Sample: 2e97c8191fcd94bfc77cea13b9eea463

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 07:59:02 (p3pperp0tts platform's analysis date)

Exe timestamp: 2016-03-20 07:23:34 (timestamp of the original sample)

Unpacked mods max timestamp: 2016-03-20 07:23:34 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2018-05-21 16:10:34 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: 2e97c8191fcd94bfc77cea13b9eea463

AV detections

- Microsoft: VirTool:Win32/Injector
- Kaspersky: HEUR:Trojan.Win32.Generic
- Symantec: Trojan Horse
- Malwarebytes:

Source

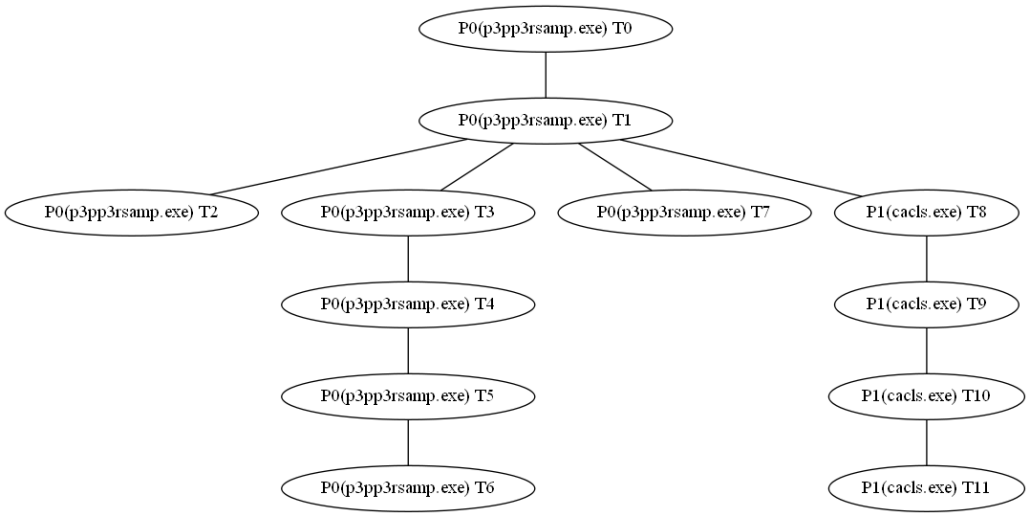
-

Virustotal

- https://virustotal.com/es/file/5e1ca094e11b2dcfdd4c729e2eaf1bdfd0ec84067a39f1c3a233bfff1ff6dcb5/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 (HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\UNCAsIntranet Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\AutoDetect Type: REG_DWORD, Length: 4, Data: 1)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32 Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
- RegCreateKey (HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings Desired Access: Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ProxyEnable Type: REG_DWORD, Length: 4, Data: 0)
- RegCreateKey (HKCU\\Software\\Microsoft\\windows\\CurrentVersion\\Internet Settings\\Connections Desired Access: Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections\\SavedLegacySettings Type: REG_BINARY, Length: 472, Data: 46 00 00 00 07 00 00 00 09 00 00 00 00 00 00 00)
- Process Create (C:\\Windows\\system32\\cacls.exe PID: P1, Command line: C:\\Windows\\System32\\cacls.exe)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\uki4Kk2o Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)

• RegCreateKey (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0} Desired Access: Set Value, Create Sub Key, Enumerate Sub Keys, Disposition: REG_OPENED_EXISTING_KEY)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0}\\WpadDecisionReason Type: REG_DWORD, Length: 4, Data: 1)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0}\\WpadDecisionTime Type: REG_BINARY, Length: 8, Data: 10 D6 93 34 FA DA D4 01)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0}\\WpadDecision Type: REG_DWORD, Length: 4, Data: 3)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0}\\WpadNetworkName Type: REG_SZ, Length: 22, Data: Network 7)
• RegCreateKey (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95 Desired Access: Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95\\WpadDecisionReason Type: REG_DWORD, Length: 4, Data: 1)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95\\WpadDecisionTime Type: REG_BINARY, Length: 8, Data: 10 D6 93 34 FA DA D4 01)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95\\WpadDecision Type: REG_DWORD, Length: 4, Data: 3)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections\\DefaultConnectionSettings Type: REG_BINARY, Length: 312, Data: 46 00 00 00 04 00 00 00 09 00 00 00 00 00 00 00)
• RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\WpadLastNetwork Type: REG_SZ, Length: 78, Data: {B900EE6D-B82B-4345-8AA5-C861F6DBBAB0})
• 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)
• RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\ProxyBypass)
• RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\ProxyBypass)
• RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\IntranetName)
• RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\IntranetName)
• Thread Create (Thread ID: T3)
• RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ProxyServer)
• RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ProxyOverride)
• RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\AutoConfigURL)
• Thread Create (Thread ID: T7)
• Thread Create (Thread ID: TUNKALIAS)
• Thread Create (Thread ID: T4)
• Thread Create (Thread ID: T5)
• Thread Create (Thread ID: T6)
• Thread Create (Thread ID: T9)
• Thread Create (Thread ID: T10)
• Thread Create (Thread ID: T11)

Most interesting strings

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

- <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
- <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
- !This program cannot be run in DOS mode.
- abnormal program termination
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- c:\\windows\\notepad.exe
- REG_MULTI_SZ -
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- REG_REG_EXPAND_SZ -
- commctrl_DragListMsg
- DOMAIN error
- IsBadReadPtr
- CallWindowProcA
- ClosePrinter
- RootGenius.exe
- C:\\Users\\Administrator\\Desktop
- OriginalFilename
- CMapPtrToPtr
- PathFileExistsA
- StringFileInfo
- WritePrivateProfileStringA
- GetEnvironmentStrings
- FileTimeToLocalFileTime
- GetSysColorBrush
- GlobalUnlock
- _`abcdefgh@i?jk
- LCMapStringA
- - not enough space for lowio initialization
- GlobalDeleteAtom
- GetCurrentThreadId
- Microsoft Visual C++ Runtime Library
- <program name unknown>
- CryptGetHashParam
- CryptDestroyHash
- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- GetMessageTime
- - unable to open console device
- GetProcAddress
- _lmnopqrs$tuvwx
- <requestedPrivileges>
- </requestedPrivileges>
- SetWindowLongA
- SetErrorMode
- InternalName
- Process32First
- LCMapStringW
- OpenFileMappingA
- GetDeviceCaps
- CryptCreateHash
- DefWindowProcA

- IsBadWritePtr
- VS_VERSION_INFO
- SetWaitableTimer
- </trustInfo>
- runtime error
- PreviewPages
- MonitorFromPoint
- SetUnhandledExceptionFilter
- TerminateProcess
- GetWindowLongA
- RegisterClassA
- GlobalAddAtomA
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- SetFilePointer
- - unable to initialize heap
- 6789:;<=>?@ABCD
- deleted; expires=Fri, 1-Jan-1999 1:1:1 GMT; path=/;
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- EnumDisplayMonitors
- - not enough space for thread data
- FlushFileBuffers
- GlobalFindAtomA
- JanFebMarAprMayJunJulAugSepOctNovDec
- GetCurrentThread
- DocumentPropertiesA
- Copyright 2016
- D*)''+(**#&+&'*')&&&*((.(-%(&*')(((((')UG
- SetFileAttributesA
- - unexpected multithread lock error
- InterlockedExchange
- - floating point not loaded
- LegalCopyright
- UnregisterClassA
- GetDlgCtrlID
- GetMenuItemID
- SetMenuItemBitmaps
- - pure virtual function call
- STUVW$#0XYZ[\\]^
- GetClassLongA
- WindowFromPoint
- __GLOBAL_HEAP_SELECTED
- i"`B+))***)++***(+),)+$*%-).*+))(*pT
- GetCurrentProcess
- FreeEnvironmentStringsA
- PostQuitMessage
- IsBadCodePtr
- - not enough space for arguments
- FileTimeToSystemTime
- - not enough space for environment
- .?AVCCmdTarget@@
- CreateProcessA
- abcdefghijklmnopqrstuvwxyz
- .?AV_AFX_WIN_STATE@@

- .?AV_AFX_BASE_MODULE_STATE@@
- HKEY_CURRENT_USER
- .?AVtype_info@@
- BlackMoon RunTime Error:
- .?AVAFX_MODULE_THREAD_STATE@@
- .?AVCMapPtrToPtr@@
- program internal error number is %d.
- U^,NeAc')QVxa)
- HKEY_LOCAL_MACHINE
- .?AV_AFX_THREAD_STATE@@
- HKEY_CLASSES_ROOT
- REG_BINARY -
- SystemTimeToVariantTime
- ResumeThread
- REG_DWORD - DWORD
- .?AV_AFX_CTL3D_THREAD@@
- .?AVCTempMenu@@
- .?AVCWinThread@@
- MapViewOfFile
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WideCharToMultiByte
- GetAsyncKeyState
- CallNextHookEx
- GetForegroundWindow
- VirtualAllocEx
- GetThreadContext
- SetThreadContext
- VirtualProtectEx
- ReadProcessMemory
- WriteProcessMemory
- InternetSetCookieA
- InternetGetCookieExA
- InternetGetCookieA
- GetMenuCheckMarkDimensions
- VirtualAlloc
- CloseClipboard
- GetClassNameA
- RtlMoveMemory
- SendMessageA
- MonitorFromRect
- MonitorFromWindow
- GetProcessVersion
- IsWindowVisible
- GetModuleHandleA
- EnableMenuItem
- RaiseException
- SystemParametersInfoA
- PostMessageA
- LocalReAlloc
- GetCommandLineA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- UnhookWindowsHookEx
- GetEnvironmentStringsW
- CryptHashData

- GlobalGetAtomNameA
- GetTopWindow
- RegDeleteValueA
- GetLastError
- EmptyClipboard
- RegDeleteKeyA
- OpenClipboard
- RegEnumValueA
- GetMenuItemCount
- SetWindowsHookExA
- CreateWaitableTimerA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- CryptReleaseContext
- GetProcessHeap
- LeaveCriticalSection
- GetSystemMetrics
- LoadLibraryA
- GetVersionExA
- RegisterWindowMessageA
- GetMonitorInfoA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- GetCursorPos
- RegSetValueExA
- GetWindowRect
- CreateWindowExA
- TabbedTextOutA
- GetStartupInfoA
- GetWindowPlacement
- SetClipboardData
- IsWindowEnabled
- PeekMessageA
- MapWindowPoints
- EnableWindow
- GetModuleFileNameA
- RegCreateKeyExA
- GetMenuState
- RegQueryValueExA
- GetEnvironmentVariableA
- SetLastError
- GetWindowTextA
- MsgWaitForMultipleObjects
- InterlockedDecrement
- GlobalHandle
- InitializeCriticalSection
- GetActiveWindow
- GetStringTypeW
- GetNextDlgTabItem
- GetClientRect
- GetStringTypeA
- GetClassInfoA
- SetStdHandle
- RegOpenKeyExA

- FreeEnvironmentStringsW
- CryptAcquireContextA
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- ValidateRect
- RegCreateKeyA
- DestroyWindow
- GetStdHandle
- SetForegroundWindow
- FindNextFileA
- FindFirstFileA
- ZwUnmapViewOfSection
- WaitForSingleObject

Hosts

- 203.205.151.50:http
- google-public-dns-a.google.com:domain
- 192.168.149.168:49159
- 203.205.151.50:80

Dns queries

- isatap.localdomain ---> no answers
- 254.149.168.192.in-addr.arpa ---> no answers
- users.qzone.qq.com ---> no answers
- 8.8.8.8.in-addr.arpa ---> no answers
- dns.msftncsi.com ---> 131.107.255.255

Network traffic

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

- **tcp 192.168.149.168:49159 ---> 203.205.151.50:80**

  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36[...]Host: users.qzone.qq.com[...]GET /fcg-bin/cgi_get_portrait.fcg?uins=1293362886 HTTP/1.1[...]Connection: Keep-Alive

- **tcp 203.205.151.50:80 ---> 192.168.149.168:49159**

  <h1>301 Moved Permanently</h1> [...]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 [...]Location: https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=1293362886[...]Date: Fri, 15 Mar 2019 06:43:08 GMT[...]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.

- <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
- <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
- !This program cannot be run in DOS mode.
- abnormal program termination
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- c:\\windows\\notepad.exe
- REG_MULTI_SZ -
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- REG_REG_EXPAND_SZ -
- commctrl_DragListMsg
- DOMAIN error
- IsBadReadPtr
- CallWindowProcA
- ClosePrinter
- RootGenius.exe
- C:\\Users\\Administrator\\Desktop
- OriginalFilename
- CMapPtrToPtr
- PathFileExistsA
- StringFileInfo
- WritePrivateProfileStringA
- GetEnvironmentStrings
- FileTimeToLocalFileTime
- GetSysColorBrush
- GlobalUnlock
- _`abcdefgh@i?jk
- LCMapStringA
- - not enough space for lowio initialization
- GlobalDeleteAtom
- GetCurrentThreadId
- Microsoft Visual C++ Runtime Library
- <program name unknown>
- CryptGetHashParam
- CryptDestroyHash
- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- GetMessageTime
- - unable to open console device
- GetProcAddress
- _lmnopqrs$tuvwx
- <requestedPrivileges>
- </requestedPrivileges>
- SetWindowLongA
- SetErrorMode
- InternalName
- Process32First
- LCMapStringW
- OpenFileMappingA
- GetDeviceCaps
- CryptCreateHash
- DefWindowProcA

- IsBadWritePtr
- VS_VERSION_INFO
- SetWaitableTimer
- </trustInfo>
- runtime error
- PreviewPages
- MonitorFromPoint
- SetUnhandledExceptionFilter
- TerminateProcess
- GetWindowLongA
- RegisterClassA
- GlobalAddAtomA
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- SetFilePointer
- - unable to initialize heap
- 6789:;<=>?@ABCD
- deleted; expires=Fri, 1-Jan-1999 1:1:1 GMT; path=/;
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- EnumDisplayMonitors
- - not enough space for thread data
- FlushFileBuffers
- GlobalFindAtomA
- JanFebMarAprMayJunJulAugSepOctNovDec
- GetCurrentThread
- DocumentPropertiesA
- Copyright 2016
- D*)''+(**#&+&'*')&&&*((.(-%(&*')(((((')UG
- SetFileAttributesA
- - unexpected multithread lock error
- InterlockedExchange
- - floating point not loaded
- LegalCopyright
- UnregisterClassA
- GetDlgCtrlID
- GetMenuItemID
- SetMenuItemBitmaps
- - pure virtual function call
- STUVW$#0XYZ[\\]^
- GetClassLongA
- WindowFromPoint
- __GLOBAL_HEAP_SELECTED
- i"`B+))***)++***(+),)+$*%-).*+))(*pT
- GetCurrentProcess
- FreeEnvironmentStringsA
- PostQuitMessage
- IsBadCodePtr
- - not enough space for arguments
- FileTimeToSystemTime
- - not enough space for environment
- .?AVCCmdTarget@@
- CreateProcessA
- abcdefghijklmnopqrstuvwxyz
- .?AV_AFX_WIN_STATE@@

- .?AV_AFX_BASE_MODULE_STATE@@
- HKEY_CURRENT_USER
- .?AVtype_info@@
- BlackMoon RunTime Error:
- .?AVAFX_MODULE_THREAD_STATE@@
- .?AVCMapPtrToPtr@@
- program internal error number is %d.
- U^,NeAc')QVxa)
- HKEY_LOCAL_MACHINE
- .?AV_AFX_THREAD_STATE@@
- HKEY_CLASSES_ROOT
- REG_BINARY -
- SystemTimeToVariantTime
- ResumeThread
- REG_DWORD - DWORD
- .?AV_AFX_CTL3D_THREAD@@
- .?AVCTempMenu@@
- .?AVCWinThread@@
- MapViewOfFile
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WideCharToMultiByte
- GetAsyncKeyState
- CallNextHookEx
- GetForegroundWindow
- VirtualAllocEx
- GetThreadContext
- SetThreadContext
- VirtualProtectEx
- ReadProcessMemory
- WriteProcessMemory
- InternetSetCookieA
- InternetGetCookieExA
- InternetGetCookieA
- GetMenuCheckMarkDimensions
- VirtualAlloc
- CloseClipboard
- GetClassNameA
- RtlMoveMemory
- SendMessageA
- MonitorFromRect
- MonitorFromWindow
- GetProcessVersion
- IsWindowVisible
- GetModuleHandleA
- EnableMenuItem
- RaiseException
- SystemParametersInfoA
- PostMessageA
- LocalReAlloc
- GetCommandLineA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- UnhookWindowsHookEx
- GetEnvironmentStringsW
- CryptHashData

- GlobalGetAtomNameA
- GetTopWindow
- RegDeleteValueA
- GetLastError
- EmptyClipboard
- RegDeleteKeyA
- OpenClipboard
- RegEnumValueA
- GetMenuItemCount
- SetWindowsHookExA
- CreateWaitableTimerA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- CryptReleaseContext
- GetProcessHeap
- LeaveCriticalSection
- GetSystemMetrics
- LoadLibraryA
- GetVersionExA
- RegisterWindowMessageA
- GetMonitorInfoA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- GetCursorPos
- RegSetValueExA
- GetWindowRect
- CreateWindowExA
- TabbedTextOutA
- GetStartupInfoA
- GetWindowPlacement
- SetClipboardData
- IsWindowEnabled
- PeekMessageA
- MapWindowPoints
- EnableWindow
- GetModuleFileNameA
- RegCreateKeyExA
- GetMenuState
- RegQueryValueExA
- GetEnvironmentVariableA
- SetLastError
- GetWindowTextA
- MsgWaitForMultipleObjects
- InterlockedDecrement
- GlobalHandle
- InitializeCriticalSection
- GetActiveWindow
- GetStringTypeW
- GetNextDlgTabItem
- GetClientRect
- GetStringTypeA
- GetClassInfoA
- SetStdHandle
- RegOpenKeyExA

- FreeEnvironmentStringsW
- CryptAcquireContextA
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- ValidateRect
- RegCreateKeyA
- DestroyWindow
- GetStdHandle
- SetForegroundWindow
- SelectObject
- CArchiveException
- FileDescription
- oleaut32.dll
- SetViewportOrgEx
- 532A4C47797E747F67634C43696364757D23224C7371737C633E756875E8F9E6128
- SetTextColor
- IPHLPAPI.DLL
- AXYT3R8AFHF9E9F
- 732A4C67797E747F67634C282020207367AEF5A
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4C8AAE76796
- CTempGdiObject
- AfxOleControl42s
- GAIsProcessorFeaturePresent
- 877018489400
- GetStockObject
- CreateBitmap
- AfxFrameOrView42s
- CResourceException
- 7371737C633E756875CB269016C
- - unexpected heap error
- 980418011502
- CStringArray
- DeleteObject
- winspool.drv
- AfxMDIFrame42s
- CUserException
- 43USBAEUIA8NA8762
- VB7547TS87HNC8
- advapi32.dll
- sef97d54y6uidrt87ddvgsd8fse76w4brs8
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E644675626
3797F7E4C42657ED43368AD2
- OffsetViewportOrgEx
- kernel32.dll
- ProductVersion
- CMemoryException
- comctl32.dll
- SetViewportExtEx
- CNotSupportedException
- SetWindowExtEx
- InitCommonControlsEx
- ScaleViewportExtEx
- AfxControlBar42s
- i0v@;3vxB/v.a-v
- ScaleWindowExtEx

- COMDLG32.dll
- 908998720014
- OpenPrinterA
- AfxOldWndProc423
- ,-./0$120345
- SDF74THS8XN843
- FindNextFileA
- FindFirstFileA
- ZwUnmapViewOfSection
- WaitForSingleObject
- U:j%qV7D_i6R2
- .?AUCThreadData@@
- .?AVCHandleMap@@
- .?AVCMemoryException@@
- .PAVCException@@
- .?AV_AFX_CTL3D_STATE@@
- .?AVCNotSupportedException@@
- .?AVCGdiObject@@
- .?AVCCmdUI@@
- .PAVCObject@@
- .?AVCObject@@
- .?AVCStringArray@@
- .?AVCTestCmdUI@@
- "@0123456789ABCDEF
- .?AVCUserException@@
- .?AVCArchiveException@@
- .?AVCNoTrackObject@@
- .?AVCResourceException@@
- .?AVCException@@
- .?AVCWinApp@@
- .PAVCArchiveException@@
- .PAVCMemoryException@@
- .?AVCSimpleException@@
- .?AVAFX_MODULE_STATE@@
- .?AVCTempGdiObject@@
- .PAVCSimpleException@@
- Wwuupsqzwyzwyyvxwwwxqtwtvwtvwuuxvvwwwxstytvd
- m0v$\\.v+d-v*k0v
- wvxqrprqssqpsuvrrrpppqsspppqqqpppsqqpppprrr
- __MSVCRT_HEAP_SELECT
- Y-*,,)+******+++(+)-++++++++,,,*+)UF%
- o"I3,+-,\'))))+,*-++)++.,,$)\'-).\'))\')*J?#
- EFGHIJKLMNOPQ@R
- c'A4+))*)%******+++')*%'(wqj
- i&@3-(**(((&%)'&+(*%(,-*,()-'%$
- .?AVCTempWnd@@
- .?AVCTempDC@@

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 T7 (in process P0, p3pp3rsamp.exe)
    - Thread T8 (in process P1, cacls.exe)
  - **Thread' events**
    - RegCreateKey (HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - Thread Create (Thread ID: T2)
    - RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\ProxyBypass)
    - RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\ProxyBypass)
    - RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\IntranetName)
    - RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\IntranetName)
    - RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\UNCAsIntranet Type: REG_DWORD, Length: 4, Data: 0)
    - RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\AutoDetect Type: REG_DWORD, Length: 4, Data: 1)
    - RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\ProxyBypass)
    - RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\ProxyBypass)
    - RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\IntranetName)
    - RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\IntranetName)
    - RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\UNCAsIntranet Type: REG_DWORD, Length: 4, Data: 0)
    - RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\AutoDetect Type: REG_DWORD, Length: 4, Data: 1)
    - Thread Create (Thread ID: T3)
    - RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32 Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)

- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
- RegCreateKey (HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings Desired Access: Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ProxyEnable Type: REG_DWORD, Length: 4, Data: 0)
- RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ProxyServer)
- RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ProxyOverride)
- RegDeleteValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\AutoConfigURL)
- RegCreateKey (HKCU\\Software\\Microsoft\\windows\\CurrentVersion\\Internet Settings\\Connections Desired Access: Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections\\SavedLegacySettings Type: REG_BINARY, Length: 472, Data: 46 00 00 00 07 00 00 00 09 00 00 00 00 00 00 00)
- Thread Create (Thread ID: T7)
- Process Create (C:\\Windows\\system32\\cacls.exe PID: P1, Command line: C:\\Windows\\System32\\cacls.exe)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\uki4Kk2o Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)

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

Thread's childs

- No childs found

Thread' events

- Thread Create (Thread ID: TUNKALIAS)

Thread T3 (in process P0, p3pp3rsamp.exe) description

Thread's childs

- Thread T4 (in process P0, p3pp3rsamp.exe)

Thread' events

- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)

- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
- Thread Create (Thread ID: T4)

- **Thread T4 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T5 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T5)
- **Thread T5 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T6 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T6)
- **Thread T6 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)
- **Thread T7 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create (Thread ID: TUNKALIAS)
    - RegCreateKey (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0} Desired Access: Set Value, Create Sub Key, Enumerate Sub Keys, Disposition: REG_OPENED_EXISTING_KEY)
    - RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0}\\WpadDecisionReason Type: REG_DWORD, Length: 4, Data: 1)

- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0}\\WpadDecisionTime Type: REG_BINARY, Length: 8, Data: 10 D6 93 34 FA DA D4 01)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0}\\WpadDecision Type: REG_DWORD, Length: 4, Data: 3)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\{B900EE6D-B82B-4345-8AA5-C861F6DBBAB0}\\WpadNetworkName Type: REG_SZ, Length: 22, Data: Network 7)
- RegCreateKey (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95 Desired Access: Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95\\WpadDecisionReason Type: REG_DWORD, Length: 4, Data: 1)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95\\WpadDecisionTime Type: REG_BINARY, Length: 8, Data: 10 D6 93 34 FA DA D4 01)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95\\WpadDecision Type: REG_DWORD, Length: 4, Data: 3)
- RegCreateKey (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\00-50-56-e8-06-95 Desired Access: Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\windows\\CurrentVersion\\Internet Settings\\Connections Desired Access: Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections\\DefaultConnectionSettings Type: REG_BINARY, Length: 312, Data: 46 00 00 00 04 00 00 00 09 00 00 00 00 00 00 00)
- RegSetValue (HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad\\WpadLastNetwork Type: REG_SZ, Length: 78, Data: {B900EE6D-B82B-4345-8AA5-C861F6DBBAB0})

- **Thread T8 (in process P1, cacls.exe) description**
  - **Thread's childs**
    - Thread T9 (in process P1, cacls.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T9)
- **Thread T9 (in process P1, cacls.exe) description**
  - **Thread's childs**
    - Thread T10 (in process P1, cacls.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T10)
    - 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: TUNKALIAS)
- **Thread T10 (in process P1, cacls.exe) description**
  - **Thread's childs**
    - Thread T11 (in process P1, cacls.exe)

- **Thread' events**
  - Thread Create (Thread ID: T11)

- **Thread T11 (in process P1, cacls.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 (cacls.exe)'s network events

- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- 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 (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- 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 (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- 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 (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- 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 (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- 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 (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- 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 (36))
- 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 (447))
- 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**
    - 44616e530000000000000000000000006f1f0b00090000006f1f0a00060000007b1c0c0003000000c30f5f0004000000831c0e00200000003
      6260a00890000083085d0002000000c30f5d00210000000000010006020000362 60b00740000000000000001000000e81f0b00
  - **Module 1 strings**
    - **Module 1 most interesting strings**
      - <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
      - <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
      - !This program cannot be run in DOS mode.
      - abnormal program termination
      - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
      - c:\\windows\\notepad.exe
      - commctrl_DragListMsg
      - DOMAIN error
      - IsBadReadPtr
      - CallWindowProcA
      - ClosePrinter
      - RootGenius.exe
      - C:\\Users\\Administrator\\Desktop
      - OriginalFilename
      - CMapPtrToPtr
      - PathFileExistsA
      - StringFileInfo
      - WritePrivateProfileStringA
      - GetEnvironmentStrings
      - FileTimeToLocalFileTime
      - GetSysColorBrush
      - GlobalUnlock
      - _`abcdefgh@i?jk
      - LCMapStringA
      - - not enough space for lowio initialization
      - GlobalDeleteAtom
      - GetCurrentThreadId
      - Microsoft Visual C++ Runtime Library
      - <program name unknown>
      - CryptGetHashParam
      - CryptDestroyHash
      - - not enough space for _onexit/atexit table
      - SunMonTueWedThuFriSat
      - GetMessageTime
      - - unable to open console device
      - GetProcAddress
      - _lmnopqrs$tuvwx
      - <requestedPrivileges>
      - </requestedPrivileges>
      - SetWindowLongA

- SetErrorMode
- InternalName
- Process32First
- LCMapStringW
- OpenFileMappingA
- GetDeviceCaps
- CryptCreateHash
- DefWindowProcA
- IsBadWritePtr
- VS_VERSION_INFO
- SetWaitableTimer
- </trustInfo>
- runtime error
- PreviewPages
- MonitorFromPoint
- SetUnhandledExceptionFilter
- TerminateProcess
- GetWindowLongA
- RegisterClassA
- GlobalAddAtomA
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- SetFilePointer
- - unable to initialize heap
- 6789:;<=>?@ABCD
- deleted; expires=Fri, 1-Jan-1999 1:1:1 GMT; path=/;
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- EnumDisplayMonitors
- - not enough space for thread data
- FlushFileBuffers
- GlobalFindAtomA
- JanFebMarAprMayJunJulAugSepOctNovDec
- GetCurrentThread
- DocumentPropertiesA
- Copyright 2016
- D*)''+(**#&+&'*')&&&*((.(-%(&*')((((')UG
- SetFileAttributesA
- - unexpected multithread lock error
- InterlockedExchange
- - floating point not loaded
- LegalCopyright
- UnregisterClassA
- GetDlgCtrlID
- GetMenuItemID
- SetMenuItemBitmaps
- - pure virtual function call
- STUVW$#0XYZ[\\]^
- GetClassLongA
- WindowFromPoint
- __GLOBAL_HEAP_SELECTED
- i"`B+))***)++***(+),)+$*%-).*+))(*pT
- GetCurrentProcess
- FreeEnvironmentStringsA
- PostQuitMessage

- IsBadCodePtr
- - not enough space for arguments
- FileTimeToSystemTime
- - not enough space for environment
- MapViewOfFile
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WideCharToMultiByte
- GetAsyncKeyState
- CallNextHookEx
- GetForegroundWindow
- InternetSetCookieA
- InternetGetCookieExA
- InternetGetCookieA
- GetMenuCheckMarkDimensions
- VirtualAlloc
- CloseClipboard
- GetClassNameA
- RtlMoveMemory
- SendMessageA
- MonitorFromRect
- MonitorFromWindow
- GetProcessVersion
- IsWindowVisible
- GetModuleHandleA
- EnableMenuItem
- RaiseException
- SystemParametersInfoA
- PostMessageA
- LocalReAlloc
- GetCommandLineA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- UnhookWindowsHookEx
- GetEnvironmentStringsW
- CryptHashData
- GlobalGetAtomNameA
- GetTopWindow
- RegDeleteValueA
- GetLastError
- EmptyClipboard
- RegDeleteKeyA
- OpenClipboard
- RegEnumValueA
- GetMenuItemCount
- SetWindowsHookExA
- CreateWaitableTimerA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- CryptReleaseContext
- GetProcessHeap
- LeaveCriticalSection
- GetSystemMetrics
- LoadLibraryA

- GetVersionExA
- RegisterWindowMessageA
- GetMonitorInfoA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- GetCursorPos
- RegSetValueExA
- GetWindowRect
- CreateWindowExA
- TabbedTextOutA
- GetStartupInfoA
- GetWindowPlacement
- SetClipboardData
- IsWindowEnabled
- PeekMessageA
- MapWindowPoints
- EnableWindow
- GetModuleFileNameA
- RegCreateKeyExA
- GetMenuState
- RegQueryValueExA
- GetEnvironmentVariableA
- SetLastError
- GetWindowTextA
- MsgWaitForMultipleObjects
- InterlockedDecrement
- GlobalHandle
- InitializeCriticalSection
- GetActiveWindow
- GetStringTypeW
- GetNextDlgTabItem
- GetClientRect
- GetStringTypeA
- GetClassInfoA
- SetStdHandle
- RegOpenKeyExA
- FreeEnvironmentStringsW
- CryptAcquireContextA
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- ValidateRect
- RegCreateKeyA
- DestroyWindow
- GetStdHandle
- SetForegroundWindow

- **Module 1 other strings**

- SelectObject
- CArchiveException
- FileDescription
- oleaut32.dll
- SetViewportOrgEx

- 532A4C47797E747F67634C43696364757D23224C7371737C633E756875E8F9E6128
- SetTextColor
- IPHLPAPI.DLL
- AXYT3R8AFHF9E9F
- 732A4C67797E747F67634C282020207367AEF5A
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4C8AAE76796
- CTempGdiObject
- AfxOleControl42s
- GAIsProcessorFeaturePresent
- 877018489400
- GetStockObject
- CreateBitmap
- AfxFrameOrView42s
- CResourceException
- 7371737C633E756875CB269016C
- - unexpected heap error
- 980418011502
- CStringArray
- DeleteObject
- winspool.drv
- AfxMDIFrame42s
- CUserException
- 43USBAEUIA8NA8762
- VB7547TS87HNC8
- advapi32.dll
- sef97d54y6uidrt87ddvgsd8fse76w4brs8
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657ED43368AD2
- OffsetViewportOrgEx
- kernel32.dll
- ProductVersion
- CMemoryException
- comctl32.dll
- SetViewportExtEx
- CNotSupportedException
- SetWindowExtEx
- InitCommonControlsEx
- ScaleViewportExtEx
- AfxControlBar42s
- i0v@;3vxB/v.a-v
- ScaleWindowExtEx
- COMDLG32.dll
- 908998720014
- OpenPrinterA
- AfxOldWndProc423
- ,-./0$120345
- SDF74THS8XN843
- Wwuupsqzwyzwyyvxwwwxqtwtvwtvwuuxvvwwwxstytvd
- m0v$\\.v+d-v*k0v
- wvxqrprqssqpsuvrrrpppqsspppqqqpppsqqpppprrr
- __MSVCRT_HEAP_SELECT
- Y-*,,)+******+++(+)-++++++++,,,*+)UF%
- o"I3,+-,\'))))+,*-++)++.,,$)\'-).\'))\')*J?#
- EFGHIJKLMNOPQ@R
- c'A4+))*)%******+++')*%'(wqj
- i&@3-(**(((&%)'&+(*%(,-*,()-'%$

- **Module 2 (probably unpacked / injected by the sample)**
  - **Module 2 rich signatures**
    - 44616e530000000000000000000000006f1f0b00090000006f1f0a00060000007b1c0c0003000000c30f5f00040000000831c0e00200000003
      6260a00890000008308 5d0002000000c30f5d00210000000000010006020000362 60b00740000000000000001000000e81f0b00
  - **Module 2 strings**
    - **Module 2 most interesting strings**
      - REG_MULTI_SZ -
      - C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
      - <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
      - <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
      - !This program cannot be run in DOS mode.
      - abnormal program termination
      - REG_REG_EXPAND_SZ -
      - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
      - c:\\windows\\notepad.exe
      - commctrl_DragListMsg
      - DOMAIN error
      - IsBadReadPtr
      - CallWindowProcA
      - ClosePrinter
      - .?AVCCmdTarget@@
      - CreateProcessA
      - C:\\Users\\Administrator\\Desktop
      - OriginalFilename
      - CMapPtrToPtr
      - <requestedPrivileges>
      - PathFileExistsA
      - StringFileInfo
      - WritePrivateProfileStringA
      - GetEnvironmentStrings
      - FileTimeToLocalFileTime
      - abcdefghijklmnopqrstuvwxyz
      - GetSysColorBrush
      - GlobalUnlock
      - _`abcdefgh@i?jk
      - LCMapStringA
      - - not enough space for lowio initialization
      - GlobalDeleteAtom
      - .?AV_AFX_WIN_STATE@@
      - GetCurrentThreadId
      - Microsoft Visual C++ Runtime Library
      - .?AV_AFX_BASE_MODULE_STATE@@
      - <program name unknown>
      - CryptGetHashParam
      - HKEY_CURRENT_USER
      - CryptDestroyHash
      - - not enough space for _onexit/atexit table
      - SunMonTueWedThuFriSat
      - GetMessageTime

- - unable to open console device
- GetProcAddress
- _lmnopqrs$tuvwx
- </requestedPrivileges>
- SetWindowLongA
- SetErrorMode
- InternalName
- Process32First
- LCMapStringW
- OpenFileMappingA
- GetDeviceCaps
- CryptCreateHash
- .?AVtype_info@@
- DefWindowProcA
- BlackMoon RunTime Error:
- IsBadWritePtr
- VS_VERSION_INFO
- .?AVAFX_MODULE_THREAD_STATE@@
- .?AVCMapPtrToPtr@@
- program internal error number is %d.
- SetWaitableTimer
- </trustInfo>
- runtime error
- PreviewPages
- i"`B+))***)++***(+),)+$*%-).*+))(*pT
- MonitorFromPoint
- SetUnhandledExceptionFilter
- U^,NeAc')QVxa)
- TerminateProcess
- GetWindowLongA
- HKEY_LOCAL_MACHINE
- RegisterClassA
- GlobalAddAtomA
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- .?AV_AFX_THREAD_STATE@@
- SetFilePointer
- - unable to initialize heap
- 6789:;<=>?@ABCD
- deleted; expires=Fri, 1-Jan-1999 1:1:1 GMT; path=/;
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- EnumDisplayMonitors
- - not enough space for thread data
- RootGenius.exe
- FlushFileBuffers
- GlobalFindAtomA
- JanFebMarAprMayJunJulAugSepOctNovDec
- GetCurrentThread
- HKEY_CLASSES_ROOT
- DocumentPropertiesA
- Copyright 2016
- REG_BINARY -
- SystemTimeToVariantTime
- ResumeThread

- SetFileAttributesA
- - unexpected multithread lock error
- InterlockedExchange
- - floating point not loaded
- LegalCopyright
- UnregisterClassA
- GetDlgCtrlID
- REG_DWORD - DWORD
- GetMenuItemID
- SetMenuItemBitmaps
- - pure virtual function call
- STUVW$#0XYZ[\\]^
- GetClassLongA
- WindowFromPoint
- D*)''+(**#&+&'*')&&&*((.(-%(&*')((((')UG
- .?AV_AFX_CTL3D_THREAD@@
- .?AVCTempMenu@@
- __GLOBAL_HEAP_SELECTED
- GetCurrentProcess
- FreeEnvironmentStringsA
- .?AVCWinThread@@
- PostQuitMessage
- IsBadCodePtr
- - not enough space for arguments
- FileTimeToSystemTime
- - not enough space for environment
- MapViewOfFile
- VirtualAllocEx
- GetThreadContext
- SetThreadContext
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WriteProcessMemory
- WideCharToMultiByte
- GetAsyncKeyState
- CallNextHookEx
- GetForegroundWindow
- InternetSetCookieA
- InternetGetCookieExA
- InternetGetCookieA
- GetMenuCheckMarkDimensions
- VirtualAlloc
- CloseClipboard
- GetClassNameA
- RtlMoveMemory
- SendMessageA
- MonitorFromRect
- MonitorFromWindow
- GetProcessVersion
- IsWindowVisible
- GetModuleHandleA
- EnableMenuItem
- RaiseException
- SystemParametersInfoA

- PostMessageA
- LocalReAlloc
- GetCommandLineA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- UnhookWindowsHookEx
- GetEnvironmentStringsW
- CryptHashData
- GlobalGetAtomNameA
- GetTopWindow
- RegDeleteValueA
- GetLastError
- EmptyClipboard
- RegDeleteKeyA
- OpenClipboard
- RegEnumValueA
- GetMenuItemCount
- SetWindowsHookExA
- FindNextFileA
- CreateWaitableTimerA
- FindFirstFileA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- CryptReleaseContext
- GetProcessHeap
- ZwUnmapViewOfSection
- LeaveCriticalSection
- GetSystemMetrics
- LoadLibraryA
- GetVersionExA
- RegisterWindowMessageA
- GetMonitorInfoA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- GetCursorPos
- RegSetValueExA
- GetWindowRect
- CreateWindowExA
- TabbedTextOutA
- GetStartupInfoA
- GetWindowPlacement
- SetClipboardData
- IsWindowEnabled
- PeekMessageA
- MapWindowPoints
- EnableWindow
- GetModuleFileNameA
- RegCreateKeyExA
- GetMenuState
- RegQueryValueExA
- GetEnvironmentVariableA
- SetLastError
- GetWindowTextA
- MsgWaitForMultipleObjects

- InterlockedDecrement
- GlobalHandle
- InitializeCriticalSection
- GetActiveWindow
- GetStringTypeW
- GetNextDlgTabItem
- GetClientRect
- GetStringTypeA
- GetClassInfoA
- SetStdHandle
- RegOpenKeyExA
- FreeEnvironmentStringsW
- CryptAcquireContextA
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- ValidateRect
- RegCreateKeyA
- WaitForSingleObject
- DestroyWindow
- GetStdHandle
- SetForegroundWindow

- **Module 2 other strings**

- j%qV7D_i6R2
- .?AUCThreadData@@
- SelectObject
- CArchiveException
- FileDescription
- SetViewportOrgEx
- 532A4C47797E747F67634C43696364757D23224C7371737C633E756875E8F9E6128
- SetTextColor
- IPHLPAPI.DLL
- .?AVCHandleMap@@
- .?AVCMemoryException@@
- AXYT3R8AFHF9E9F
- 732A4C67797E747F67634C282020207367AEF5A
- .PAVCException@@
- .?AV_AFX_CTL3D_STATE@@
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4C8AAE76796
- CTempGdiObject
- AfxOleControl42s
- GAIsProcessorFeaturePresent
- 877018489400
- .?AVCNotSupportedException@@
- .?AVCGdiObject@@
- GetStockObject
- .?AVCCmdUI@@
- CreateBitmap
- AfxFrameOrView42s
- CResourceException
- 7371737C633E756875CB269016C
- - unexpected heap error
- .PAVCObject@@

- 980418011502
- .?AVCObject@@
- CStringArray
- .?AVCStringArray@@
- DeleteObject
- winspool.drv
- AfxMDIFrame42s
- .?AVCTestCmdUI@@
- CUserException
- "@0123456789ABCDEF
- 43USBAEUIA8NA8762
- VB7547TS87HNC8
- sef97d54y6uidrt87ddvgsd8fse76w4brs8
- .?AVCUserException@@
- .?AVCArchiveException@@
- .?AVCNoTrackObject@@
- .?AVCResourceException@@
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E644675626
3797F7E4C42657ED43368AD2
- OffsetViewportOrgEx
- .?AVCException@@
- advapi32.dll
- oleaut32.dll
- kernel32.dll
- ProductVersion
- CMemoryException
- .?AVCWinApp@@
- .PAVCArchiveException@@
- .PAVCMemoryException@@
- comctl32.dll
- SetViewportExtEx
- .?AVCSimpleException@@
- CNotSupportedException
- SetWindowExtEx
- InitCommonControlsEx
- .?AVAFX_MODULE_STATE@@
- ScaleViewportExtEx
- .?AVCTempGdiObject@@
- AfxControlBar42s
- i0v@;3vxB/v.a-v
- ScaleWindowExtEx
- .PAVCSimpleException@@
- COMDLG32.dll
- 908998720014
- OpenPrinterA
- AfxOldWndProc423
- ,-./0$120345
- SDF74THS8XN843
- Wwuupsqzwyzwyyvxwwwxqtwtvwtvwuuxvvwwwxstytvd
- .?AVCTempWnd@@
- m0v$\\.v+d-v*k0v
- wvxqrprqssqpsuvrrrpppqsspppqqqpppsqqpppprrr
- Y-*,,)+******+++(+)-++++++++,,,*+)UF%
- __MSVCRT_HEAP_SELECT
- .?AVCTempDC@@
- o"I3,+-,\'))))+,*-++)++.,,$)\'-).\'))\')*J?#
- EFGHIJKLMNOPQ@R

- `c'A4+))*)%******+++')*%'(wqj`
- `i&@3-(**(((&%)'&+(*%(,-*,()-'%$`

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.blw

.net

.net.blw

.kr

.kr.blw

ET

step_down.php?key=8cf34dd63915898b

```
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