>uPEt

hT#ga`nN3a6

<n9XNoF9

Arguments

L@zu5rN)@

/c start

ar1.KHq

OpenSubKey

OpenSubKey

GetValue

\\DefaultIcon\\

GetValue

Not resolved yet.

Ydzv@ebg

UOhoHP7

Software\\Classes

d8t0O/Kl

Software\\Classes\\ms-settings\\shell\\open\\command

C K0JC7pue

7Csa_

DelegateExecute

Software\\Classes

a@ZhKK

DOpvTQ

C:\\Windows\\System32\\computerdefaults.exe

Software\\Classes\\ms-settings\\shell

open\\command

Software\\Classes

oepi`

s_GzfE(

C:\\Windows\\System32\\eventvwr.exe

Software\\Classes\\mscfile\\shell

FBSPpg

RrMGeK6up

dLNPW

webpanel

webpanel

webpanel

Lanx<>m

Johnson

:T3RDl VGa

Miller

)\\5sdvN

michael

sm\\mf

Emily

root\\CIMV2

SELECT * FROM Win32_VideoController

S)fVPup@

SELECT * FROM Win32_Processor

QyT8im

YHqKr3

WtQTk

Screen Capture

Time:

VFO>Q8

UserName:

ComputerName:

CPU:

RAM:

esqLXM4

IP:

thai@dahger-hinnawi.com

Screen

.jpeg

/log.tmp

MM/dd/yyyy HH:mm:ss

0_RRA75LE

06),d

ENwMKw

4e7_a,F

Keystrokes

(nhARVg

Time:

UserName:

ComputerName:

)ZIszv

8Jeze

CPU:

RAM:

IP:

thai@dahger-hinnawi.com

E4GZcKD

Keystrokes_

.html

<html>Time:

UserName:

ComputerName:

Y,YxU\\

CPU:

RAM:

IP:

</html>

Keystrokes_

.html

<html>Time:

vQNEpl)ww

UserName:

ComputerName:

a80 D

PV6).tf5

CPU:

RAM:

IP:

</html>

LFq8>6V<Dt

http://checkip.amazonaws.com/

Iti KT

k(LrRvw

dLxbK6

MSp6o`)

u(xw1

zAa7)

@@h>M

Software\\Microsoft\\Windows\\CurrentVersion\\Run

a<08vAf

EKP4sH

uninstall

uninstall

Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows

KlP22

K1@fP5

HYFNz8

yO>Q:

52eLs

tiAoMVI@H

RILdG

HKEY_CURRENT_USER\\Software\\FTPWare\\COREFTP\\Sites\\

D1Cz V

oPoyKQ

gxtIi:,-5q>

JlwLD

>kMmHYfY

Username:

Password:

Application:

webpanel

d2QV4,6

jPIfTI1

2NQyecQ

,_ND7b3

Time:

UserName:

ComputerName:

B65Ri<

WmfUpBt<

CPU:

RAM:

\\iVr),

IP:

thai@dahger-hinnawi.com

Recovery_

.html

<html>Time:

UserName:

:,gTazhg

ComputerName:

CPU:

RAM:

.4@4Sz

IP:

</html>

webpanel

thai@dahger-hinnawi.com

rWyOi0

OxMrdKp2

smtp.dahger-hinnawi.com

HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System

Y3Ef<(

EnableLUA

REG add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System /v DisableTaskMgr /t REG_DWORD /d 1 /f

HsoTc

NRN7ty

kK.\\p

REG add HKCU\\Software\\Policies\\Microsoft\\Windows\\System /v DisableCMD /t REG_DWORD /d 1 /f

DisableCMD

zHJ6(Da/t

REG add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer /v NoRun /t REG_DWORD /d 1 /f

REG add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer /v NoControlPanel /t REG_DWORD /d 1 /f

HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System

DisableRegistryTools

FNAF(c

TOaE7e2I

REG add HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer /v NoFolderOptions /t REG_DWORD /d 1 /f

Z rtFiC

MSCONFIG.EXE

NyS4LI a

\\tmpG

s8`Q4

Length

length must be > 0

v9(jR

kR_zAJk

j_24q

AosALJ

<span
style=font-style:normal;text-decoration:none;text-transform:none;color:#FF0000;>[clipboard]

vu`uZmo

XsDjMC

T1O.gc

MM/dd/yyyy HH:mm:ss

QA97b

False

RkRtS_8Dx

:wpoV:l

HfprR:

.57UQ

_j12Zw

A)E@TD)

DSuv$xQ1j/o

Qqt>3]0sY\\c

ww8usw93T

PLjo(1

,P8pl

_Sc:U

iQeP@S\\

//OUz

FJAkQ

B&cgojz0;`g)

TY5dcF

Profile

Default

\\Login Data

\\Login Data

Chrome

logins

Opera Software\\Opera Stable\\Login Data

Opera

logins

Yandex\\YandexBrowser\\User Data\\Default\\Login Data

imBBm

>pu2\\H

GetSavedPasswords

pDEl,z

8P`2<Bd

Rzw`WVF7

Windows Web Password Credential

Windows Domain Certificate Credential

Bo2ZGnoTc

Windows Domain Password Credential

ZUmpS.3

Windows Extended Credential

Tq5CBk2

h4)TT

x`TUj

Ok.lFEJ

pIdentityElement

57U)_d@FHm

ykQd.60

IE/Edge

\\Common Files\\Apple\\Apple Application Support\\plutil.exe

9SqbY

,_Sdab

hseIXG

tM8JDL(

m2uHZx

oHJfQp

CoolNovo

(5Vhy

logins

Chromium\\User Data\\Default\\Login Data

SRWare Iron

logins

Torch\\User Data\\Default\\Login Data

_L5nYRn

Torch Browser

wS9rG

logins

UCBrowser\\

6.m)xr9<\\

Login Data

journal

UC Browser

wow_logins

PopPassword

SmtpPassword

Software\\IncrediMail\\Identities\\

\\Accounts_New

PopPassword

SmtpPassword

gr_E5o

EmailAddress

SmtpServer

incredimail

HKEY_CURRENT_USER\\Software\\Qualcomm\\Eudora\\CommandLine

F@<U(>

9m/ VA

Vml)L3

Settings

ReturnAddress

scOkwx

Eudora

thunderbird

thunderbird

Wg,ae8

BlackHawk

BlackHawk

CyberFox

S2KaQJ4lzt

CyberFox

(eHe_Lo

IceCat

J2,q)

IceCat

postbox

postbox

signons3.txt

objects

objects

objects

objects

L1ipEi/Y

objects

r@(y 7c

DecryptTripleDes

mVGFTA\\cXf

All User Profile

7ZPPH

)syiNVp

Key Content * : (?<password>.*)

KrKF)

Vq$M):1X(N@Q

t6KzXhCh

http://DynDns.com

roU>)z

\\Z_ju

<Server>

<Host>

iHrAW0)IR

<Host>

</Host>

<Port>

</Port>

<User>

<User>

</User>

ZpP`tIS

LU_Nh63

</Pass>

<Pass>

KSgw Zr@

<Pass>

</Pass>

FileZilla

SOFTWARE\\\\Martin Prikryl\\\\WinSCP 2\\\\Sessions

hostname

G2:ij c

UserName

Password

PublicKeyFile

PortNumber

_/I>J

fHX5iR

FlashFXP

SystemDrive

\\FTP Navigator\\Ftplist.txt

CHDNQBL

VSmc8

programfiles

\\jDownloader\\config\\database.script

>aNJMN

Programfiles(x86)

HKEY_CURRENT_USER\\Software\\Paltalk\\

7YajT<w

http://Paltalk.com

my<(NJ9

G23WSW

/NrzhAf9

APPDATA

\\.purple\\accounts.xml

qeUivl

H.XPC

:72eiO

cVhSjH 9

yi@ZKQd5

_<(qk7:z/

JbMos(

<Host>

</Host>

<Port>

</Port>

<User>

</User>

<password>

</password>

<name>

7jfctw.

</name>

SmartFTP

APPDATA

\\Ipswitch\\WS_FTP\\Sites\\ws_ftp.ini

APPDATA

Q\\Pw_1m8

\\Ipswitch\\WS_FTP\\Sites\\ws_ftp.ini

xMY_U

WS_FTP

Substring

PwrL1

Length

Length

Substring

Substring

Password decryption failed!

fRFTp7/

/RtGyRK

iBqPB

FIzQH

)k7FLN

uF3keph\\L

FTPCommander

HKEY_LOCAL_MACHINE\\SOFTWARE\\Vitalwerks\\DUC

HKEY_CURRENT_USER\\SOFTWARE\\Vitalwerks\\DUC

UserName

,U98T'o@Xno

Password

UserName

Password

http://no-ip.com

:ZYdW

Input text must be a multiple of 4 characters!

+-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Input contains illegal character '

APPDATA

APPDATA

ZPkRL4

\\Account.CFN

\\Account.CFN

1MDRP

TheBat

Software\\Microsoft\\Office\\15.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676

vFeS\\e>y

GU`q3(memk

Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676

52.hmF,y

Email

4OxTOU)V

IMAP Password

POP3 Password

HTTP Password

SMTP Password

IMAP Password

POP3 Password

HTTP Password

SMTP Password

Email

GetBytes

SMTP Server

SMTP Server

SMTP Server

I8tn/

Outlook

HKEY_CURRENT_USER\\Software\\Aerofox\\FoxmailPreview

R9QH\\y

/Q.uS6X

PCIGUs

ov`eWn

Bc UFhIf/

Z7P BB

w/EYV.u

\\Account.stg

\\fox.temp

\\fox.temp

T:Uqi

\\fox.temp

\\fox.temp

IKUNMu

Length

Close

Dispose

POP3Host

v)wXI

SMTPHost

IncomingServer

Account

MailAddress

Password

POP3Password

:VkCeH

Foxmail

\\Opera Mail\\Opera Mail\\wand.dat

oZKqry

opera:

Opera Mail

zdLPvi

abcdefghijklmno

\\S@IkTa2R

03`cv

APPDATA

\\Pocomail\\accounts.ini

3 Z6r/q

LOQHF

5YqdJw

jn~0mC3_D2.

mmDau

\\fixed_keychain.xml"

F/YDIx

.RQgyxlE

`c/SSid

\\Postbox\\

GJZJ2sSb

\\Thunderbird\\

\\Mozilla\\SeaMonkey\\

3yYwq2`YC

2Y</3zWkO

C_sT

W@uCQ

\\Mozilla\\icecat\\

RUjUWv7

HTzyGk

1LrQel/Z

daPr0

tGuTB

j>>\\<p

profiles.ini

vsJO`

logins.json

5XD9Tn

logins.json

4QxTZBO

P(\\pZ

encryptedPassword

aGEyyt

JFSto:

```
Padding

CreateDecryptor

TransformFinalBlock

aS`jR.y

Value

EndsWith

Substring

Length

Ppzo>

IndexOf

Substring

IndexOf

UNIQUE

table

Software\\DownloadManager\\Passwords\\

AigA\\uT

d2sAFr

EncPassword

Internet Download Manager
```

- **DecryptedStringInconsistent**

```
.lnk

.lnk

.lnk

%8

<y-
```

.lnk

$~Ro`9

Ze'j,; $

2u9lU$

(`15V&

J@YtB'zDB=

H

i+;n_;f}b

i.t!w=6:3l1

5W9&`0

H?Y

')P=i?5

/O+P

J]N$

p?Z!yk_8

[K;}x

:3- ".

d"S2qF,2

3^W.Uv

dNu

sFn"BB

mN9G

aa$[gZo

)lqC^I@>

?Wyt2>,jy

```
q//q#5[N
h(F)Fd&
|4Wsdq
-tlVb m
&explorer; /root,"%CD%
$rV{AUZ
.v-tN8ef=
s,0
ZtlF
*Ci^ap
kVd
#sA
pu
Z]4MT?`NTi=c&sqn;
z"9-t{
c^#Hw6
!0^z?Es]
t#7|>-r
b/tw
M|TnE
y_'gJ$;j[%yg
0
SMTP
]8%#]S
%startupfolder%
Ne`[
```

```
\\%insfolder%\\%insname%

@y2KTH"S1

tpr=F.T

9eLF

#-zm

&*(Dm

NtzT

7-q-

;:2QRNgg{

D~E"=J

.VG=|`

YM3D~

[>k_IS8p_

$h1XAE

tDF1D2?T

{@0@d

!.>^~

Eu<?n$d

#F4Y

BW,pn&c7;)

6NDC-9:Yf

lR5V(&yGrG;

!q@{D

8*7s#`+W

rBb[beY
```

```
*@GBiLzBT6

,cS;d%

0}Nwz/

XV$yP

0/wn

8P;J98C

f&J5d;(~l

]0w

*_u

Il24

-:kh(

?7#jt{m

5K=:Ea

MLZ/*q0|

qi'#z}W

\\5

-et*Yo

$W^l

:tK"\\h7@.}\\D

*ZN^{M^,

5{cfm<

1`>

mp^Oc|

~B[E<'

nn&uxIf;

djWQcg;
```

```
>V7+ai
eNfP+
0!KD
eya#:9K
:;.2vJ|7G
= m{!r>gR6;@
&*gpz;S2!v
?Ep9z
MG2~|-
K}K_ i&
$1oe
scbY"~/8
True
<=+80
<G:-+Y
//rX#xqw>.
Abby
3VP>-\\
bL;m(
John
dNQ;9pWb
95<
'7~.D(n
2@=2YaMrN
M&XI;
```

```
.s4&

QAY,&

`%{!-} KYy.T

j`b

$1q.yM

|DZ[h<]

4]tfe7

ixP;

>51=

W&o;@0

!5$L

#n7db'

pnXf

j"NEoY

"r_<p\'1

*IU$j8

Q5u/> o+

y@yo

lKku#'

85v==4+ W

|ys@t1=DY

N~= F;:L

"K$O7B

W{l

+|F*H

VJ)j$#t9R
```

?8.d+

\\~@Dtz<

%D"S

2.`@E)c?

<hr>

NuZR

L_1q

M-=T)

Sr.(

uHs&X;

^~mMCMt\\+

%^E!KPD&U;

b&fP4Wq;

-I97Z

y}'E4l

|M{

hD}J>X:D3

],`\\a

5=\\="]VXo

/2c

s;}j

s{ZBo}

[*8|}u:`EK

f!FL $\\

4#+bf:

```
FD^]f3

_D<H+

=}.Z4"

:?E;&v;

\\lr;&>e

g5~q,b

Qkp^v

O!7~\\

3Xe!$U

e!FTB.E

3zr|@s)

:)+E1fb

Qqvo}(

dpI=ryf2-

'-TErR^P

XQ;"H/13O

aJ=i

?m.H

}C1L>B[

[\\"S>

858G

:a_u%v t@

eC2#

*eI7b

W'4xZ

{ffAs&S;
```

```
;xtqAUD%0w
m]%z);P:
@+@@7+{Sj!
2RDM
@pP3#-_
<hr>
\\!C"
;J_M)
[U1oe
ryWQj'
~x2)'p%
cur$,vi
8Rt+x
2]YtBH
Aizf
wLvZ
_SMJ
b \\_<Lq-&
H1X]HP.
^fe.T
GJ]z`,J
Rni'W4b|{H
);8A
%c'@<1Y
L $e$;M
```

<1lN*@M

<hr>

Ga/=^{My

-7V[nv%?9

%O`eAv

Y`

Ug

]7E*=8

IgGu2"w

[\\YAs

zp&421

#S= P'

<hr>

|*ND_!+QY

32A!*zp\\A]M

[(

X' 0

)]

fzI,z!X

%}[tL

9^V`&-WX

}b[-o#Qa

H[`3%I`

rOaK3[_^

rMQT}A-U

```
'T,[Y}

aTx$]

pe9P{|dr

2B=

T7-=0R's2

ru>z">F

r#

"Cv-5)

t~|s

e>^\\F=&t;

d?-[n^9;

}|zgCn

(+]g;

+6H<Jz

D%&"

)0]R8

n^i./C)

+Xi+0h

NQ;53A

bRTL\\~H^<x#

3dn

2'-MxqwM

o{BE8hT

q

qjQ<=
```

```
b6!}|

\\eNwG!]3]

_7&uSc;

"WJ&j;`

MD&X;|u

}pOrw

y}%]/

=@qY}

`R~cU[

Load

[+GX'nr

?DTo=kqHS^

%insregname%

aJF,^

type={0}hwid={1}

h?R0U+4lU

X(sZ

P0~

h[bU=5k

}//v-<i

JU>;

SU6_K9?C

S={!p<d

egN$I

t7tJ

~VH
```

```
i+np*l

7yrb%

`\\q@;Oz`

[c\\U3rSRT

&bODw8kK;

C[H

?zF{Lx`

&\\SWfl

'7_S

),)~V

,~sIrOv

+}GD

4[=(k

_A"y@

v4oP

D_)Qh|?

&x0.;}x

Mp<|h

ae!1r^U

m?AV7

0#-/i4eN

X

]j>]$[:`y{a

:(~)_

]B,Z,
```

```
N~5N28

WAG%cy(%

REY*A|j

HNYs

type={0}hwid={1}

zu%~8#Uc

yQ %J)~

3+2JX1

-c7R

GC-K7p5f8

]Z;*"1

5^"$pj1y

9=I;qDKLh

!B-bO-

,[?"+

K0]hB&

BN-$3Y$

X#[a0u55

I#8Q]~

wD

3z+g$

\\;U:C

vX{$w

g}vl

A'#lB

QL'&V9jm;*S
```

```
#AMEiIvB}

O00Z

9G]]

KX^qWz1

%FrEl

b#wn9_\\Z

tLR=U>Q

'+y)!jb

dtk]JP

.*ZP@Rz

c%MwgZ

[{WE+lxo

SMTP

W(/s

URL:

^;

<br>

Y(eP'!52

&0'I

<br>

.N1L^n8,

+`V=nka

<br>

Z

i1u%
```

```
<br>

drJ-_FmtG

<hr>

;$"HNh_

!rMW

client[]={0}

"7Nh\'

7AbmR;DAN

z\\(s/&?

H~gFQua7}

pu|Ti

^,S8V1I

4=!c4zN

yW]j9

A%uC

'RMAi4fVb4]s

Dc&j0;{

<eNl"a_P

fGBO!@j

Dv#pe1b\\.1

R;sCU

Di$O0m

l)BmSM']

Q3Fl>~u@l

4|Q92

PCE/$
```

```
MP#$;c3.V

40<Ay?

Kg7%g3D

Q\\'|iIS

\\0K#

_+kaz1Hw

a5-8

dUez&f;

Rt`4|}x

<hr>

`?r92oN

Pw]

w:B{$CX-ax

;wQh>pn%Vp

SqC

!Xq

([^>~

Ojo

:R"<j

l8p]%

b7[^of.rgP

Lh5$}wk

tu{Xe\\"I[QI

T~UE

<hr>
```

```
0D|h

}^pf/

!3X<,

b='

K}$

6#B)LiUz

"~F\'ek

b2Yy9K:;&

h.FQ

o$4>C

"*\\"6yhssH

` Yo~

]}QNFg

O#p>

Lrkd{d`xR

m1'j*l

{w2)~

*ch|a

/|Vupp!~

B)L

!hfY

##n:

j*^7]7A

ul//[?K#s

]=1+}

@-fx&g;}|5
```

```
gWR

4(BuiC-/

bUlC.#

s/kRG!

;lm)_F dE

ioOI%w,

j_$pI<

ZS.au[rT

-A^:pW

ZuTc$;

&&B;?'t]

zaiB~

{PuOC."

L|KcpZ

6+? se7(

&u;,K/

']+_~

eI )

H(0rI{G|

[~+h9c

pCW=/[jP

EEuT1VN=

So'sd[=e7r>

D#*.UBe6ZHW

#$t2b
```

```
$(xwx`

.tmp

F=-c69so

l1';!O|x

Ejn'2

|#wD

D30

$+hrI5R

?!"}#[+A

\\{2Rs

n2rYD2]

[bLkc

^T>CVB+<v

[/Z:,>K

gjiI

!4op.Co

G`*h

F|L@orH !

E1|>8d

603~niv

\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}

dQz~WW[

tfL{S\\^p19

&

jxefJ"K

<
```

T<:XAFQP^

>

"

>lR|H2`

S`:=c

`D^phG

bN#)`$6-

xju%

%Ms]@

K&Db.Z;")

Zgz5|K

}nC>2)0+

A:b

[

]2fJQx:

f]sxs+V

":n6YQc/@g

2

] (

%(qC>r

Mxs8+

]yi:

RAD#l

^4"3Y"j=

/sJlB6{"G@7

QXY

{BACK}

B<zw

V^Z9c4R-z

2_{oT&HjI9n;_

{ALT+TAB}

3@_}A

,+ja(a`

{ALT+F4}

`;Yww{g

{TAB}

bB

&bc;>

{ESC}

Ha?trPU

yFkm@+w

{Win}

^-u,d^,

!+4<DK.0A

{CAPSLOCK}

#:<H#N

↑

-OlaJH 8jb

aJ6[gC

↓

C:

s6

←

qE}p

7VA

→

)S{+Yp

]dQVL(N

{DEL}

6a`[u58

{END}

Vj*X

Rl4$C

{HOME}

~ILU45

k~mF5 w

{Insert}

v2&=

N`=~H

{NumLock}

tx[q)Z

A+n|?

{PageDown}

'75

{PageUp}

??,Km,

loGB;Q

{ENTER}

P.v_1[mv"

a)

Erd?V

{F1}

EJs`

<gql:x{]

E:11^b

$I+

{F3}

OFY$(9T

*/]L

MZj-3U

{F5}

%S"

Qri}9])

+cJPRft

{F7}

*tgTa9V

"HH)

VYs

{F9}

```
t*Av

$8%EcbY

'wITL}

7ty

>mm+=

)el{d`Z*d

!?~[[

#B<P~/LQ

&j;*

>*jdm

C8r0ql]

XIY|^mF

3FbG&\\Y%ooB

JgY[=0h

T9E|1)

/43;v1b

I!J/N'W

dmnW

hb?]X

q:30!

o*j@

f>A_Qa[t

g>=wI

lw68>+Z

cvnl[;
```

```
-`}"Ihh|

&4a=oKgNKb

LQ3$$Q

b4n='s*

aTflbP-

` ~76\\

}3JUz7

A.*4m;

Y9gKU;

Awm#l.J)

9vQ%@G%enQ=

hi*s

*0{, R

.l8}

+M2

,T c&Gohb;

-

w=j! c

P_aA

sDH=4Bw

a}_^

#v.>

XhtP

NU[0>6i

!A*{U8

M|f{:Ku
```

```
KL;A-7

6eJHW+

8c&'oQ8Nqn&De;

lpvq[i

@b

5q>3^LZy<

"zw.,Ti%v

Y($HD

KNy~8X

n'Um].EM

'-{`mI

Uk+#

.ELq?KN%

'Q0l]2,a

XpFbM;

{!L(yXt

"--cfeON$

G^Sd

7Y$nsh

(#fs

UMv]#2<M

y[?8qk^

$d{z

qo6|-n

|VrWd00
```

3CCD5499-87A8-4B10-A215-608888DD3B55

ULOf8Ne"

newD

[XL3wt7

!gAY{,2

yJ*

tN"

8BKh

.ox(

!bpV>/

O^u>

Cr"wx%W

^n'

$Bxd^\\P

lH@pX!

sg|L-zR

*IWU\\U&

$r\\h

t:8

a#:Lq

}1Iv&mi;

E69D7838-91B5-4FC9-89D5-230D4D4CC2BC

:={{lB^K

4iE! e\\

ON?nCY1BQh

%g|8l

3E0E35BE-1B77-43E7-B873-AED901B6275B

jV"X<{DV

8gYx

8R5.:~

3C886FF3-2669-4AA2-A8FB-3F6759A77548

F!'zY[&g;

Qh^d;C.

C?m*

[Rv{QO

*3Ara^^CCh

TJ<;IT+

A*=:

#zjT387

E6I>

87%' F%=[gzL,

S/ -

I~\\h

4[cz|!&P;

uB

_

E>|SE*"

N<"[[be!

#pq"0u

H Y(vm'q

SM.

iP^I#8r

+M8kh4

,;O`5l

[%$K2

_7G

IG3

sZ[e`FI

J?MhgdY

P5PS

&STYG;^T

n$Dd5

g/?]GH

C@}23Bp

4" If

Wzg:

_6r o1!XN

bni/#f

DF

^EJP"

qjER:B/1.&

+6f?!c'

5#G4$(

5g'pv+^*f

N,USq]8

98?F)-

ERj^3e

-hQWtp7

?HIh

77N&2

hn-B

5g2g

G_

/gT@]8

8!2q-__A

V}awp

]J}d8m>Sx

,Y\\=:

<Z''uB1

LD ^8"

fW

)s-JixT

Kv`{

K-Meleon

DFs%'

K-Meleon

.6n;tO

)Rg]M

Hr}p9f*

*i-u(0BX

JX@,#

'GB@

```
{`%1luLW
}'f[
Data
WVAoL#BD
T_?5~_
Data
"kV-a(Io$
zsqKw{
@"0q%`5o\'F
`X[Ihmn8
j0K]~
]*rv2]l
$;`
{BJD
[BYl,tNA
q)>};TNQK
[oSju
qQ{KY$
#)h6Vg
+>&0
a+9B; l
L!yW
" key=clear
6>K`W0~
zTAo
VmI$L>
```

```
jj2\\

|5l

/e`G7-3R

[=FO}Qq

;up5>5&1

"l5.9

username=

/t2`

password=

4^~>

)G%fv9))x)

* 7C|~2

0// K!rd

5X&^b}b

nO~5[~/Y

#uHcp

hS-dNj

R4/U-^.

_":sf

,2|Q 29$&

.cl!SHq9

EAO7

F/O]5=M

YxCy+

C;=8'6
```

```
<Pass encoding="base64">

*9>ZV@6

k7,^,aC?6

AqY|KOt

<Sc{kvxh5p

}@MA/

21j N^

}>BSLZ

Gc# 0<

+N_c:`,P

S;K'

q>U?I

1[]}3j

[PRIVATE KEY LOCATION: "{0}"]

.~r|},

?Ry7QT|

)R\\l

v~njdo

hr7c'

Qn2c;&y;

f_iQ?Z:E 7

@x.=

\\D

[?.qF

N$! };*

4OUX|9hZEU
```

```
port=
user=
6RY[uCu
pass=
created=
^ydY.I~
F".oQx
tya=
"j Xo|WO
366n7?(
'wGf) oT
U
"k!@Qr?{
(I|#{!A
=5 %@~zw
sv8H=
KR*gqr
}LH]Yk.z
9_e&
-Kft;[c
hS+*g?L?b
hQ_*<f_
ZO{~S"6\\M
c],X
.e[6ez)s
```

```
kQ)wo*JP>*
L*%[QH
K WC$4D
!5dp.:U3n
eru|/J
O5p9iBb-p
3W$>y,^
;wk!o1
n"|
DPO{%MH*6q
v
5uU!
>2&
XAbg
"(R\\sJFSB
tN2G"\\!
T\\Q
h>?1B
=V-{&F;
QU_j
}Z!glw
\\r'Uylbq;
YC,
[~7.K*
rED`
~{-/O=
```

)(-8#_

W0vljfR|fU

d3/*(R#X9Q;a?

'8.]3W0m

=a%Wo

CYij

~0n:r

(Pef

p_~Q]@q

_?~fP0V}

3Z

3C?(mR9

(3C|Kw/y

G&~HX~*

EpKi

#rIA@V

Id%~>7$

E)wH

lXR,

st#

gDC:

%V^ge{P^

z&Mf;

mxK/}l$

9r6-7I>]

{W^A

Host

d+<eZ.BA|

PWD=

e"">lD&

PWD=

O#aTs7

~s:;

.UG"W7

n}%5m6n

#'t

}k:}K5V9q

K *$

L$)g+*

iQ9d

V;a

k*dO5&H;

Q?y67`L

{NzFh+%.

27Z|^}u

;Server=

;Port=

"OI|dU7)u

;Port=

'Rq_UizK_

;Password=

```
gjLH'7

;User=

H|2k%@

;Anonymous=

;Password=

":gA\\S

;User=

Name=

nZAZf&"{

;Server=

^$u?K

t9$lR>W

4`sa

0) @

"xppel4F

-<[eALGa

)m)^G/g%NG

UV$*b'%\\?B

#UFqZ S

h{'9KOI

!B.0?G

A

`;|m

/{^}t1Rx

>)_DD$R?
```

NO-IP

!QM

.?%"

[b<Yw\\#;b

#C'[;l

>W]RZ|Q

cXBY3~

RAeZ@2O>`#

;6

\\The Bat!

~98P|yh

\\The Bat!

X"fi

$=?bea

Hb5i

p&>#zz

+Mhmq

mCWp

Bh6p

X'sR7]P#

Lu]k4B.

GuzS

~{ \\TC

+$ wa:f6k

^`OEoea

#&ea;$[6u

```
b`fy*]$

f{yZ,Sd

CD\\)0}*^

7o+Kd

9U2G

X,%W'(]@

K=

!T-Rr.

%X]W sW

m1'w4^

pu'(Oj

e5-g.gZE=

<U;R@

+}+6dk]

gRzfS|

Not found!

P}x0kM

*ERpt_

S*+k!i

*!hI>

=g

U3Xv

M>*Q:

ItN q=

"`\'^8
```

```
*#qV1

we{@'ep

=j0

v<bW{

%FA-#

'K%c

T}B9B\\\\

I8/t

Uop1B{

*cT@nDDri

^PU_pL+?$

EW<lQd$

sSuM@-

&gxkQ;

#s,n

^_Z }SLt

PleG&B;

;=L

3rd

dWR+0>

7]t

hF

Read

}X-RT;5}

$d&

6oz~|
```

;2z]Y

x98T!K

3y')A1l

r`Bl=8

V/-sXq

^sf3HpJ

!empty!

@{@ ~0

No Data!

LIH?jE_g&

q!+$n

{W?d(t

md%}avF

LZ*uN

^@VNd

$I:78`

`H[

mE+

;:2

06Z

x{!%)

8?h

I(Fx

fr:uz{Ca

OeZ.2&

jP_"h/(

)W2&S;%

u';Cr

J^n^

[*22vL

E$r2g

5Hl:

|(jO

vs}f

NHe(B]R

N

F}PUNo

&3P$O

+,l/AUQ

?5N<

7b;t|ye3

$(b>

)1:7

&[>75

^mi~b

}>&.G

q0HzW|

v:P"

nv,ve}

"MGsu&

2.X^ne

```
\\U#$l+nT

p{pqbGc

,r:%E

?i<"

JTjs#v~<5

D'Z

i8ANid+B

<G_W?0l

}v)7>tB

9<LE

<0} k

5-UX

\\K-Meleon\\

0,Lq=WkL

c7q-M(+F

1@li=a?E

[S-1no;FWHX

l(je

sr|e{~P

Fil"2\\X=%STPrR

7yY

c~U[S^L

~vIua

bbl[O|n

`a%ys{dr
```

lfYA

0UZi

b}f$

q+Z

W5Pt~85

B8}So

B*lV^S'sa]J

F7s

q4& r.Z/^

!

[z'

0l7

A~_(

5P@W{

+-q%XO

">WURbS

g9L*{

W`5Pr|}B-z

6Jr.I~mT.

'

D`Hq

Q>e3~8v

\\"(hostname|encryptedPassword|encryptedUsername)":"(.*?)"

ZFm(

Vb~rC|9

E_X+[

[5{w'E Y

j6%VF

[^\\u0020-\\u007F]

~g-6 Vya

f>?8Z8+Q

C _*B

81'tYH,~4I

[js!X

2ps@&"3

kP`J

Q{E -a

yQ#3ak!diT

_!o@T0

s^~t'Fw

]1F"0

[^\\u0020-\\u007F]

.CGS!

75XiRG~I>6

DP~{.]

@`'

JZcTqC%Z

9]E@;2[`

|N"\'EI

en7]Fs

Mode

*%f&fkSa;

0D!D

t0=8k

_Hb{uEG

q;>w

rCiU}A lt

{xh2}

'4Bay

d\\d{oJR

vqQu

(VH$/t4

/w+grg

Type

#nr

n[*pZIA+Z

]EfK![U

C?'L

I!&D;%

&st5;)Gl

Eh-%Bs \\r

3@Yf=t=

>W[0_H}

User

Dd-*U7

R

O8Y!_e7M

```
h1m|

qgf/

qb=k;'g@

UM7>![M

DS70|

$g2Y>Q`m

PXDXm##

YIr*j%

-L<8B-h
```

Configs Recovered

In this section there are malware configs recovered by platform plugins

- **CnC**

  smtp.dahger-hinnawi.com

  thai@dahger-hinnawi.com