Sample: 3f77b24c569600e73f9c112b9e7be43f

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: **#BANKER #JIMMYNUKEBOT** (based on p3pperp0tts rules)

Analysis date: 2019-01-02 11:36:04 (p3pperp0tts platform's analysis date)

Exe timestamp: 2017-11-30 16:52:14 (timestamp of the original sample)

Unpacked mods max timestamp: 2018-08-27 19:54:50 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2018-12-30 05:40:32 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: 3f77b24c569600e73f9c112b9e7be43f

AV detections

- Microsoft: Trojan:Win32/Occamy.C
- Kaspersky: Trojan.Win32.Chapak.arjw
- Symantec: Packed.Generic.525
- Malwarebytes: Trojan.MalPack

Source

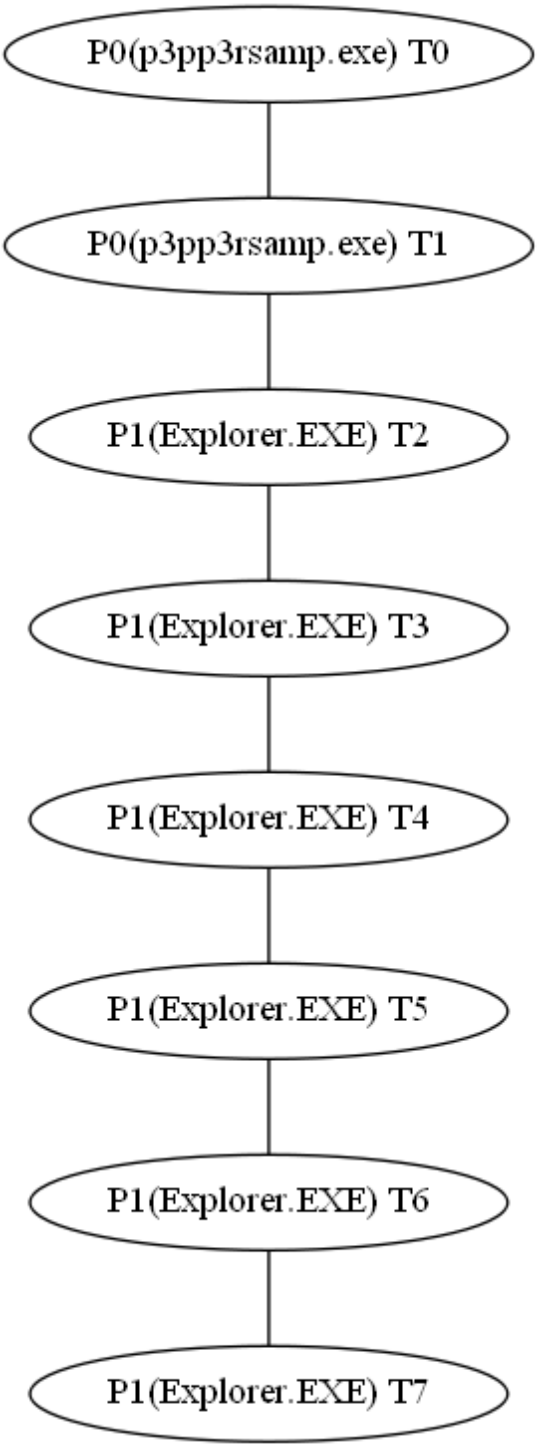
-

Virustotal

- https://virustotal.com/es/file/13000a0da5fc8da437e70649fe39802cce240bf1529b6ab7ce3c273a592eb615/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:\\Windows\\explorer.exe PID: P1, Command line: "C:\\Windows\\explorer.exe")
- RegSetValue (HKCU\\Software\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt\\D Type: REG_BINARY, Length: 56, Data: 49 00 56 00 2B 00 75 00 36 00 38 00 47 00 48 00)
- RegSetValue (HKLM\\System\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp\\MaxConnectionTime Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\System\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp\\MaxDisconnectionTime Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\System\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp\\MaxIdleTime Type: REG_DWORD, Length: 4, Data: 0)
- Thread Create (Thread ID: T1)
- Thread Create (Thread ID: TUNKALIAS)
- Thread Create (Thread ID: T3)
- Thread Create (Thread ID: T4)
- Thread Create (Thread ID: T5)
- Thread Create (Thread ID: T6)
- 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.

- !This program cannot be run in DOS mode.
- iMb}Agb:nBK<Fs3pP]D;igf:oR\\}PML:PRDfidPfi`_
- reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /ve /t REG_SZ /d "%ls" /f
- %ls\\nss3.dll
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
- Content-Type: application/x-www-form-urlencoded
- --disable-http2 --use-spdy=off --disable-quic
- user_pref("network.http.spdy.enabled.http2", false);
- user_pref("network.http.spdy.enabled", false);
- Content-Type: multipart/form-data; boundary=--------------------------%d
- Rundll32.exe SHELL32.DLL,ShellExec_RunDLL "cmd.exe" "/c %ls"
- Rundll32.exe SHELL32.DLL,ShellExec_RunDLL "%ls"
- GetCurrentThread
- kBX:iNe|F9DfS9\\skRX?nRHaSRXfi8\\sng\\sDI?`h8:|nMLpk9G
- InitializeAcl
- TerminateProcess
- CryptBinaryToStringW
- Module32NextW
- explorer.exe
- CryptBinaryToStringA
- CreateFileMappingW
- Process32FirstW
- GetProcAddress
- MultiByteToWideChar
- SetSecurityInfo
- GetCurrentProcessId
- Module32FirstW
- GetCurrentProcess
- Process32NextW
- D:(D;OICI;GA;;;BG)(D;OICI;GA;;;AN)(A;OICI;GA;;;AU)(A;OICI;GA;;;BA)
- GetUserGeoID
- FlushFileBuffers
- GetSystemInfo
- OutputDebugStringW
- u?8X*u:jRXjCf
- Software\\Microsoft\\Office\\Outlook\\OMI Account Manager\\Accounts
- Windows Live Mail IMAP
- InternetCrackUrlA
- Outlook 2003/2010 HTTP
- Referer: %ls
- InterlockedExchange
- HTTP Password
- ObtainUserAgentString
- profiles.ini
- GetWindowThreadProcessId
- ns1.rodgerbruce.com
- Content-Disposition: form-data;name="fname"
- %sPOST data:
- Connection: close
- IMAP User Name
- SuspendThread

- InterlockedCompareExchange
- SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp
- Mozilla\\Firefox
- SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- HttpOpenRequestW
- Rundll32.exe zipfldr.dll,RouteTheCall "%ls"
- <POP3_User_Name
- philipostendorf.de
- inject_after_keyword
- InternetConnectW
- Software\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt\\
- Pgdiplus.dll
- CMD notepad test
- c2hpdHmjcmF6eUBleHBsb2l0Lmlt
- ns1.moderntld.com
- Software\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt\\Dns\\
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)
- Outlook Express POP3
- HTTPMail Server
- HttpSendRequestW
- SELECT displayName FROM AntiVirusProduct
- Thunderbird.Url.news\\DefaultIcon
- RtlInitAnsiString
- GetPrivateProfileIntW
- RtlCreateUserThread
- POP3 User Name
- Software\\Microsoft\\Windows Live Mail
- Windows Live Mail POP3
- newton.bambusoft.mx
- Software\\Microsoft\\Windows Mail
- Accept-Encoding
- ewininet.dll
- a.dnspod.com
- "encryptedUsername":"
- Content-Length: %i
- Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676
- cmd&%ls&%ls&%i&%i&%i&%i&%i&%ls&%s&%ls&%ls
- CreateRemoteThread
- Outlook Express HTTP
- GetExitCodeProcess
- Content-Length: %d
- GET %s HTTP/1.0
- Content-Disposition: form-data; name="data"; filename="%ls"
- Content-Length
- MaxConnectionTime
- GetCurrentThreadId
- <IMAP_Server
- ns1.opennameserver.org
- LdrGetProcedureAddress
- NtGetContextThread
- <POP3_Server
- <IMAP_User_Name
- SetUnhandledExceptionFilter
- GetExitCodeThread
- secondary.server.edv-froehlich.de
- HTTPMail Password2

- GdipGetImageEncoders
- CreateEventW
- GetPrivateProfileStringW
- HTTP authentication (encoded): %s
- Rundll32.exe url.dll,FileProtocolHandler "%ls"
- freya.stelas.de
- Microsoft Unified Security Protocol Provider
- \\\\.\\pipe\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt
- "hostname":"
- POST %s HTTP/1.0
- Software\\Microsoft\\Internet Account Manager\\Accounts
- HTTP Server URL
- PK11SDR_Decrypt
- NtSetContextThread
- EnumProcesses
- PR_OpenTCPSocket
- Content-Type
- OutputDebugStringA
- RtlDecompressBuffer
- inject_setting
- inject_before_keyword
- ns.dotbit.me
- ResumeThread
- IsWow64Process
- ConnectNamedPipe
- CreateThread
- GetLogicalDrives
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
- Resource: (%s), Service: (%s), User: (%s), Password: (%s)
- Outlook Express IMAP
- MaxDisconnectionTime
- HTTPMail User Name
- b.dnspod.com
- Cookie: %s=%s
- egdiplus.dll
- SetErrorMode
- HTTP authentication: username="%s", password="%s"
- GetSystemTime
- DisconnectNamedPipe
- sourpuss.net
- c.dnspod.com
- Content-Type: application/octet-stream
- %s\\Thunderbird\\profiles.ini
- ns14.ns.ph2network.org
- Cookie: %s=%s;uid=%ls
- GetOverlappedResult
- Transfer-Encoding
- Thread32First
- RtlCompressBuffer
- CoCreateInstance
- MapViewOfFile
- WideCharToMultiByte
- CheckRemoteDebuggerPresent
- OpenProcessToken
- GetTickCount
- IsDebuggerPresent

- CreateToolhelp32Snapshot
- VirtualAllocEx
- ReadProcessMemory
- InternetReadFile
- InternetWriteFile
- VirtualProtectEx
- InternetCloseHandle
- SetThreadContext
- InternetCloseHandle gle: 0x%X, %u
- InternetQueryDataAvailable
- NtWriteVirtualMemory
- FlushInstructionCache
- WriteProcessMemory
- GetThreadContext
- Thread32Next
- CryptStringToBinaryW
- CryptStringToBinaryA
- CryptUnprotectData
- VirtualAlloc
- SetFileAttributesW
- QueryDosDeviceW
- RegSetValueExA
- VirtualQuery
- UnmapViewOfFile
- RegSetValueExW
- GetClassNameW
- RegDeleteValueW
- GetModuleHandleW
- FindFirstFileW
- GetModuleFileNameExW
- GetComputerNameExW
- GetSidSubAuthority
- GetTempPathW
- FindNextFileW
- RegCreateKeyExW
- GetUserNameW
- GetTempFileNameW
- GetLocaleInfoW
- RegOpenKeyExA
- RegOpenKeyExW
- EnableWindow
- GetWindowsDirectoryW
- GetSystemMetrics
- GetSidSubAuthorityCount
- RegQueryValueExW
- RegCreateKeyExA
- WaitForSingleObject
- GetModuleFileNameW
- RegQueryValueExA
- GetShortPathNameW
- GetLastError
- GetTokenInformation
- CreateProcessW
- RtlSetLastWin32Error
- NtFreeVirtualMemory
- RegDeleteKeyW
- CreateNamedPipeW

- LeaveCriticalSection
- GetModuleInformation
- WaitForMultipleObjects
- RtlCreateUnicodeStringFromAsciiz
- GetProcessHeap
- CreateDirectoryW
- NtAllocateVirtualMemory
- SetThreadExecutionState
- VirtualProtect
- GetVersionExW
- LoadLibraryW
- EnterCriticalSection
- InterlockedIncrement
- CreateMutexW
- VirtualQueryEx
- NtProtectVirtualMemory
- NtQueryVirtualMemory
- RtlGetCompressionWorkSpaceSize
- SetLastError
- GetEnvironmentVariableW
- InterlockedDecrement
- InitializeCriticalSection
- RtlNtStatusToDosError
- NtReadVirtualMemory
- GetFileAttributesW
- CallNamedPipeW
- GetDriveTypeW

Hosts

- 107.161.16.236:domain
- 151.120.36.59.broad.dg.gd.dynamic.163data.com.cn:domain
- 180.163.8.114:domain
- 50.3.82.162:domain
- freya.stelas.de:domain
- google-public-dns-a.google.com:domain
- mx5.sourpuss.net:domain
- newton.bambusoft.mx:domain
- ns14.ns.ph2network.org:domain
- philipostendorf.de:domain
- reverse.gdsz.cncnet.net:domain
- smtp.sourpuss.net:domain
- static.38.133.76.144.clients.your-server.de:domain

Dns queries

- securityupdateserver4.com ---> no answers
- sourpuss.net ---> 63.231.92.27
- 8.8.8.8.in-addr.arpa ---> no answers
- 27.92.231.63.in-addr.arpa ---> no answers
- ns1.opennameserver.org ---> 144.76.133.38
- dns.msftncsi.com ---> 131.107.255.255
- 38.133.76.144.in-addr.arpa ---> no answers
- freya.stelas.de ---> 5.135.183.146

Network traffic

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

- No network traffic captured

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.

- !This program cannot be run in DOS mode.
- iMb}Agb:nBK<Fs3pP]D;igf:oR\\}PML:PRDfidPfi`_
- reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /ve /t REG_SZ /d "%ls" /f
- %ls\\nss3.dll
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
- Content-Type: application/x-www-form-urlencoded
- --disable-http2 --use-spdy=off --disable-quic
- user_pref("network.http.spdy.enabled.http2", false);
- user_pref("network.http.spdy.enabled", false);
- Content-Type: multipart/form-data; boundary=--------------------------%d
- Rundll32.exe SHELL32.DLL,ShellExec_RunDLL "cmd.exe" "/c %ls"
- Rundll32.exe SHELL32.DLL,ShellExec_RunDLL "%ls"
- GetCurrentThread
- kBX:iNe|F9DfS9\\skRX?nRHaSRXfi8\\sng\\sDI?`h8:|nMLpk9G
- InitializeAcl
- TerminateProcess
- CryptBinaryToStringW
- Module32NextW
- explorer.exe
- CryptBinaryToStringA
- CreateFileMappingW
- Process32FirstW
- GetProcAddress
- MultiByteToWideChar
- SetSecurityInfo
- GetCurrentProcessId
- Module32FirstW
- GetCurrentProcess
- Process32NextW
- D:(D;OICI;GA;;;BG)(D;OICI;GA;;;AN)(A;OICI;GA;;;AU)(A;OICI;GA;;;BA)
- GetUserGeoID
- FlushFileBuffers
- GetSystemInfo
- OutputDebugStringW
- u?8X*u:jRXjCf
- Software\\Microsoft\\Office\\Outlook\\OMI Account Manager\\Accounts
- Windows Live Mail IMAP
- InternetCrackUrlA
- Outlook 2003/2010 HTTP
- Referer: %ls
- InterlockedExchange
- HTTP Password
- ObtainUserAgentString
- profiles.ini
- GetWindowThreadProcessId
- ns1.rodgerbruce.com
- Content-Disposition: form-data;name="fname"
- %sPOST data:
- Connection: close
- IMAP User Name
- SuspendThread

- InterlockedCompareExchange
- SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp
- Mozilla\\Firefox
- SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- HttpOpenRequestW
- Rundll32.exe zipfldr.dll,RouteTheCall "%ls"
- <POP3_User_Name
- philipostendorf.de
- inject_after_keyword
- InternetConnectW
- Software\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt\\
- Pgdiplus.dll
- CMD notepad test
- c2hpdHmjcmF6eUBleHBsb2l0Lmlt
- ns1.moderntld.com
- Software\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt\\Dns\\
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)
- Outlook Express POP3
- HTTPMail Server
- HttpSendRequestW
- SELECT displayName FROM AntiVirusProduct
- Thunderbird.Url.news\\DefaultIcon
- RtlInitAnsiString
- GetPrivateProfileIntW
- RtlCreateUserThread
- POP3 User Name
- Software\\Microsoft\\Windows Live Mail
- Windows Live Mail POP3
- newton.bambusoft.mx
- Software\\Microsoft\\Windows Mail
- Accept-Encoding
- ewininet.dll
- a.dnspod.com
- "encryptedUsername":"
- Content-Length: %i
- Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676
- cmd&%ls&%ls&%i&%i&%i&%i&%i&%ls&%s&%ls&%ls
- CreateRemoteThread
- Outlook Express HTTP
- GetExitCodeProcess
- Content-Length: %d
- GET %s HTTP/1.0
- Content-Disposition: form-data; name="data"; filename="%ls"
- Content-Length
- MaxConnectionTime
- GetCurrentThreadId
- <IMAP_Server
- ns1.opennameserver.org
- LdrGetProcedureAddress
- NtGetContextThread
- <POP3_Server
- <IMAP_User_Name
- SetUnhandledExceptionFilter
- GetExitCodeThread
- secondary.server.edv-froehlich.de
- HTTPMail Password2

- GdipGetImageEncoders
- CreateEventW
- GetPrivateProfileStringW
- HTTP authentication (encoded): %s
- Rundll32.exe url.dll,FileProtocolHandler "%ls"
- freya.stelas.de
- Microsoft Unified Security Protocol Provider
- \\\\.\\pipe\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt
- "hostname":"
- POST %s HTTP/1.0
- Software\\Microsoft\\Internet Account Manager\\Accounts
- HTTP Server URL
- PK11SDR_Decrypt
- NtSetContextThread
- EnumProcesses
- PR_OpenTCPSocket
- Content-Type
- OutputDebugStringA
- RtlDecompressBuffer
- inject_setting
- inject_before_keyword
- ns.dotbit.me
- ResumeThread
- IsWow64Process
- ConnectNamedPipe
- CreateThread
- GetLogicalDrives
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
- Resource: (%s), Service: (%s), User: (%s), Password: (%s)
- Outlook Express IMAP
- MaxDisconnectionTime
- HTTPMail User Name
- b.dnspod.com
- Cookie: %s=%s
- egdiplus.dll
- SetErrorMode
- HTTP authentication: username="%s", password="%s"
- GetSystemTime
- DisconnectNamedPipe
- sourpuss.net
- c.dnspod.com
- Content-Type: application/octet-stream
- %s\\Thunderbird\\profiles.ini
- ns14.ns.ph2network.org
- Cookie: %s=%s;uid=%ls
- GetOverlappedResult
- Transfer-Encoding
- Thread32First
- RtlCompressBuffer
- CoCreateInstance
- MapViewOfFile
- WideCharToMultiByte
- CheckRemoteDebuggerPresent
- OpenProcessToken
- GetTickCount
- IsDebuggerPresent

- CreateToolhelp32Snapshot
- VirtualAllocEx
- ReadProcessMemory
- InternetReadFile
- InternetWriteFile
- VirtualProtectEx
- InternetCloseHandle
- SetThreadContext
- InternetCloseHandle gle: 0x%X, %u
- InternetQueryDataAvailable
- NtWriteVirtualMemory
- FlushInstructionCache
- WriteProcessMemory
- GetThreadContext
- Thread32Next
- CryptStringToBinaryW
- CryptStringToBinaryA
- CryptUnprotectData
- VirtualAlloc
- SetFileAttributesW
- QueryDosDeviceW
- RegSetValueExA
- VirtualQuery
- UnmapViewOfFile
- RegSetValueExW
- GetClassNameW
- RegDeleteValueW
- GetModuleHandleW
- FindFirstFileW
- GetModuleFileNameExW
- GetComputerNameExW
- GetSidSubAuthority
- GetTempPathW
- FindNextFileW
- RegCreateKeyExW
- GetUserNameW
- GetTempFileNameW
- GetLocaleInfoW
- RegOpenKeyExA
- RegOpenKeyExW
- EnableWindow
- GetWindowsDirectoryW
- GetSystemMetrics
- GetSidSubAuthorityCount
- RegQueryValueExW
- RegCreateKeyExA
- WaitForSingleObject
- GetModuleFileNameW
- RegQueryValueExA
- GetShortPathNameW
- GetLastError
- GetTokenInformation
- %08X-%04X-%04X-%04X-%08X%04X
- PathFindExtensionW
- advapi32.dll
- PathFindFileNameW
- CoUninitialize

- CoInitializeEx
- SHGetSpecialFolderPathW
- !o~4!~~5!(~4!e
- CoInitialize
- ShellExecuteExW
- Zr~~4!~~4!~~4!
- {%08X-%04X-%04X-%04X-%08X%04X}
- s2A3R{[n=?O}^y9~>B8@eXo<3Hak8]Yis2A3R{[n=?O}^y9~>B8@eXo<3Hak8]Yi
- kernel32.dll
- S83~F9Xbi8~pFdHeiK77
- CreateProcessW
- RtlSetLastWin32Error
- NtFreeVirtualMemory
- RegDeleteKeyW
- CreateNamedPipeW
- LeaveCriticalSection
- GetModuleInformation
- WaitForMultipleObjects
- RtlCreateUnicodeStringFromAsciiz
- GetProcessHeap
- CreateDirectoryW
- NtAllocateVirtualMemory
- SetThreadExecutionState
- VirtualProtect
- GetVersionExW
- LoadLibraryW
- EnterCriticalSection
- InterlockedIncrement
- CreateMutexW
- VirtualQueryEx
- NtProtectVirtualMemory
- NtQueryVirtualMemory
- RtlGetCompressionWorkSpaceSize
- SetLastError
- GetEnvironmentVariableW
- InterlockedDecrement
- InitializeCriticalSection
- RtlNtStatusToDosError
- NtReadVirtualMemory
- GetFileAttributesW
- CallNamedPipeW
- GetDriveTypeW
- Outlook 2003/2010 POP3
- CreateCompatibleBitmap
- 4.43494@4U4Z4`4g4
- PathFileExistsW
- MH_ERROR_UNSUPPORTED_FUNCTION
- 5&5+50555?5D5I5N5X5]5b5g5
- SelectObject
- Outlook 2003/2010 IMAP
- 0%0,01070C0J0X0^0q0
- IMAP Password2
- 7"8W8]8i8r8x8
- PR_GetNameForIdentity
- <POP3_Password2
- IMAP Password
- 8 848>8Q8e8o8

- SECITEM_ZfreeItem
- MH_ERROR_NOT_INITIALIZED
- MH_ERROR_FUNCTION_NOT_FOUND
- MH_ERROR_ALREADY_INITIALIZED
- GdipCreateBitmapFromHBITMAP
- PathCombineW
- POP3 Password2
- 3'3/3`3f3r3x3
- application/x-www-form-urlencoded
- GdipGetImageEncodersSize
- GdiplusShutdown
- Authorization
- 5 5)505B5I5R5X5a5i5q5
- POP3 Password
- S83~F9Xbi8~pFdHeiK77mozglue.dll
- 7*8?8^8u839n9
- Proxy-Connection
- MH_ERROR_ALREADY_CREATED
- CreateCompatibleDC
- DeleteObject
- If-Modified-Since
- MH_ERROR_MEMORY_ALLOC
- 9(9<9K9s9,:M:
- 5Z6`6e6j6o6t6
- 5O6X6_6e6n6u6}6
- MH_ERROR_MODULE_NOT_FOUND
- SHGetFolderPathW
- MH_ERROR_MEMORY_PROTECT
- 3Q4W4\\4b4h4q4
- PStoreCreateInstance
- GdiplusStartup
- PathAddBackslashW
- %s\\%s\\account*.oeaccount
- <IMAP_Password2
- MH_ERROR_NOT_EXECUTABLE
- GdipSaveImageToFile
- %s\\Thunderbird\\%s\\logins.json
- MH_ERROR_NOT_CREATED
- MH_ERROR_DISABLED
- 4/4_4B5L5g5q5
- 9!9&989":9:P:g:
- InitSecurityInterfaceA
- 5"5,565@5J5T5^5.6_7
- bc00595440e801f8a5d2a2ad13b9791b
- MH_ERROR_ENABLED
- 5$505<5Q5V5\\5
- data_keyword
- 9%:+:R:d:s:|:
- :4;;;B;I;P;g=~=
- schannel.dll
- /.v?`.v!a/vAp.v
- "encryptedPassword":"
- 9\t:6:?:G:M:U:_:d:i:s:x:~:
- =R>X>]>c>i>q>
- >$>*>0>6><>B>H>N>b>h>n>t>
- :z;)<F<R<X<]<c<o<t<{<
- ? ?$?(?,?0?4?8?<?

- <(=1=9=M=S=Y=b=

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 P1, Explorer.EXE)
  - **Thread' events**
    - Process Create (C:\\Windows\\explorer.exe PID: P1, Command line: "C:\\Windows\\explorer.exe")
- **Thread T2 (in process P1, Explorer.EXE) description**
  - **Thread's childs**
    - Thread T3 (in process P1, Explorer.EXE)
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)
    - Thread Create (Thread ID: T3)
- **Thread T3 (in process P1, Explorer.EXE) description**
  - **Thread's childs**
    - Thread T4 (in process P1, Explorer.EXE)
  - **Thread' events**
    - Thread Create (Thread ID: T4)
- **Thread T4 (in process P1, Explorer.EXE) description**
  - **Thread's childs**
    - Thread T5 (in process P1, Explorer.EXE)

- **Thread' events**

  - RegSetValue (HKCU\\Software\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt\\D Type: REG_BINARY, Length: 56, Data: 49 00 56 00 2B 00 75 00 36 00 38 00 47 00 48 00)
  - RegSetValue (HKLM\\System\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp\\MaxConnectionTime Type: REG_DWORD, Length: 4, Data: 0)
  - RegSetValue (HKLM\\System\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp\\MaxDisconnectionTime Type: REG_DWORD, Length: 4, Data: 0)
  - RegSetValue (HKLM\\System\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp\\MaxIdleTime Type: REG_DWORD, Length: 4, Data: 0)
  - Thread Create (Thread ID: T5)

Thread T5 (in process P1, Explorer.EXE) description

- **Thread's childs**

  - Thread T6 (in process P1, Explorer.EXE)

- **Thread' events**

  - Thread Create (Thread ID: T6)

Thread T6 (in process P1, Explorer.EXE) description

- **Thread's childs**

  - Thread T7 (in process P1, Explorer.EXE)

- **Thread' events**

  - Thread Create (Thread ID: T7)

Thread T7 (in process P1, Explorer.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.

Process P1 (Explorer.EXE)'s network events

- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (116))
- UDP Send (P3PP3R-PC.localdomain:dynport-> mx5.sourpuss.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> mx5.sourpuss.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> mx5.sourpuss.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> mx5.sourpuss.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> mx5.sourpuss.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> freya.stelas.de:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> freya.stelas.de:domain (116))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 107.161.16.236:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 107.161.16.236:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 107.161.16.236:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 107.161.16.236:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 107.161.16.236:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> smtp.sourpuss.net:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> smtp.sourpuss.net:domain (503))
- UDP Send (P3PP3R-PC.localdomain:dynport-> ns14.ns.ph2network.org:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> ns14.ns.ph2network.org:domain (116))
- UDP Send (P3PP3R-PC.localdomain:dynport-> newton.bambusoft.mx:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> newton.bambusoft.mx:domain (503))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 50.3.82.162:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> 50.3.82.162:domain (116))
- UDP Send (P3PP3R-PC.localdomain:dynport-> philipostendorf.de:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> philipostendorf.de:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> reverse.gdsz.cncnet.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> reverse.gdsz.cncnet.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> reverse.gdsz.cncnet.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> reverse.gdsz.cncnet.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> reverse.gdsz.cncnet.net:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 151.120.36.59.broad.dg.gd.dynamic.163data.com.cn:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 151.120.36.59.broad.dg.gd.dynamic.163data.com.cn:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 151.120.36.59.broad.dg.gd.dynamic.163data.com.cn:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 151.120.36.59.broad.dg.gd.dynamic.163data.com.cn:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 151.120.36.59.broad.dg.gd.dynamic.163data.com.cn:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 180.163.8.114:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 180.163.8.114:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 180.163.8.114:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 180.163.8.114:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> 180.163.8.114:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (116))
- UDP Send (P3PP3R-PC.localdomain:dynport-> smtp.sourpuss.net:domain (43))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> smtp.sourpuss.net:domain (503))
- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))

- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))
- UDP Send (P3PP3R-PC.localdomain:dynport-> static.38.133.76.144.clients.your-server.de:domain (43))

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**
    - 44616e530000000000000000000000000831c0e000100000009788300030000000978930011000000000001005600000001b9dab00150000001b9d9d00
  - **Module 1 strings**
    - **Module 1 most interesting strings**
      - !This program cannot be run in DOS mode.
      - iMb}Agb:nBK<Fs3pP]D;igf:oR\\}PML:PRDfidPfi`_
      - GetCurrentThread
      - kBX:iNe|F9DfS9\\skRX?nRHaSRXfi8\\sng\\sDI?`h8:|nMLpk9G
      - InitializeAcl
      - TerminateProcess
      - CryptBinaryToStringW
      - Module32NextW
      - explorer.exe
      - CryptBinaryToStringA
      - CreateFileMappingW
      - Process32FirstW
      - GetProcAddress
      - MultiByteToWideChar
      - SetSecurityInfo
      - GetCurrentProcessId
      - Module32FirstW
      - GetCurrentProcess
      - Process32NextW
      - D:(D;OICI;GA;;;BG)(D;OICI;GA;;;AN)(A;OICI;GA;;;AU)(A;OICI;GA;;;BA)
      - GetUserGeoID
      - FlushFileBuffers
      - GetSystemInfo
      - OutputDebugStringW
      - u?8X*u:jRXjCf
      - CoCreateInstance
      - MapViewOfFile
      - WideCharToMultiByte
      - CheckRemoteDebuggerPresent
      - OpenProcessToken
      - GetTickCount
      - IsDebuggerPresent
      - CreateToolhelp32Snapshot
      - CryptStringToBinaryW
      - CryptStringToBinaryA
      - VirtualAlloc
      - SetFileAttributesW
      - QueryDosDeviceW
      - RegSetValueExA
      - VirtualQuery

- UnmapViewOfFile
- RegSetValueExW
- GetClassNameW
- RegDeleteValueW
- GetModuleHandleW
- FindFirstFileW
- GetModuleFileNameExW
- GetComputerNameExW
- GetSidSubAuthority
- GetTempPathW
- FindNextFileW
- RegCreateKeyExW
- GetUserNameW
- GetTempFileNameW
- GetLocaleInfoW
- RegOpenKeyExA
- RegOpenKeyExW
- EnableWindow
- GetWindowsDirectoryW
- GetSystemMetrics
- GetSidSubAuthorityCount
- RegQueryValueExW
- RegCreateKeyExA
- WaitForSingleObject
- GetModuleFileNameW
- RegQueryValueExA
- GetShortPathNameW
- GetLastError
- GetTokenInformation

- **Module 1 other strings**

- %08X-%04X-%04X-%04X-%08X%04X
- PathFindExtensionW
- advapi32.dll
- PathFindFileNameW
- CoUninitialize
- CoInitializeEx
- SHGetSpecialFolderPathW
- !o~4!~~5!(~4!e
- CoInitialize
- ShellExecuteExW
- Zr~~4!~~4!~~4!
- {%08X-%04X-%04X-%04X-%08X%04X}
- s2A3R{[n=?O}^y9~>B8@eXo<3Hak8]Yis2A3R{[n=?O}^y9~>B8@eXo<3Hak8]Yi
- kernel32.dll
- S83~F9Xbi8~pFdHeiK77
- No strings found

• Module 2 (probably unpacked / injected by the sample)

• Module 2 rich signatures

- 44616e530000000000000000000000000831c0e000100000009788300030000000978930011000000000001005600000001b9dab00150000001b9d9d00

- **Module 2 strings**
  - **Module 2 most interesting strings**
    - !This program cannot be run in DOS mode.
    - iMb}Agb:nBK<Fs3pP]D;igf:oR\\}PML:PRDfidPfi`_
    - GetCurrentThread
    - kBX:iNe|F9DfS9\\skRX?nRHaSRXfi8\\sng\\sDI?`h8:|nMLpk9G
    - InitializeAcl
    - TerminateProcess
    - CryptBinaryToStringW
    - Module32NextW
    - explorer.exe
    - CryptBinaryToStringA
    - CreateFileMappingW
    - Process32FirstW
    - GetProcAddress
    - MultiByteToWideChar
    - SetSecurityInfo
    - GetCurrentProcessId
    - Module32FirstW
    - GetCurrentProcess
    - Process32NextW
    - D:(D;OICI;GA;;;BG)(D;OICI;GA;;;AN)(A;OICI;GA;;;AU)(A;OICI;GA;;;BA)
    - GetUserGeoID
    - FlushFileBuffers
    - GetSystemInfo
    - OutputDebugStringW
    - u?8X*u:jRXjCf
    - CoCreateInstance
    - MapViewOfFile
    - WideCharToMultiByte
    - CheckRemoteDebuggerPresent
    - OpenProcessToken
    - GetTickCount
    - IsDebuggerPresent
    - CreateToolhelp32Snapshot
    - CryptStringToBinaryW
    - CryptStringToBinaryA
    - VirtualAlloc
    - SetFileAttributesW
    - QueryDosDeviceW
    - RegSetValueExA
    - VirtualQuery
    - UnmapViewOfFile
    - RegSetValueExW
    - GetClassNameW
    - RegDeleteValueW
    - GetModuleHandleW
    - FindFirstFileW
    - GetModuleFileNameExW
    - GetComputerNameExW
    - GetSidSubAuthority
    - GetTempPathW
    - FindNextFileW

- RegCreateKeyExW
- GetUserNameW
- GetTempFileNameW
- GetLocaleInfoW
- RegOpenKeyExA
- RegOpenKeyExW
- EnableWindow
- GetWindowsDirectoryW
- GetSystemMetrics
- GetSidSubAuthorityCount
- RegQueryValueExW
- RegCreateKeyExA
- WaitForSingleObject
- GetModuleFileNameW
- RegQueryValueExA
- GetShortPathNameW
- GetLastError
- GetTokenInformation

• Module 2 other strings

- %08X-%04X-%04X-%04X-%08X%04X
- PathFindExtensionW
- advapi32.dll
- PathFindFileNameW
- CoUninitialize
- CoInitializeEx
- SHGetSpecialFolderPathW
- !o~4!~~5!(~4!e
- CoInitialize
- ShellExecuteExW
- Zr~~4!~~4!~~4!
- {%08X-%04X-%04X-%04X-%08X%04X}
- s2A3R{[n=?O}^y9~>B8@eXo<3Hak8]Yis2A3R{[n=?O}^y9~>B8@eXo<3Hak8]Yi
- kernel32.dll
- S83~F9Xbi8~pFdHeiK77
- No strings found

• Module 3 (probably unpacked / injected by the sample)

• Module 3 rich signatures

• 44616e530000000000000000000000000e81f040002000000831c0e0002000000097883000300000000000100f10000000978930001d0000000978840001000000 1b9daa00050000001b9dab00380000001b9d9d00

• Module 3 strings

• Module 3 most interesting strings

- reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /ve /t REG_SZ /d "%ls" /f
- %ls\\nss3.dll
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
- !This program cannot be run in DOS mode.
- Content-Type: application/x-www-form-urlencoded
- --disable-http2 --use-spdy=off --disable-quic

- iMb}Agb:nBK<Fs3pP]D;igf:oR\\}PML:PRDfidPfi`_
- user_pref("network.http.spdy.enabled.http2", false);
- user_pref("network.http.spdy.enabled", false);
- Content-Type: multipart/form-data; boundary=--------------------------%d
- Rundll32.exe SHELL32.DLL,ShellExec_RunDLL "cmd.exe" "/c %ls"
- Rundll32.exe SHELL32.DLL,ShellExec_RunDLL "%ls"
- Software\\Microsoft\\Office\\Outlook\\OMI Account Manager\\Accounts
- Windows Live Mail IMAP
- InternetCrackUrlA
- Outlook 2003/2010 HTTP
- Referer: %ls
- InterlockedExchange
- HTTP Password
- ObtainUserAgentString
- profiles.ini
- GetWindowThreadProcessId
- ns1.rodgerbruce.com
- Content-Disposition: form-data;name="fname"
- %sPOST data:
- Connection: close
- IMAP User Name
- SuspendThread
- GetCurrentThread
- Process32FirstW
- InterlockedCompareExchange
- SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp
- Mozilla\\Firefox
- SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- HttpOpenRequestW
- Rundll32.exe zipfldr.dll,RouteTheCall "%ls"
- <POP3_User_Name
- philipostendorf.de
- GetCurrentProcessId
- inject_after_keyword
- InternetConnectW
- Process32NextW
- Software\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt\\
- Pgdiplus.dll
- CMD notepad test
- c2hpdHmjcmF6eUBleHBsb2l0Lmlt
- ns1.moderntld.com
- Software\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt\\Dns\\
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)
- Outlook Express POP3
- HTTPMail Server
- HttpSendRequestW
- SELECT displayName FROM AntiVirusProduct
- Thunderbird.Url.news\\DefaultIcon
- RtlInitAnsiString
- GetPrivateProfileIntW
- RtlCreateUserThread
- GetProcAddress
- POP3 User Name
- Software\\Microsoft\\Windows Live Mail
- Windows Live Mail POP3
- newton.bambusoft.mx
- Software\\Microsoft\\Windows Mail

- Accept-Encoding
- ewininet.dll
- a.dnspod.com
- "encryptedUsername":"
- Content-Length: %i
- explorer.exe
- Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676
- cmd&%ls&%ls&%i&%i&%i&%i&%i&%ls&%s&%ls&%ls
- CreateRemoteThread
- FlushFileBuffers
- Outlook Express HTTP
- GetExitCodeProcess
- Content-Length: %d
- GET %s HTTP/1.0
- Content-Disposition: form-data; name="data"; filename="%ls"
- Content-Length
- MaxConnectionTime
- GetCurrentThreadId
- <IMAP_Server
- ns1.opennameserver.org
- LdrGetProcedureAddress
- NtGetContextThread
- TerminateProcess
- <POP3_Server
- GetSystemInfo
- <IMAP_User_Name
- SetUnhandledExceptionFilter
- GetExitCodeThread
- secondary.server.edv-froehlich.de
- HTTPMail Password2
- GdipGetImageEncoders
- CreateEventW
- GetPrivateProfileStringW
- HTTP authentication (encoded): %s
- MultiByteToWideChar
- Rundll32.exe url.dll,FileProtocolHandler "%ls"
- freya.stelas.de
- Microsoft Unified Security Protocol Provider
- \\\\.\\pipe\\c2hpdHmjcmF6eUBleHBsb2l0Lmlt
- "hostname":"
- POST %s HTTP/1.0
- Software\\Microsoft\\Internet Account Manager\\Accounts
- HTTP Server URL
- PK11SDR_Decrypt
- NtSetContextThread
- EnumProcesses
- PR_OpenTCPSocket
- Content-Type
- OutputDebugStringA
- RtlDecompressBuffer
- inject_setting
- inject_before_keyword
- ns.dotbit.me
- ResumeThread
- IsWow64Process
- ConnectNamedPipe

- CreateThread
- GetLogicalDrives
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
- Resource: (%s), Service: (%s), User: (%s), Password: (%s)
- kBX:iNe|F9DfS9\\skRX?nRHaSRXfi8\\sng\\sDI?`h8:|nMLpk9G
- CryptBinaryToStringA
- Outlook Express IMAP
- MaxDisconnectionTime
- HTTPMail User Name
- b.dnspod.com
- Cookie: %s=%s
- egdiplus.dll
- SetErrorMode
- HTTP authentication: username="%s", password="%s"
- GetSystemTime
- GetCurrentProcess
- DisconnectNamedPipe
- sourpuss.net
- CryptBinaryToStringW
- c.dnspod.com
- Content-Type: application/octet-stream
- %s\\Thunderbird\\profiles.ini
- ns14.ns.ph2network.org
- Cookie: %s=%s;uid=%ls
- GetOverlappedResult
- Transfer-Encoding
- Thread32First
- RtlCompressBuffer
- CoCreateInstance
- VirtualAllocEx
- ReadProcessMemory
- InternetReadFile
- InternetWriteFile
- VirtualProtectEx
- InternetCloseHandle
- OpenProcessToken
- GetTickCount
- CreateToolhelp32Snapshot
- SetThreadContext
- InternetCloseHandle gle: 0x%X, %u
- InternetQueryDataAvailable
- NtWriteVirtualMemory
- FlushInstructionCache
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- Thread32Next
- CryptStringToBinaryW
- CryptStringToBinaryA
- CryptUnprotectData
- VirtualAlloc
- CreateProcessW
- GetModuleHandleW
- RtlSetLastWin32Error
- NtFreeVirtualMemory
- RegDeleteKeyW

- CreateNamedPipeW
- GetLastError
- GetTokenInformation
- LeaveCriticalSection
- GetModuleInformation
- WaitForMultipleObjects
- FindFirstFileW
- RtlCreateUnicodeStringFromAsciiz
- GetComputerNameExW
- FindNextFileW
- GetTempFileNameW
- GetProcessHeap
- CreateDirectoryW
- NtAllocateVirtualMemory
- SetThreadExecutionState
- GetSystemMetrics
- VirtualProtect
- GetVersionExW
- LoadLibraryW
- EnterCriticalSection
- InterlockedIncrement
- CreateMutexW
- VirtualQueryEx
- RegSetValueExA
- VirtualQuery
- RegSetValueExW
- RegDeleteValueW
- NtProtectVirtualMemory
- NtQueryVirtualMemory
- RegQueryValueExW
- RegCreateKeyExA
- RtlGetCompressionWorkSpaceSize
- GetModuleFileNameW
- RegQueryValueExA
- RegCreateKeyExW
- SetLastError
- GetEnvironmentVariableW
- SetFileAttributesW
- InterlockedDecrement
- InitializeCriticalSection
- WaitForSingleObject
- GetTempPathW
- RtlNtStatusToDosError
- RegOpenKeyExA
- GetModuleFileNameExW
- RegOpenKeyExW
- NtReadVirtualMemory
- GetFileAttributesW
- CallNamedPipeW
- GetDriveTypeW

- **Module 3 other strings**

- Outlook 2003/2010 POP3
- CreateCompatibleBitmap
- 4.43494@4U4Z4`4g4

- PathFileExistsW
- MH_ERROR_UNSUPPORTED_FUNCTION
- 5&5+50555?5D5I5N5X5]5b5g5
- SelectObject
- Outlook 2003/2010 IMAP
- CoInitialize
- 0%0,01070C0J0X0^0q0
- IMAP Password2
- 7"8W8]8i8r8x8
- PR_GetNameForIdentity
- <POP3_Password2
- IMAP Password
- advapi32.dll
- 8 848>8Q8e8o8
- SECITEM_ZfreeItem
- MH_ERROR_NOT_INITIALIZED
- MH_ERROR_FUNCTION_NOT_FOUND
- MH_ERROR_ALREADY_INITIALIZED
- GdipCreateBitmapFromHBITMAP
- PathCombineW
- POP3 Password2
- 3'3/3`3f3r3x3
- application/x-www-form-urlencoded
- GdipGetImageEncodersSize
- GdiplusShutdown
- Authorization
- 5 5)505B5I5R5X5a5i5q5
- POP3 Password
- kernel32.dll
- S83~F9Xbi8~pFdHeiK77mozglue.dll
- 7*8?8^8u839n9
- Proxy-Connection
- MH_ERROR_ALREADY_CREATED
- CreateCompatibleDC
- DeleteObject
- If-Modified-Since
- MH_ERROR_MEMORY_ALLOC
- M:
- CoUninitialize
- 5Z6`6e6j6o6t6
- 5O6X6_6e6n6u6}6
- MH_ERROR_MODULE_NOT_FOUND
- SHGetFolderPathW
- MH_ERROR_MEMORY_PROTECT
- 3Q4W4\\4b4h4q4
- PStoreCreateInstance
- GdiplusStartup
- PathAddBackslashW
- %s\\%s\\account*.oeaccount
- <IMAP_Password2
- MH_ERROR_NOT_EXECUTABLE
- PathFindExtensionW
- GdipSaveImageToFile
- %s\\Thunderbird\\%s\\logins.json
- MH_ERROR_NOT_CREATED
- MH_ERROR_DISABLED
- 4/4_4B5L5g5q5

- 9:P:g:
- InitSecurityInterfaceA
- s2A3R{[n=?O}^y9~>B8@eXo<3Hak8]Yis2A3R{[n=?O}^y9~>B8@eXo<3Hak8]Yi
- 5"5,565@5J5T5^5.6_7
- bc00595440e801f8a5d2a2ad13b9791b
- MH_ERROR_ENABLED
- 5$505<5Q5V5\\5
- data_keyword
- +:R:d:s:|:
- 4;;;B;I;P;g=~=
- schannel.dll
- /.v?`.v!a/vAp.v
- "
- 6:?:G:M:U:_:d:i:s:x:~:
- =R>X>]>c>i>q>
- >$>*>0>6><>B>H>N>b>h>n>t>
- z;)<F<R<X<]<c<o<t<{<
- ? ?$?(?,?0?4?8?<?
- <(=1=9=M=S=Y=b=

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