

## **Sample: 1e9765081745e4328d52547c01427669**

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.

This work is licensed under a Creative Commons Attribution 4.0 International License. To view a copy of this license visit <http://creativecommons.org/licenses/by/4.0/>.

Classification: **#BANKER #BLACKMOON** (based on p3pperp0tts rules)

Analysis date: 2019-03-15 03:36:13 (p3pperp0tts platform's analysis date)

Exe timestamp: 2016-03-06 06:41:30 (timestamp of the original sample)

Unpacked mods max timestamp: 2016-03-06 06:41:30 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2016-03-17 08:09:54 (date of last time that the sample was analyzed at vt)

### **Index**

- [Sample](#)
- [AV detections](#)
- [Source](#)
- [Virustotal](#)
- [Threads tree](#)
- [Most Interesting behavior](#)
- [Most Interesting strings](#)
- [Hosts](#)
- [Dns queries](#)
- [Network traffic](#)
- [Full strings list](#)
- [Threads behaviour](#)
- [Network by processes](#)
- [Unpacked or injected modules](#)
- [Extra Information Recovered](#)
- [Configs Recovered](#)

## Sample

•md5: 1e9765081745e4328d52547c01427669

## AV detections

- Microsoft: VirTool:Win32/Injector.HY
- Kaspersky: Trojan-Banker.Win32.Banbra.tkpu
- Symantec: Suspicious.Cloud.9
- Malwarebytes: Trojan.Injector

## Source

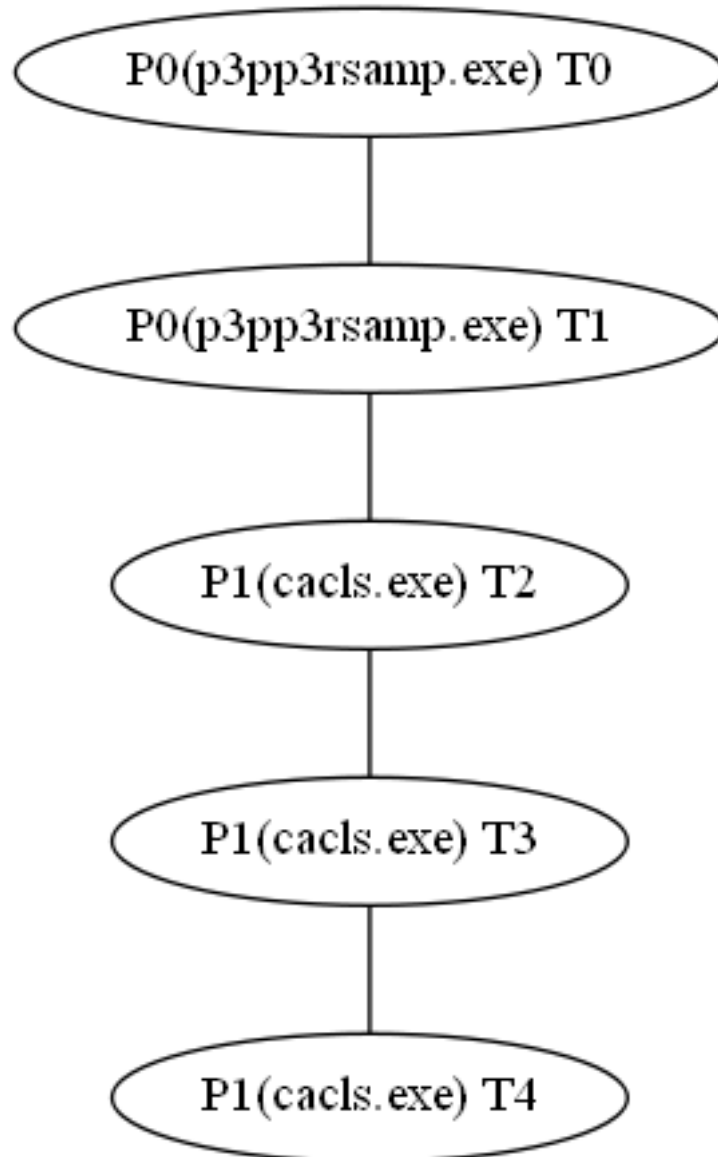
•

## Virustotal

- <https://virustotal.com/es/file/2012486d87dcc3362745c6f8f178b9be5417c595e79c452a20729d2e60ec814b/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 is 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\\66qscw4Q 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 is a collection of the most interesting strings found in the sample's modules (unpacked modules too) code or data.

- version="6.0.0.0" processorArchitecture="" publicKeyToken="6595b64144cc1df"
- <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
- !This program cannot be run in DOS mode.
- C:\Windows\System32\cacls.exe
- abnormal program termination
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- 6CAYioPjq+AL)@P7R`3Ra5Tc:WfC\_p?\_r@dtZ~
- REG\_MULTI\_SZ -
- C:\Users\p3pp3r\Downloads\p3pp3rsamp.exe
- REG\_REG\_EXPAND\_SZ -
- commctrl\_DragListMsg
- DOMAIN error
- LOADER ERROR
- type="win32" name="Microsoft.Windows.Common-Controls"
- - not enough space fo
- - unable to open console device
- PathFileExistsA
- ^qv2NU)@P8Sa5Sd4Sb0L)/K\#\#>R"CVt
- StringFileInfo
- c:\windows\8000
- - not enough space for lowio initialization
- DUjKcwKcy(BR'<Q3P\_7Xh?'p?Jn9Zj5Ti@dtOq
- ClosePrinter
- Software\Microsoft\Windows\CurrentVersion\Run\
- \*GU+DX6Te8Vg5Vf7Rf8Yi>\_rCgwOx
- <dependency>
- VS\_VERSION\_INFO
- GetProcAddress
- I`zJdu+FT'?Q3Ra3Qb0Qa5Sd?Jn<JpEl{S
- GetDeviceCaps
- CMapPtrToPtr
- runtime error
- PreviewPages
- MonitorFromPoint
- - unable to initialize heap
- </dependency>
- - not enough space for stdio initialization
- EnumDisplayMonitors
- - not enough space for thread data
- </dependentAssembly>
- - unexpected multithread lock error
- <assemblyIdentity version="1.0.0.0" processorArchitecture="" name="UnityTechnologies.Unity.UnityPlayer" type="win32" />
- ex{:QY&=M(CQ#CP(ET
- - pure virtual function call
- 2G\$@Q\*FW7UfB^oGbv;Yl:`rLo
- \_\_GLOBAL\_HEAP\_SELECTED
- - not enough space for \_onexit/atexit table
- The procedure entry point %s could not be located in the dynamic link library %s
- <dependentAssembly>
- language=""

- HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- The ordinal %u could not be located in the dynamic link library %s
- - not enough space for environment
- IsBadReadPtr
- CallWindowProcA
- .?AVCCmdTarget@@
- HKEY\_LOCAL\_MACHINE
- CreateProcessA
- HKEY\_CURRENT\_USER
- IsBadCodePtr
- SetFilePointer
- WritePrivateProfileStringA
- GetEnvironmentStrings
- GetSysColorBrush
- GlobalUnlock
- LCMAP\_STRINGA
- GlobalDeleteAtom
- .?AV\_AFX\_WIN\_STATE@@
- GetCurrentThreadId
- GlobalFindAtomA
- <program name unknown>
- GetClassLongA
- SunMonTueWedThuFriSat
- GetMessageTime
- GetWindowLongA
- abcdefghijklmnopqrstuvwxyz
- SetWindowLongA
- Process32First
- LCMAP\_STRINGW
- .?AVtype\_info@@
- FlushFileBuffers
- DefWindowProcA
- IsBadWritePtr
- .?AVAFX\_MODULE\_THREAD\_STATE@@
- .?AVCMAP\_PTR\_TO\_PTR@@
- .?AVCTEMP\_MENU@@
- program internal error number is %d.
- SetWaitableTimer
- SetUnhandledExceptionFilter
- TerminateProcess
- GlobalAddAtomA
- RegisterClassA
- Microsoft Visual C++ Runtime Library
- .?AV\_AFX\_THREAD\_STATE@@
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- JanFebMarAprMayJunJulAugSepOctNovDec
- GetCurrentThread
- HKEY\_CLASSES\_ROOT
- DocumentPropertiesA
- REG\_BINARY -
- ResumeThread
- SetFileAttributesA
- - floating point not loaded
- UnregisterClassA

- GetDlgCtrlID
- REG\_DWORD - DWORD
- GetMenuItemID
- .?AV\_AFX\_BASE\_MODULE\_STATE@@
- SetErrorMode
- OpenFileMappingA
- .?AV\_AFX\_CTL3D\_THREAD@@
- GetCurrentProcess
- FreeEnvironmentStringsA
- .?AVCWinThread@@
- PostQuitMessage
- - not enough space for arguments
- SetMenuItemBitmaps
- SetThreadContext
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- CallNextHookEx
- GetForegroundWindow
- MonitorFromRect
- MonitorFromWindow
- GetModuleHandleA
- GetSystemMetrics
- LoadLibraryA
- GetMonitorInfoA
- RegSetValueExA
- GetMenuCheckMarkDimensions
- VirtualAlloc
- GetProcessVersion
- GetClassNameA
- RtlMoveMemory
- IsWindowVisible
- GetTopWindow
- EnableMenuItem
- RaiseException
- SystemParametersInfoA
- PostMessageA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- UnhookWindowsHookEx
- IsDBCSLeadByte
- GetEnvironmentStringsW
- GlobalGetAtomNameA
- LocalReAlloc
- GetLastError
- RegDeleteKeyA
- LeaveCriticalSection
- RegEnumValueA
- SetWindowsHookExA
- CreateWaitableTimerA

- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- GetProcessHeap
- ZwUnmapViewOfSection
- GetWindowRect
- GetStartupInfoA
- RegisterWindowMessageA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- RegDeleteValueA
- 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
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- ValidateRect
- RegCreateKeyA
- WaitForSingleObject
- DestroyWindow
- GetStdHandle
- SetForegroundWindow



## Hosts

- 203.205.151.50:http
- google-public-dns-a.google.com:domain
- 192.168.149.219:49159
- 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 192.168.149.219:49159 ---> 203.205.151.50 (users.qzone.qq.com) :80**

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101  
Safari/537.36[...]Host: users.qzone.qq.com[...]Connection: Keep-Alive[...]GET  
/fcg-bin/cgi_get_portrait.fcg?uins=2058060008 HTTP/1.1
```

- **tcp 203.205.151.50 (users.qzone.qq.com) :80 ---> 192.168.149.219:49159**

```
<center><h1>301 Moved Permanently</h1></center>[...]<hr><center>stgw/1.3.10.5_1.13.5</center>[...]Content-Type:  
text/html[...]Content-Length: 193[...]Server: stgw/1.3.10.5_1.13.5[...]<head><title>301 Moved  
Permanently</title></head>[...]Date: Fri, 15 Mar 2019 02:20:15 GMT[...]HTTP/1.1 301 Moved  
Permanently[...]Connection: Keep-Alive[...]<body bgcolor="white">[...]Location:  
https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=2058060008
```

## 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.

- version="6.0.0.0" processorArchitecture="" publicKeyToken="6595b64144cc1df"
- <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
- !This program cannot be run in DOS mode.
- C:\Windows\System32\cacls.exe
- abnormal program termination
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- 6CAYioPjq+AL)@P7R`3Ra5Tc:WfC\_p?\_r@dtZ~
- REG\_MULTI\_SZ -
- C:\Users\p3pp3r\Downloads\p3pp3rsamp.exe
- REG\_REG\_EXPAND\_SZ -
- commctrl\_DragListMsg
- DOMAIN error
- LOADER ERROR
- type="win32" name="Microsoft.Windows.Common-Controls"
- - not enough space fo
- - unable to open console device
- PathFileExistsA
- ^qv2NU)@P8Sa5Sd4Sb0L)/K\#\#>R"CVt
- StringFileInfo
- c:\windows\8000
- - not enough space for lowio initialization
- DUjKcwKcy(BR'<Q3P\_7Xh?'p?Jn9Zj5Ti@dtOq
- ClosePrinter
- Software\Microsoft\Windows\CurrentVersion\Run\
- \*GU+DX6Te8Vg5Vf7Rf8Yi>\_rCgwOx
- <dependency>
- VS\_VERSION\_INFO
- GetProcAddress
- I`zJdu+FT'?Q3Ra3Qb0Qa5Sd?Jn<JpEl{S
- GetDeviceCaps
- CMapPtrToPtr
- runtime error
- PreviewPages
- MonitorFromPoint
- - unable to initialize heap
- </dependency>
- - not enough space for stdio initialization
- EnumDisplayMonitors
- - not enough space for thread data
- </dependentAssembly>
- - unexpected multithread lock error
- <assemblyIdentity version="1.0.0.0" processorArchitecture="" name="UnityTechnologies.Unity.UnityPlayer" type="win32" />
- ex{:QY&=M(CQ#CP(ET
- - pure virtual function call
- 2G\$@Q\*FW7UfB^oGbv:Yl:`rLo
- \_\_GLOBAL\_HEAP\_SELECTED
- - not enough space for \_onexit/atexit table
- The procedure entry point %s could not be located in the dynamic link library %s
- <dependentAssembly>
- language=""

- HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- The ordinal %u could not be located in the dynamic link library %s
- - not enough space for environment
- IsBadReadPtr
- CallWindowProcA
- .?AVCCmdTarget@@
- HKEY\_LOCAL\_MACHINE
- CreateProcessA
- HKEY\_CURRENT\_USER
- IsBadCodePtr
- SetFilePointer
- WritePrivateProfileStringA
- GetEnvironmentStrings
- GetSysColorBrush
- GlobalUnlock
- LCMAP\_STRINGA
- GlobalDeleteAtom
- .?AV\_AFX\_WIN\_STATE@@
- GetCurrentThreadId
- GlobalFindAtomA
- <program name unknown>
- GetClassLongA
- SunMonTueWedThuFriSat
- GetMessageTime
- GetWindowLongA
- abcdefghijklmnopqrstuvwxyz
- SetWindowLongA
- Process32First
- LCMAP\_STRINGW
- .?AVtype\_info@@
- FlushFileBuffers
- DefWindowProcA
- IsBadWritePtr
- .?AVAFX\_MODULE\_THREAD\_STATE@@
- .?AVCMAP\_PTR\_TO\_PTR@@
- .?AVCTEMP\_MENU@@
- program internal error number is %d.
- SetWaitableTimer
- SetUnhandledExceptionFilter
- TerminateProcess
- GlobalAddAtomA
- RegisterClassA
- Microsoft Visual C++ Runtime Library
- .?AV\_AFX\_THREAD\_STATE@@
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- JanFebMarAprMayJunJulAugSepOctNovDec
- GetCurrentThread
- HKEY\_CLASSES\_ROOT
- DocumentPropertiesA
- REG\_BINARY -
- ResumeThread
- SetFileAttributesA
- - floating point not loaded
- UnregisterClassA

- GetDlgCtrlID
- REG\_DWORD - DWORD
- GetMenuItemID
- .?AV\_AFX\_BASE\_MODULE\_STATE@@
- SetErrorMode
- OpenFileMappingA
- .?AV\_AFX\_CTL3D\_THREAD@@
- GetCurrentProcess
- FreeEnvironmentStringsA
- .?AVCWinThread@@
- PostQuitMessage
- - not enough space for arguments
- SetMenuItemBitmaps
- SetThreadContext
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- CallNextHookEx
- GetForegroundWindow
- MonitorFromRect
- MonitorFromWindow
- GetModuleHandleA
- GetSystemMetrics
- LoadLibraryA
- GetMonitorInfoA
- RegSetValueExA
- Unity Version
- ProductVersion
- nf948tnaet98n
- @nf948tnaed98n
- 350012195511216262
- <description>Unity</description>
- <assemblyIdentity
- CTempGdiObject
- AfxOleControl42s
- AfxFrameOrView42s
- CResourceException
- 4.5.0f6\_fd4616464986
- - unexpected heap error
- NF48TNA98NASF
- winspool.drv
- AfxMDIFrame42s
- 4.5.0.149807
- comctl32.dll
- CUserException
- kernel32.dll
- CMemoryException
- CNotSupportedException
- InitCommonControlsEx
- AfxControlBar42s

- advapi32.dll
- AfxOldWndProc423
- GetMenuCheckMarkDimensions
- VirtualAlloc
- GetProcessVersion
- GetClassNameA
- RtlMoveMemory
- IsWindowVisible
- GetTopWindow
- EnableMenuItem
- RaiseException
- SystemParametersInfoA
- PostMessageA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- UnhookWindowsHookEx
- IsDBCSLeadByte
- GetEnvironmentStringsW
- GlobalGetAtomNameA
- LocalReAlloc
- GetLastError
- RegDeleteKeyA
- LeaveCriticalSection
- RegEnumValueA
- SetWindowsHookExA
- CreateWaitableTimerA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA
- GetProcessHeap
- ZwUnmapViewOfSection
- GetWindowRect
- GetStartupInfoA
- RegisterWindowMessageA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- RegDeleteValueA
- 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
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- ValidateRect
- RegCreateKeyA
- WaitForSingleObject
- DestroyWindow
- GetStdHandle
- SetForegroundWindow
- .?AUThreadData@@
- SelectObject
- SetViewportOrgEx
- SetTextColor
- .?AVCUserException@@
- .?AVCHandleMap@@
- .?AVCMemoryException@@
- .?AVCTempGdiObject@@
- .PAVCEXception@@
- .?AV\_AFX\_CTL3D\_STATE@@
- GAIIsProcessorFeaturePresent
- .?AVCNotSupportedException@@
- .?AVCGdiObject@@
- GetStockObject
- .?AVCCmdUI@@
- CreateBitmap
- .?AVCWinApp@@
- .PAVCObject@@
- .?AVCObject@@
- DeleteObject
- .?AVCTestCmdUI@@
- ScaleWindowExtEx
- .?AVAFX\_MODULE\_STATE@@
- .?AVCNoTrackObject@@
- .?AVCResourceException@@
- OffsetViewportOrgEx
- .?AVCEXception@@
- COMDLG32.dll
- .PAVCMemoryException@@
- SetViewportExtEx
- .?AVCSimpleException@@
- SetWindowExtEx
- ScaleViewportExtEx



- .PAVCSimpleException@@
- OpenPrinterA
- \_\_MSVCRT\_HEAP\_SELECT
- K[1Qi{Jcs.JU&?O,J[.N[5Vf;Yj?]nAbvQu
- -v.a-vxB/v@;3v
- MS Shell Dlg
- .?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 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\\66qscw4Q 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 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 (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**

- 44616e53000000000000000000000000007b1c0c0001000000c30f5f0003000000831c0e001f00000036260a0077000000c30f5d0013000000000001007201000036260b006c0000000000000001000000e81f0b00

- **Module 1 strings**

- **Module 1 most interesting strings**

- version="6.0.0.0" processorArchitecture="" publicKeyToken="6595b64144cc1df"
      - <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
      - !This program cannot be run in DOS mode.
      - C:\Windows\System32\cacls.exe
      - abnormal program termination
      - <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
      - 6CAyioPjq+AL)@P7R`3Ra5Tc:WfC\_p?\_r@dtZ~
      - commctrl\_DragListMsg
      - DOMAIN error
      - LOADER ERROR
      - type="win32" name="Microsoft.Windows.Common-Controls"
      - - not enough space fo
      - - unable to open console device
      - PathFileExistsA
      - ^qv2NU)@P8Sa5Sd4Sb0L/K\#\#>R"CVt
      - StringFileInfo
      - c:\windows\8000
      - - not enough space for lowio initialization
      - DUjKcwKcy(BR'<Q3P\_7Xh?'p?Jn9Zj5Ti@dtOq
      - ClosePrinter
      - Software\Microsoft\Windows\CurrentVersion\Run\
      - \*GU+DX6Te8Vg5Vf7Rf8Yi>\_rCgwOx
      - <dependency>
      - VS\_VERSION\_INFO
      - GetProcAddress
      - I`zJdu+FT'?Q3Ra3Qb0Qa5Sd?Jn<JpEl{S
      - GetDeviceCaps
      - CMapPtrToPtr
      - runtime error
      - PreviewPages
      - MonitorFromPoint
      - - unable to initialize heap
      - </dependency>
      - - not enough space for stdio initialization
      - EnumDisplayMonitors
      - - not enough space for thread data
      - </dependentAssembly>
      - - unexpected multithread lock error
      - <assemblyIdentity version="1.0.0.0" processorArchitecture="" name="UnityTechnologies.Unity.UnityPlayer" type="win32"/>

- ex{:QY&=M(CQ#CP(ET
- - pure virtual function call
- 2G\$@Q\*FW7UfB\*oGbv;Yl:`rLo
- \_\_GLOBAL\_HEAP\_SELECTED
- - not enough space for \_onexit/atexit table
- The procedure entry point %s could not be located in the dynamic link library %s
- <dependentAssembly>
- language=""
- HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- The ordinal %u could not be located in the dynamic link library %s
- - not enough space for environment
- MonitorFromRect
- MonitorFromWindow
- GetModuleHandleA
- GetSystemMetrics
- LoadLibraryA
- GetMonitorInfoA
- RegSetValueExA

- **Module 1 other strings**

- Unity Version
- ProductVersion
- nf948tnaet98n
- @nf948tnaed98n
- 350012195511216262
- <description>Unity</description>
- <assemblyIdentity
- CTempGdiObject
- AfxOleControl42s
- AfxFrameOrView42s
- CResourceException
- 4.5.0f6\_fd4616464986
- - unexpected heap error
- NF48TNA98NASF
- winspool.drv
- AfxMDIFrame42s
- 4.5.0.149807
- comctl32.dll
- CUserException
- kernel32.dll
- CMemoryException
- CNotSupportedException
- InitCommonControlsEx
- AfxControlBar42s
- advapi32.dll
- AfxOldWndProc423
- \_\_MSVCRT\_HEAP\_SELECT
- K[1Qi{Jcs.JU&?O,J[.N[5Vf;Yj?]nAbvQu
- -v.a-vxB/v@;3v

- **Module 2 (probably unpacked / injected by the sample)**

- **Module 2 rich signatures**

- 44616e530000000000000000000007b1c0c000100000c30f5f000300000831c0e001f00000036260a007700000c30f5d001300000000001007201000036260b006c000000000000001000000e81f0b00

- **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"?>
- !This program cannot be run in DOS mode.
- C:\Windows\System32\cacls.exe
- abnormal program termination
- REG\_EXPAND\_SZ -
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- version="6.0.0.0" processorArchitecture="" publicKeyToken="6595b64144ccfddf"
- 6CAYioPjq+AL)@P7R`3Ra5Tc:WfC\_p?\_r@dtZ~
- commctrl\_DragListMsg
- DOMAIN error
- IsBadReadPtr
- CallWindowProcA
- LOADER ERROR
- .?AVCCmdTarget@@
- HKEY\_LOCAL\_MACHINE
- CreateProcessA
- HKEY\_CURRENT\_USER
- type="win32" name="Microsoft.Windows.Common-Controls"
- CMapPtrToPtr
- Software\Microsoft\Windows\CurrentVersion\Run\
- IsBadCodePtr
- The procedure entry point %s could not be located in the dynamic link library %s
- SetFilePointer
- PathFileExistsA
- runtime error
- ^qv2NU)@P8Sa5Sd4Sb0L)/K\#\#>R"CVt
- StringFileInfo
- WritePrivateProfileStringA
- GetEnvironmentStrings
- GetSysColorBrush
- c:\windows\8000
- GlobalUnlock
- 2G\$@Q\*FW7UfB^oGbv;Yl:`rLo
- LCMaPStringA
- - not enough space for lowio initialization
- DUjKcwKcy(BR'<Q3P\_7Xh?'p?ln9Zj5Ti@dtOq
- GlobalDeleteAtom
- .?AV\_AFX\_WIN\_STATE@@
- GetCurrentThreadId
- GlobalFindAtomA
- <program name unknown>
- ClosePrinter
- GetClassLongA
- - not enough space for \_onexit/atexit table
- SunMonTueWedThuFriSat
- GetMessageTime
- <dependency>

- </dependentAssembly>
- GetWindowLongA
- - unable to open console device
- GetProcAddress
- abcdefghijklmnopqrstuvwxyz
- I`zJdu+FT' ?Q3Ra3Qb0Qa5Sd? ]n<]pE1{S
- SetWindowLongA
- Process32First
- LCMaPStringW
- GetDeviceCaps
- .?AVtype\_info@@
- FlushFileBuffers
- DefWindowProcA
- IsBadWritePtr
- VS\_VERSION\_INFO
- .?AVAFX\_MODULE\_THREAD\_STATE@@
- .?AVCMapPtrToPtr@@
- .?AVCTempMenu@@
- program internal error number is %d.
- \*GU+DX6Te8Vg5Vf7Rf8Yi>\_rCgwOx
- SetWaitableTimer
- PreviewPages
- MonitorFromPoint
- SetUnhandledExceptionFilter
- TerminateProcess
- GlobalAddAtomA
- RegisterClassA
- Microsoft Visual C++ Runtime Library
- </dependency>
- .?AV\_AFX\_THREAD\_STATE@@
- - unable to initialize heap
- - not enough space for stdio initialization
- TranslateMessage
- Runtime Error!
- MultiByteToWideChar
- UnhandledExceptionFilter
- EnumDisplayMonitors
- - not enough space for thread data
- JanFebMarAprMayJunJulAugSepOctNovDec
- GetCurrentThread
- HKEY\_CLASSES\_ROOT
- DocumentPropertiesA
- REG\_BINARY -
- ResumeThread
- SetFileAttributesA
- - unexpected multithread lock error
- <assemblyIdentity version="1.0.0.0" processorArchitecture="" name="UnityTechnologies.Unity.UnityPlayer" type="win32"/>
- ex{:QY&=M(CQ#CP(ET
- - floating point not loaded
- UnregisterClassA
- GetDlgCtrlID
- REG\_DWORD - DWORD
- GetMenuItemID
- - pure virtual function call
- .?AV\_AFX\_BASE\_MODULE\_STATE@@
- SetErrorMode



- OpenFileMappingA
- .?AV\_AFX\_CTL3D\_THREAD@@
- language=""
- \_\_GLOBAL\_HEAP\_SELECTED
- <dependentAssembly>
- GetCurrentProcess
- FreeEnvironmentStringsA
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- .?AVCWinThread@@
- PostQuitMessage
- - not enough space for arguments
- SetMenuItemBitmaps
- The ordinal %u could not be located in the dynamic link library %s
- - not enough space for environment
- SetThreadContext
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- GetMessagePos
- WriteProcessMemory
- WideCharToMultiByte
- GetThreadContext
- CallNextHookEx
- GetForegroundWindow
- GetMenuCheckMarkDimensions
- VirtualAlloc
- GetProcessVersion
- GetClassNameA
- RtlMoveMemory
- MonitorFromRect
- MonitorFromWindow
- IsWindowVisible
- GetTopWindow
- EnableMenuItem
- RaiseException
- SystemParametersInfoA
- PostMessageA
- AdjustWindowRectEx
- GetCurrentDirectoryA
- UnhookWindowsHookEx
- IsDBCSLeadByte
- GetEnvironmentStringsW
- GlobalGetAtomNameA
- LocalReAlloc
- GetLastError
- RegDeleteKeyA
- LeaveCriticalSection
- RegEnumValueA
- SetWindowsHookExA
- CreateWaitableTimerA
- GetLastActivePopup
- GlobalReAlloc
- CheckMenuItem
- SetWindowTextA

- GetProcessHeap
- ZwUnmapViewOfSection
- GetWindowRect
- GetStartupInfoA
- GetSystemMetrics
- LoadLibraryA
- RegisterWindowMessageA
- GetMonitorInfoA
- SetHandleCount
- EnterCriticalSection
- InterlockedIncrement
- RegDeleteValueA
- RegSetValueExA
- CreateWindowExA
- TabbedTextOutA
- GetWindowPlacement
- GetModuleHandleA
- 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
- ClientToScreen
- DispatchMessageA
- DeleteCriticalSection
- SetWindowPos
- ValidateRect
- RegCreateKeyA
- WaitForSingleObject
- DestroyWindow
- GetStdHandle
- SetForegroundWindow

- **Module 2 other strings**

- .?AUThreadData@@
- SelectObject
- nf948tnaet98n
- SetViewportOrgEx
- <assemblyIdentity
- @nf948tnaed98n
- SetTextColor
- .?AVUserException@@
- .?AVHandleMap@@
- 350012195511216262
- NF48TNA98NASF
- .?AVMemoryException@@
- .?AVTempGdiObject@@
- .PAVCEXception@@
- .?AV\_AFX\_CTL3D\_STATE@@
- CTempGdiObject
- 4.5.0.149807
- AfxOleControl42s
- GAIsProcessorFeaturePresent
- .?AVCNotSupportedException@@
- .?AVCGdiObject@@
- GetStockObject
- .?AVCCmdUI@@
- CreateBitmap
- AfxFrameOrView42s
- CResourceException
- .?AVCWinApp@@
- - unexpected heap error
- .PAVCOBJECT@@
- Unity Version
- .?AVCOBJECT@@
- <description>Unity</description>
- DeleteObject
- AfxMDIFrame42s
- .?AVCTestCmdUI@@
- CUserException
- winspool.drv
- ScaleWindowExtEx
- .?AVAFX\_MODULE\_STATE@@
- .?AVCNoTrackObject@@
- .?AVCResourceException@@
- OffsetViewportOrgEx
- .?AVCEXception@@
- advapi32.dll
- COMDLG32.dll
- kernel32.dll
- ProductVersion
- CMemoryException
- .PAVCMemoryException@@
- comctl32.dll
- SetViewportExtEx
- .?AVCSimpleException@@
- CNotSupportedException

- SetWindowExtEx
- InitCommonControlsEx
- 4.5.0f6\_fd4616464986
- ScaleViewportExtEx
- AfxControlBar42s
- .PAVCSimpleException@@
- OpenPrinterA
- AfxOldWndProc423
- MS Shell Dlg
- .?AVCTempWnd@@
- \_\_MSVCRT\_HEAP\_SELECT
- .?AVCTempDC@@
- K[1Qi{Jcs.JU&?O,J[.N[5Vf;Yj?]nAbvQu
- -v.a-vxB/v@;3v

## 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.acq

.kr

.kr.acq

ET

step\_down.php?key=a0c1dbdbe6cd191f

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