Sample: 3cfd66340f204e1b8697e7a8514c00ab

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 #BLACKMOON** (based on p3pperp0tts rules)

Analysis date: 2019-03-15 09:18:27 (p3pperp0tts platform's analysis date)

Exe timestamp: 2016-04-08 04:29:43 (timestamp of the original sample)

Unpacked mods max timestamp: 2016-04-08 04:29:43 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2016-09-12 08:02:21 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: 3cfd66340f204e1b8697e7a8514c00ab

AV detections

- Microsoft: VirTool:Win32/Injector.HY
- Kaspersky: Trojan-Banker.Win32.Banbra.tlgl
- Symantec: Infostealer.Boyapki.E
- Malwarebytes: Trojan.Injector

Source

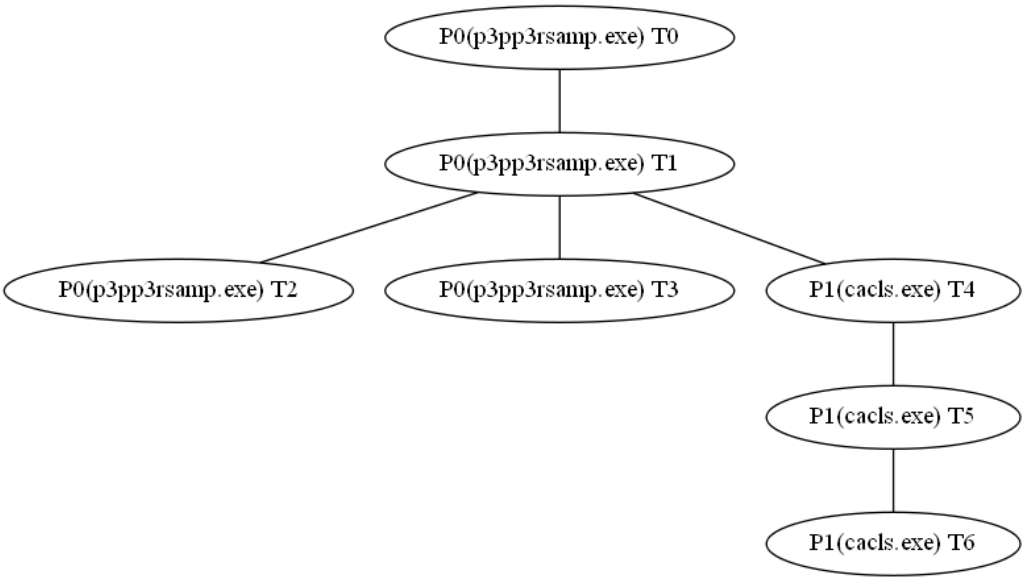
-

Virustotal

- https://virustotal.com/es/file/406c50ed0333d2023de55ce798a4e7d5fa6e45df65c16733ef48961e94277807/analysis

Threads tree

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



Most interesting behavior

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

- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- Process Create (C:\\Windows\\system32\\cacls.exe PID: P1, Command line: C:\\Windows\\System32\\cacls.exe)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\35V5Bj9b Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- RegCreateKey (HKCU\\Software\\Microsoft\\Windows Script\\Settings Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
- Thread Create (Thread ID: T1)
- Thread Create (Thread ID: T2)
- Thread Create (Thread ID: T3)
- Thread Create (Thread ID: TUNKALIAS)
- Thread Create (Thread ID: T5)
- Thread Create (Thread ID: T6)

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.
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- abnormal program termination
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- REG_MULTI_SZ -
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- REG_REG_EXPAND_SZ -
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- Select FreeVirtualMemory From Win32_OperatingSystem
- DOMAIN error
- LOADER ERROR
- Select CodeSet From Win32_OperatingSystem
- OriginalFilename
- Select DataExecutionPrevention_32BitApplications From Win32_OperatingSystem
- Qihu 360 Software Co., Ltd.
- - unable to open console device
- PathFileExistsA
- WbemScripting.SWbemDateTime
- StringFileInfo
- Select FreePhysicalMemory From Win32_OperatingSystem
- </requestedPrivileges>
- - not enough space for lowio initialization
- LastBootUpTime
- Select CountryCode From Win32_OperatingSystem
- {dc12a687-737f-11cf-884d-00aa004b2e24}
- Microsoft Visual C++ Runtime Library
- <program name unknown>
- GetProcAddress
- - not enough space for _onexit/atexit table
- Select Debug From Win32_OperatingSystem
- Select CSDVersion From Win32_OperatingSystem
- SunMonTueWedThuFriSat
- Select Distributed From Win32_OperatingSystem
- VS_VERSION_INFO
- Select ForegroundApplicationBoost From Win32_OperatingSystem
- Select FreeSpaceInPagingFiles From Win32_OperatingSystem
- Select DataExecutionPrevention_SupportPolicy From Win32_OperatingSystem
- CurrentTimeZone
- FreeSpaceInPagingFiles
- ForegroundApplicationBoost
- </trustInfo>
- Select CurrentTimeZone From Win32_OperatingSystem
- runtime error
- - unable to initialize heap
- Select Description From Win32_OperatingSystem
- DataExecutionPrevention_SupportPolicy
- - not enough space for stdio initialization
- DataExecutionPrevention_Drivers
- - not enough space for thread data
- JanFebMarAprMayJunJulAugSepOctNovDec
- Select EncryptionLevel From Win32_OperatingSystem

- <requestedPrivileges>
- 360 Internet Security Base Module
- Select DataExecutionPrevention_Available From Win32_OperatingSystem
- Select DataExecutionPrevention_Drivers From Win32_OperatingSystem
- LegalCopyright
- - unexpected multithread lock error
- SELECT Caption FROM Win32_OperatingSystem
- - floating point not loaded
- Select BootDevice From Win32_OperatingSystem
- Select InstallDate From Win32_OperatingSystem
- Runtime Error!
- - pure virtual function call
- 360 Internet Security
- __GLOBAL_HEAP_SELECTED
- Select CSName From Win32_OperatingSystem
- InternalName
- - not enough space for arguments
- The procedure entry point %s could not be located in the dynamic link library %s
- Select BuildType From Win32_OperatingSystem
- (C) 2013 Qihu 360 Software Co., Ltd.
- Select BuildNumber From Win32_OperatingSystem
- The ordinal %u could not be located in the dynamic link library %s
- - not enough space for environment
- IsBadCodePtr
- Select PAEEnabled From Win32_OperatingSystem
- IsBadReadPtr
- CallWindowProcA
- Select Version From Win32_OperatingSystem
- Select OSLanguage From Win32_OperatingSystem
- CLSIDFromProgID
- Select Primary From Win32_OperatingSystem
- CreateProcessA
- Select MaxProcessMemorySize From Win32_OperatingSystem
- HKEY_CURRENT_USER
- PlusVersionNumber
- GetCurrentThreadId
- Select SystemDirectory From Win32_OperatingSystem
- Select Organization From Win32_OperatingSystem
- Select LocalDateTime From Win32_OperatingSystem
- Select ServicePackMajorVersion From Win32_OperatingSystem
- Select SystemDrive From Win32_OperatingSystem
- Select Status From Win32_OperatingSystem
- PlusProductID
- GetCurrentProcessId
- Select Manufacturer From Win32_OperatingSystem
- Select OtherTypeDescription From Win32_OperatingSystem
- GetEnvironmentStrings
- Select TotalVisibleMemorySize From Win32_OperatingSystem
- RegisteredUser
- program internal error number is %d.
- LCMapStringA
- MUILanguages
- SerialNumber
- LCMapStringW
- NumberOfProcesses
- SizeStoredInPagingFiles
- REG_DWORD - DWORD

- Select OSProductSuite From Win32_OperatingSystem
- CryptGetHashParam
- Select RegisteredUser From Win32_OperatingSystem
- CryptDestroyHash
- Select Locale From Win32_OperatingSystem
- HKEY_LOCAL_MACHINE
- Select PlusProductID From Win32_OperatingSystem
- CLSIDFromString
- GetUserDefaultLCID
- Select MaxNumberOfProcesses From Win32_OperatingSystem
- Process32First
- OSArchitecture
- Select NumberOfProcesses From Win32_OperatingSystem
- CryptCreateHash
- Select NumberOfUsers From Win32_OperatingSystem
- IsBadWritePtr
- Context Menu Tree
- Select TotalVirtualMemorySize From Win32_OperatingSystem
- SetWaitableTimer
- Select OSType From Win32_OperatingSystem
- Control Type:
- overridden by code
- SetUnhandledExceptionFilter
- TerminateProcess
- &Custom; Filters...
- LocalDateTime
- Select MUILanguages From Win32_OperatingSystem
- SetFilePointer
- NumberOfLicensedUsers
- TranslateMessage
- MultiByteToWideChar
- UnhandledExceptionFilter
- abcdefghijklmnopqrstuvwxyz
- CoSetProxyBlanket
- Manufacturer
- FlushFileBuffers
- Select LastBootUpTime From Win32_OperatingSystem
- Select WindowsDirectory From Win32_OperatingSystem
- MaxNumberOfProcesses
- Select TotalSwapSpaceSize From Win32_OperatingSystem
- HKEY_CLASSES_ROOT
- ResumeThread
- Select PortableOperatingSystem From Win32_OperatingSystem
- SetFileAttributesA
- Select OperatingSystemSKU From Win32_OperatingSystem
- &Show; Folders
- Select Producttype From Win32_OperatingSystem
- Select ServicePackMinorVersion From Win32_OperatingSystem
- NumberOfUsers
- Select OSArchitecture From Win32_OperatingSystem
- Select SerialNumber From Win32_OperatingSystem
- Select SizeStoredInPagingFiles From Win32_OperatingSystem
- GetLogicalDrives
- OpenFileMappingA
- REG_BINARY -
- GetCurrentProcess
- FreeEnvironmentStringsA

- Select SuiteMask From Win32_OperatingSystem
- Select NumberOfLicensedUsers From Win32_OperatingSystem
- SysAllocString
- Select SystemDevice From Win32_OperatingSystem
- Select PlusVersionNumber From Win32_OperatingSystem
- IIDFromString
- MapViewOfFile
- VirtualAllocEx
- GetThreadContext
- GetTimeZoneInformation
- CoCreateInstance
- SetThreadContext
- VirtualProtectEx
- ReadProcessMemory
- WriteProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- WideCharToMultiByte
- GetModuleHandleA
- GetLastActivePopup
- LoadLibraryA
- RegDeleteKeyA
- MsgWaitForMultipleObjects
- GetActiveWindow
- VirtualAlloc
- RtlMoveMemory
- ZwUnmapViewOfSection
- GetTopWindow
- RaiseException
- GetCommandLineA
- GetCurrentDirectoryA
- CryptHashData
- GetEnvironmentStringsW
- GetLastError
- InterlockedIncrement
- RegEnumValueA
- CreateWaitableTimerA
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- GetStartupInfoA
- GetVersionExA
- SetHandleCount
- EnterCriticalSection
- LeaveCriticalSection
- GetLocaleInfoA
- RegDeleteValueA
- RegSetValueExA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA
- RegQueryValueExA
- InitializeCriticalSection
- SetLastError
- InterlockedDecrement
- GetEnvironmentVariableA
- GetStringTypeW

- GetUserNameA
- GetStringTypeA
- SetStdHandle
- RegOpenKeyExA
- FreeEnvironmentStringsW
- DispatchMessageA
- DeleteCriticalSection
- RegCreateKeyA
- WaitForSingleObject
- GetStdHandle

Hosts

- 203.205.151.50:http
- google-public-dns-a.google.com:domain
- 192.168.149.167:49159
- 203.205.151.50:80 (users.qzone.qq.com)

Dns queries

- isatap.localdomain ---> no answers
- users.qzone.qq.com ---> 203.205.151.50
- 8.8.8.8.in-addr.arpa ---> no answers
- 50.151.205.203.in-addr.arpa ---> no answers

Network traffic

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

- **tcp 192.168.149.167:49159 ---> 203.205.151.50 (users.qzone.qq.com) :80**

  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36[...]GET /fcg-bin/cgi_get_portrait.fcg?uins=2464258288 HTTP/1.1[...]Connection: Keep-Alive[...]Host: users.qzone.qq.com

- **tcp 203.205.151.50 (users.qzone.qq.com) :80 ---> 192.168.149.167:49159**

  <h1>301 Moved Permanently</h1> [...]Content-Type: text/html[...]Location: https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=2464258288[...]Content-Length: 193[...]Date: Fri, 15 Mar 2019 08:01:26 GMT[...]Server: stgw/1.3.10.5_1.13.5[...]<hr> stgw/1.3.10.5_1.13.5 [...]HTTP/1.1 301 Moved Permanently[...]Connection: Keep-Alive[...]<body bgcolor="white">[...]<head><title>301 Moved Permanently</title></head>

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.
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- abnormal program termination
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- REG_MULTI_SZ -
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- REG_REG_EXPAND_SZ -
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- Select FreeVirtualMemory From Win32_OperatingSystem
- DOMAIN error
- LOADER ERROR
- Select CodeSet From Win32_OperatingSystem
- OriginalFilename
- Select DataExecutionPrevention_32BitApplications From Win32_OperatingSystem
- Qihu 360 Software Co., Ltd.
- - unable to open console device
- PathFileExistsA
- WbemScripting.SWbemDateTime
- StringFileInfo
- Select FreePhysicalMemory From Win32_OperatingSystem
- </requestedPrivileges>
- - not enough space for lowio initialization
- LastBootUpTime
- Select CountryCode From Win32_OperatingSystem
- {dc12a687-737f-11cf-884d-00aa004b2e24}
- Microsoft Visual C++ Runtime Library
- <program name unknown>
- GetProcAddress
- - not enough space for _onexit/atexit table
- Select Debug From Win32_OperatingSystem
- Select CSDVersion From Win32_OperatingSystem
- SunMonTueWedThuFriSat
- Select Distributed From Win32_OperatingSystem
- VS_VERSION_INFO
- Select ForegroundApplicationBoost From Win32_OperatingSystem
- Select FreeSpaceInPagingFiles From Win32_OperatingSystem
- Select DataExecutionPrevention_SupportPolicy From Win32_OperatingSystem
- CurrentTimeZone
- FreeSpaceInPagingFiles
- ForegroundApplicationBoost
- </trustInfo>
- Select CurrentTimeZone From Win32_OperatingSystem
- runtime error
- - unable to initialize heap
- Select Description From Win32_OperatingSystem
- DataExecutionPrevention_SupportPolicy
- - not enough space for stdio initialization
- DataExecutionPrevention_Drivers
- - not enough space for thread data
- JanFebMarAprMayJunJulAugSepOctNovDec
- Select EncryptionLevel From Win32_OperatingSystem

- <requestedPrivileges>
- 360 Internet Security Base Module
- Select DataExecutionPrevention_Available From Win32_OperatingSystem
- Select DataExecutionPrevention_Drivers From Win32_OperatingSystem
- LegalCopyright
- - unexpected multithread lock error
- SELECT Caption FROM Win32_OperatingSystem
- - floating point not loaded
- Select BootDevice From Win32_OperatingSystem
- Select InstallDate From Win32_OperatingSystem
- Runtime Error!
- - pure virtual function call
- 360 Internet Security
- __GLOBAL_HEAP_SELECTED
- Select CSName From Win32_OperatingSystem
- InternalName
- - not enough space for arguments
- The procedure entry point %s could not be located in the dynamic link library %s
- Select BuildType From Win32_OperatingSystem
- (C) 2013 Qihu 360 Software Co., Ltd.
- Select BuildNumber From Win32_OperatingSystem
- The ordinal %u could not be located in the dynamic link library %s
- - not enough space for environment
- IsBadCodePtr
- Select PAEEnabled From Win32_OperatingSystem
- IsBadReadPtr
- CallWindowProcA
- Select Version From Win32_OperatingSystem
- Select OSLanguage From Win32_OperatingSystem
- CLSIDFromProgID
- Select Primary From Win32_OperatingSystem
- CreateProcessA
- Select MaxProcessMemorySize From Win32_OperatingSystem
- HKEY_CURRENT_USER
- PlusVersionNumber
- GetCurrentThreadId
- Select SystemDirectory From Win32_OperatingSystem
- Select Organization From Win32_OperatingSystem
- Select LocalDateTime From Win32_OperatingSystem
- Select ServicePackMajorVersion From Win32_OperatingSystem
- Select SystemDrive From Win32_OperatingSystem
- Select Status From Win32_OperatingSystem
- PlusProductID
- GetCurrentProcessId
- Select Manufacturer From Win32_OperatingSystem
- Select OtherTypeDescription From Win32_OperatingSystem
- GetEnvironmentStrings
- Select TotalVisibleMemorySize From Win32_OperatingSystem
- RegisteredUser
- program internal error number is %d.
- LCMapStringA
- MUILanguages
- SerialNumber
- LCMapStringW
- NumberOfProcesses
- SizeStoredInPagingFiles
- REG_DWORD - DWORD

- Select OSProductSuite From Win32_OperatingSystem
- CryptGetHashParam
- Select RegisteredUser From Win32_OperatingSystem
- CryptDestroyHash
- Select Locale From Win32_OperatingSystem
- HKEY_LOCAL_MACHINE
- Select PlusProductID From Win32_OperatingSystem
- CLSIDFromString
- GetUserDefaultLCID
- Select MaxNumberOfProcesses From Win32_OperatingSystem
- Process32First
- OSArchitecture
- Select NumberOfProcesses From Win32_OperatingSystem
- CryptCreateHash
- Select NumberOfUsers From Win32_OperatingSystem
- IsBadWritePtr
- Context Menu Tree
- Select TotalVirtualMemorySize From Win32_OperatingSystem
- SetWaitableTimer
- Select OSType From Win32_OperatingSystem
- Control Type:
- overridden by code
- SetUnhandledExceptionFilter
- TerminateProcess
- &Custom; Filters...
- LocalDateTime
- Select MUILanguages From Win32_OperatingSystem
- SetFilePointer
- NumberOfLicensedUsers
- TranslateMessage
- MultiByteToWideChar
- UnhandledExceptionFilter
- abcdefghijklmnopqrstuvwxyz
- CoSetProxyBlanket
- Manufacturer
- FlushFileBuffers
- Select LastBootUpTime From Win32_OperatingSystem
- Select WindowsDirectory From Win32_OperatingSystem
- MaxNumberOfProcesses
- Select TotalSwapSpaceSize From Win32_OperatingSystem
- HKEY_CLASSES_ROOT
- ResumeThread
- Select PortableOperatingSystem From Win32_OperatingSystem
- SetFileAttributesA
- Select OperatingSystemSKU From Win32_OperatingSystem
- &Show; Folders
- Select Producttype From Win32_OperatingSystem
- Select ServicePackMinorVersion From Win32_OperatingSystem
- NumberOfUsers
- Select OSArchitecture From Win32_OperatingSystem
- Select SerialNumber From Win32_OperatingSystem
- Select SizeStoredInPagingFiles From Win32_OperatingSystem
- GetLogicalDrives
- OpenFileMappingA
- REG_BINARY -
- GetCurrentProcess
- FreeEnvironmentStringsA

- Select SuiteMask From Win32_OperatingSystem
- Select NumberOfLicensedUsers From Win32_OperatingSystem
- SysAllocString
- Select SystemDevice From Win32_OperatingSystem
- Select PlusVersionNumber From Win32_OperatingSystem
- IIDFromString
- MapViewOfFile
- VirtualAllocEx
- GetThreadContext
- GetTimeZoneInformation
- CoCreateInstance
- SetThreadContext
- VirtualProtectEx
- ReadProcessMemory
- WriteProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- WideCharToMultiByte
- GetModuleHandleA
- GetLastActivePopup
- LoadLibraryA
- RegDeleteKeyA
- MsgWaitForMultipleObjects
- GetActiveWindow
- 532A4C47797E747F67634C43696364757D23224C7371737C633E7568753375AEC2A
- FileDescription
- ProductVersion
- 7371737C633E756875133197F87
- {4590f811-1d3a-11d0-891f-00aa004b2e24}
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E88B8E8DF0
- "@0123456789ABCDEF
- GAIsProcessorFeaturePresent
- FreeVirtualMemory
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CEE14A4A29
- 1, 3, 0, 1209
- LiveUpd360.dll
- - unexpected heap error
- CoUninitialize
- oleaut32.dll
- kernel32.dll
- DataExecutionPrevention_Available
- FreePhysicalMemory
- 732A4C67797E747F67634C28202020F5B366961
- DataExecutionPrevention_32BitApplications
- EncryptionLevel
- advapi32.dll
- $*4:>>:74-./
- VirtualAlloc
- RtlMoveMemory
- ZwUnmapViewOfSection
- GetTopWindow
- RaiseException
- GetCommandLineA
- GetCurrentDirectoryA
- CryptHashData
- GetEnvironmentStringsW

- GetLastError
- InterlockedIncrement
- RegEnumValueA
- CreateWaitableTimerA
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- GetStartupInfoA
- GetVersionExA
- SetHandleCount
- EnterCriticalSection
- LeaveCriticalSection
- GetLocaleInfoA
- RegDeleteValueA
- RegSetValueExA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA
- RegQueryValueExA
- InitializeCriticalSection
- SetLastError
- InterlockedDecrement
- GetEnvironmentVariableA
- GetStringTypeW
- GetUserNameA
- GetStringTypeA
- SetStdHandle
- RegOpenKeyExA
- FreeEnvironmentStringsW
- DispatchMessageA
- DeleteCriticalSection
- RegCreateKeyA
- WaitForSingleObject
- GetStdHandle
- TotalVisibleMemorySize
- CoInitialize
- OSProductSuite
- CoInitializeEx
- PortableOperatingSystem
- TotalSwapSpaceSize
- ServicePackMajorVersion
- SystemDirectory
- Manufactured:
- OtherTypeDescription
- ServicePackMinorVersion
- CoInitializeSecurity
- Organization
- TotalVirtualMemorySize
- OperatingSystemSKU
- SystemDevice
- MaxProcessMemorySize
- WindowsDirectory
- __MSVCRT_HEAP_SELECT
- MS Shell Dlg

Threads behaviour

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

- ### Thread T0 (in process P0, p3pp3rsamp.exe) description

  - #### Thread's childs

    - Thread T1 (in process P0, p3pp3rsamp.exe)

  - #### Thread' events

    - Thread Create (Thread ID: T1)

- ### Thread T1 (in process P0, p3pp3rsamp.exe) description

  - #### Thread's childs

    - Thread T2 (in process P0, p3pp3rsamp.exe)
    - Thread T3 (in process P0, p3pp3rsamp.exe)
    - Thread T4 (in process P1, cacls.exe)

  - #### Thread' events

    - Thread Create (Thread ID: T2)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - Thread Create (Thread ID: T3)
    - Thread Create (Thread ID: TUNKALIAS)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)

- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)

- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- Process Create (C:\\Windows\\system32\\cacls.exe PID: P1, Command line: C:\\Windows\\System32\\cacls.exe)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\35V5Bj9b Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)

Thread T2 (in process P0, p3pp3rsamp.exe) description

Thread's childs

- No childs found

- **Thread' events**
  - Thread Create (Thread ID: TUNKALIAS)

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

- **Thread T4 (in process P1, cacls.exe) description**
  - **Thread's childs**
    - Thread T5 (in process P1, cacls.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T5)

- **Thread T5 (in process P1, cacls.exe) description**
  - **Thread's childs**
    - Thread T6 (in process P1, cacls.exe)
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)
    - Thread Create (Thread ID: TUNKALIAS)
    - RegCreateKey (HKCU\\Software\\Microsoft\\Windows Script\\Settings Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
    - Thread Create (Thread ID: T6)
    - Thread Create (Thread ID: TUNKALIAS)

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

- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (486))
- TCP Connect (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (0))
- TCP Send (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (251))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (333))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (114))
- TCP Disconnect (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (0))

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**
    - 44616e530000000000000000000000007b1c0c0001000000831c0e001e00000036260a0065000000c30f5f0004000000c30f5d000d00000000000100a400000036260b00410000000000000001000000e81f0b00
  - **Module 1 strings**
    - **Module 1 most interesting strings**
      - !This program cannot be run in DOS mode.
      - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
      - abnormal program termination
      - <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
      - <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
      - Select FreeVirtualMemory From Win32_OperatingSystem
      - DOMAIN error
      - LOADER ERROR
      - Select CodeSet From Win32_OperatingSystem
      - OriginalFilename
      - Select DataExecutionPrevention_32BitApplications From Win32_OperatingSystem
      - Qihu 360 Software Co., Ltd.
      - - unable to open console device
      - PathFileExistsA
      - WbemScripting.SWbemDateTime
      - StringFileInfo
      - Select FreePhysicalMemory From Win32_OperatingSystem
      - </requestedPrivileges>
      - - not enough space for lowio initialization
      - LastBootUpTime
      - Select CountryCode From Win32_OperatingSystem
      - {dc12a687-737f-11cf-884d-00aa004b2e24}
      - Microsoft Visual C++ Runtime Library
      - <program name unknown>
      - GetProcAddress
      - - not enough space for _onexit/atexit table
      - Select Debug From Win32_OperatingSystem
      - Select CSDVersion From Win32_OperatingSystem
      - SunMonTueWedThuFriSat
      - Select Distributed From Win32_OperatingSystem
      - VS_VERSION_INFO
      - Select ForegroundApplicationBoost From Win32_OperatingSystem
      - Select FreeSpaceInPagingFiles From Win32_OperatingSystem
      - Select DataExecutionPrevention_SupportPolicy From Win32_OperatingSystem
      - CurrentTimeZone
      - FreeSpaceInPagingFiles
      - ForegroundApplicationBoost
      - </trustInfo>
      - Select CurrentTimeZone From Win32_OperatingSystem
      - runtime error

- - unable to initialize heap
- Select Description From Win32_OperatingSystem
- DataExecutionPrevention_SupportPolicy
- - not enough space for stdio initialization
- DataExecutionPrevention_Drivers
- - not enough space for thread data
- JanFebMarAprMayJunJulAugSepOctNovDec
- Select EncryptionLevel From Win32_OperatingSystem
- <requestedPrivileges>
- 360 Internet Security Base Module
- Select DataExecutionPrevention_Available From Win32_OperatingSystem
- Select DataExecutionPrevention_Drivers From Win32_OperatingSystem
- LegalCopyright
- - unexpected multithread lock error
- SELECT Caption FROM Win32_OperatingSystem
- - floating point not loaded
- Select BootDevice From Win32_OperatingSystem
- Select InstallDate From Win32_OperatingSystem
- Runtime Error!
- - pure virtual function call
- 360 Internet Security
- __GLOBAL_HEAP_SELECTED
- Select CSName From Win32_OperatingSystem
- InternalName
- - not enough space for arguments
- The procedure entry point %s could not be located in the dynamic link library %s
- Select BuildType From Win32_OperatingSystem
- (C) 2013 Qihu 360 Software Co., Ltd.
- Select BuildNumber From Win32_OperatingSystem
- The ordinal %u could not be located in the dynamic link library %s
- - not enough space for environment
- GetModuleHandleA
- GetLastActivePopup
- LoadLibraryA
- RegDeleteKeyA
- MsgWaitForMultipleObjects
- GetActiveWindow

- **Module 1 other strings**

- 532A4C47797E747F67634C43696364757D23224C7371737C633E7568753375AEC2A
- FileDescription
- ProductVersion
- 7371737C633E756875133197F87
- {4590f811-1d3a-11d0-891f-00aa004b2e24}
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CEE14A4A29
3797F7E4C42657E88B8E8DF0
- "@0123456789ABCDEF
- GAIsProcessorFeaturePresent
- FreeVirtualMemory
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CEE14A4A29
- 1, 3, 0, 1209
- LiveUpd360.dll
- - unexpected heap error
- CoUninitialize
- oleaut32.dll

- kernel32.dll
- DataExecutionPrevention_Available
- FreePhysicalMemory
- 732A4C67797E747F67634C28202020F5B366961
- DataExecutionPrevention_32BitApplications
- EncryptionLevel
- advapi32.dll
- >>:74-./
- __MSVCRT_HEAP_SELECT

Module 2 (probably unpacked / injected by the sample)

Module 2 rich signatures

- 44616e530000000000000000000000007b1c0c0001000000831c0e001e00000036260a0065000000c30f5f0004000000c30f5d000d00000000000100a400000036260b00410000000000000001000000e81f0b00

Module 2 strings

Module 2 most interesting strings

- REG_MULTI_SZ -
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- !This program cannot be run in DOS mode.
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- abnormal program termination
- REG_REG_EXPAND_SZ -
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- Select FreeVirtualMemory From Win32_OperatingSystem
- DOMAIN error
- IsBadCodePtr
- Select PAEEnabled From Win32_OperatingSystem
- IsBadReadPtr
- CallWindowProcA
- Select Version From Win32_OperatingSystem
- Select OSLanguage From Win32_OperatingSystem
- CLSIDFromProgID
- Select Primary From Win32_OperatingSystem
- Select InstallDate From Win32_OperatingSystem
- CreateProcessA
- Select MaxProcessMemorySize From Win32_OperatingSystem
- HKEY_CURRENT_USER
- Select CodeSet From Win32_OperatingSystem
- PlusVersionNumber
- GetCurrentThreadId
- Select SystemDirectory From Win32_OperatingSystem
- Select DataExecutionPrevention_32BitApplications From Win32_OperatingSystem
- The procedure entry point %s could not be located in the dynamic link library %s
- Qihu 360 Software Co., Ltd.
- Select Organization From Win32_OperatingSystem
- PathFileExistsA
- WbemScripting.SWbemDateTime
- Select LocalDateTime From Win32_OperatingSystem
- Select ServicePackMajorVersion From Win32_OperatingSystem
- StringFileInfo

- Select SystemDrive From Win32_OperatingSystem
- Select FreePhysicalMemory From Win32_OperatingSystem
- Select Status From Win32_OperatingSystem
- PlusProductID
- GetCurrentProcessId
- Select Manufacturer From Win32_OperatingSystem
- Select OtherTypeDescription From Win32_OperatingSystem
- GetEnvironmentStrings
- Select ForegroundApplicationBoost From Win32_OperatingSystem
- Select TotalVisibleMemorySize From Win32_OperatingSystem
- RegisteredUser
- program internal error number is %d.
- LCMapStringA
- - not enough space for lowio initialization
- MUILanguages
- SerialNumber
- LCMapStringW
- NumberOfProcesses
- SizeStoredInPagingFiles
- REG_DWORD - DWORD
- Select OSProductSuite From Win32_OperatingSystem
- LOADER ERROR
- <program name unknown>
- CryptGetHashParam
- Select RegisteredUser From Win32_OperatingSystem
- CryptDestroyHash
- GetProcAddress
- - not enough space for _onexit/atexit table
- Select Debug From Win32_OperatingSystem
- Select Locale From Win32_OperatingSystem
- Select CSDVersion From Win32_OperatingSystem
- SunMonTueWedThuFriSat
- HKEY_LOCAL_MACHINE
- Select Distributed From Win32_OperatingSystem
- VS_VERSION_INFO
- Select PlusProductID From Win32_OperatingSystem
- - unable to open console device
- CLSIDFromString
- GetUserDefaultLCID
- </requestedPrivileges>
- Select MaxNumberOfProcesses From Win32_OperatingSystem
- Select FreeSpaceInPagingFiles From Win32_OperatingSystem
- Process32First
- OSArchitecture
- Select DataExecutionPrevention_SupportPolicy From Win32_OperatingSystem
- Select NumberOfProcesses From Win32_OperatingSystem
- CryptCreateHash
- Select NumberOfUsers From Win32_OperatingSystem
- IsBadWritePtr
- FreeSpaceInPagingFiles
- Context Menu Tree
- LastBootUpTime
- Select TotalVirtualMemorySize From Win32_OperatingSystem
- (C) 2013 Qihu 360 Software Co., Ltd.
- Select CountryCode From Win32_OperatingSystem
- ForegroundApplicationBoost
- SetWaitableTimer

- </trustInfo>
- Select CurrentTimeZone From Win32_OperatingSystem
- Select OSType From Win32_OperatingSystem
- Control Type:
- overridden by code
- SetUnhandledExceptionFilter
- TerminateProcess
- &Custom; Filters...
- Select BootDevice From Win32_OperatingSystem
- LocalDateTime
- Select CSName From Win32_OperatingSystem
- Microsoft Visual C++ Runtime Library
- InternalName
- Select MUILanguages From Win32_OperatingSystem
- SetFilePointer
- - unable to initialize heap
- Select Description From Win32_OperatingSystem
- DataExecutionPrevention_SupportPolicy
- - not enough space for stdio initialization
- NumberOfLicensedUsers
- TranslateMessage
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- LegalCopyright
- runtime error
- abcdefghijklmnopqrstuvwxyz
- - not enough space for thread data
- CoSetProxyBlanket
- Manufacturer
- FlushFileBuffers
- Select LastBootUpTime From Win32_OperatingSystem
- JanFebMarAprMayJunJulAugSepOctNovDec
- Select EncryptionLevel From Win32_OperatingSystem
- <requestedPrivileges>
- Select WindowsDirectory From Win32_OperatingSystem
- MaxNumberOfProcesses
- 360 Internet Security Base Module
- DataExecutionPrevention_Drivers
- Select TotalSwapSpaceSize From Win32_OperatingSystem
- Select DataExecutionPrevention_Available From Win32_OperatingSystem
- The ordinal %u could not be located in the dynamic link library %s
- HKEY_CLASSES_ROOT
- CurrentTimeZone
- Select DataExecutionPrevention_Drivers From Win32_OperatingSystem
- ResumeThread
- Select PortableOperatingSystem From Win32_OperatingSystem
- SetFileAttributesA
- - unexpected multithread lock error
- SELECT Caption FROM Win32_OperatingSystem
- Select OperatingSystemSKU From Win32_OperatingSystem
- &Show; Folders
- Select Producttype From Win32_OperatingSystem
- Select ServicePackMinorVersion From Win32_OperatingSystem
- - floating point not loaded
- NumberOfUsers

- Select OSArchitecture From Win32_OperatingSystem
- {dc12a687-737f-11cf-884d-00aa004b2e24}
- Select SerialNumber From Win32_OperatingSystem
- - pure virtual function call
- Select SizeStoredInPagingFiles From Win32_OperatingSystem
- GetLogicalDrives
- 360 Internet Security
- OpenFileMappingA
- __GLOBAL_HEAP_SELECTED
- REG_BINARY -
- GetCurrentProcess
- FreeEnvironmentStringsA
- Select SuiteMask From Win32_OperatingSystem
- Select NumberOfLicensedUsers From Win32_OperatingSystem
- OriginalFilename
- - not enough space for arguments
- SysAllocString
- Select SystemDevice From Win32_OperatingSystem
- Select BuildType From Win32_OperatingSystem
- Select PlusVersionNumber From Win32_OperatingSystem
- IIDFromString
- Select BuildNumber From Win32_OperatingSystem
- - not enough space for environment
- MapViewOfFile
- VirtualAllocEx
- GetThreadContext
- GetTimeZoneInformation
- CoCreateInstance
- SetThreadContext
- VirtualProtectEx
- ReadProcessMemory
- WriteProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- WideCharToMultiByte
- VirtualAlloc
- RtlMoveMemory
- ZwUnmapViewOfSection
- GetModuleHandleA
- GetTopWindow
- RaiseException
- GetCommandLineA
- GetCurrentDirectoryA
- CryptHashData
- GetEnvironmentStringsW
- GetLastError
- RegDeleteKeyA
- InterlockedIncrement
- RegEnumValueA
- CreateWaitableTimerA
- GetLastActivePopup
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- GetStartupInfoA
- LoadLibraryA
- GetVersionExA

- SetHandleCount
- EnterCriticalSection
- LeaveCriticalSection
- GetLocaleInfoA
- RegDeleteValueA
- RegSetValueExA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA
- RegQueryValueExA
- InitializeCriticalSection
- SetLastError
- MsgWaitForMultipleObjects
- InterlockedDecrement
- GetEnvironmentVariableA
- GetActiveWindow
- GetStringTypeW
- GetUserNameA
- GetStringTypeA
- SetStdHandle
- RegOpenKeyExA
- FreeEnvironmentStringsW
- DispatchMessageA
- DeleteCriticalSection
- RegCreateKeyA
- WaitForSingleObject
- GetStdHandle

- **Module 2 other strings**

- 532A4C47797E747F67634C43696364757D23224C7371737C633E7568753375AEC2A
- TotalVisibleMemorySize
- 7371737C633E756875133197F87
- CoInitialize
- OSProductSuite
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CEE14A4A29
- FreeVirtualMemory
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CEE14A4A29
- GAIsProcessorFeaturePresent
- 1, 3, 0, 1209
- {4590f811-1d3a-11d0-891f-00aa004b2e24}
- LiveUpd360.dll
- - unexpected heap error
- FileDescription
- CoUninitialize
- ProductVersion
- CoInitializeEx
- PortableOperatingSystem
- "@0123456789ABCDEF
- TotalSwapSpaceSize
- ServicePackMajorVersion
- advapi32.dll
- SystemDirectory
-
- kernel32.dll

- DataExecutionPrevention_Available
- FreePhysicalMemory
- 732A4C67797E747F67634C28202020F5B366961
- OtherTypeDescription
- DataExecutionPrevention_32BitApplications
- ServicePackMinorVersion
- oleaut32.dll
- CoInitializeSecurity
- Organization
- EncryptionLevel
- TotalVirtualMemorySize
- >>:74-./
- OperatingSystemSKU
- SystemDevice
- MaxProcessMemorySize
- WindowsDirectory
- MS Shell Dlg
- __MSVCRT_HEAP_SELECT

Extra Information Recovered

In this section there is additional information recovered by platform plugins

- **DecryptedString**

http://

/ca.php

?m=

&h;=

GET

?p

POST

users.qzone.qq.com

GET /fcg-bin/cgi_get_portrait.fcg?uins=

HTTP/1.1
Host: users.qzone.qq.com
Connection: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36

Date:

GMT

function lakwi(){var st = '

';var t2 = Date.parse(new Date(st))/1000;return t2;}

ScriptControl

Language

JScript

ExecuteStatement

Run

lakwi

Software\\Microsoft\\Internet Explorer\\Main\\Start Page

www.naver.com

0.0.0.0

.com.opx

.kr

.kr.opx

ET

step_down.php?key=8c542178bbf0bd79

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: text/plain
Content-Length:
```

VBScript

```
Function MACAddress()
Dim mc,mo
Set mc=GetObject("Winmgmts:").InstancesOf("Win32_NetworkAdapterConfiguration")
For Each mo In mc
If mo.IPEnabled=True Then
MACAddress= mo.MacAddress
Exit For
End If
```

MACAddress

WinHttp.WinHttpRequest.5.1

Open

Send

responseBody

Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\AutoConfigURL

http://127.0.0.1:

CreateObject("Scripting.FileSystemObject").CopyFolder "{tmp}","{tmp_}"

AddCode

Applications\\zipfldr.dll\\NoOpenWith

regsvr32 /s zipfldr.dll

```
zip


Error


Sub run(ByVal A, ByVal B)
Set fso = CreateObject("Scripting.FileSystemObject")
If fso.GetExtensionName(B) <> "zip" Then
Exit Sub
ElseIf fso.FolderExists(A) Then
FType = "Folder"
ElseIf fso.FileExists(A) Then


Line


ConnId


ProxyId
```

Configs Recovered

In this section there are malware configs recovered by platform plugins