

Sample: 09a0220648cfec926f72d2ad3d0c3ec0

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: #VIRTOOL #INJECTOR (based on p3pperp0tts rules)

Analysis date: 2019-03-14 23:40:42 (p3pperp0tts platform's analysis date)

Exe timestamp: 2016-03-10 04:19:56 (timestamp of the original sample)

Unpacked mods max timestamp: 2016-03-10 04:19:56 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2016-08-09 12:31:42 (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: 09a0220648cfec926f72d2ad3d0c3ec0

AV detections

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

Source

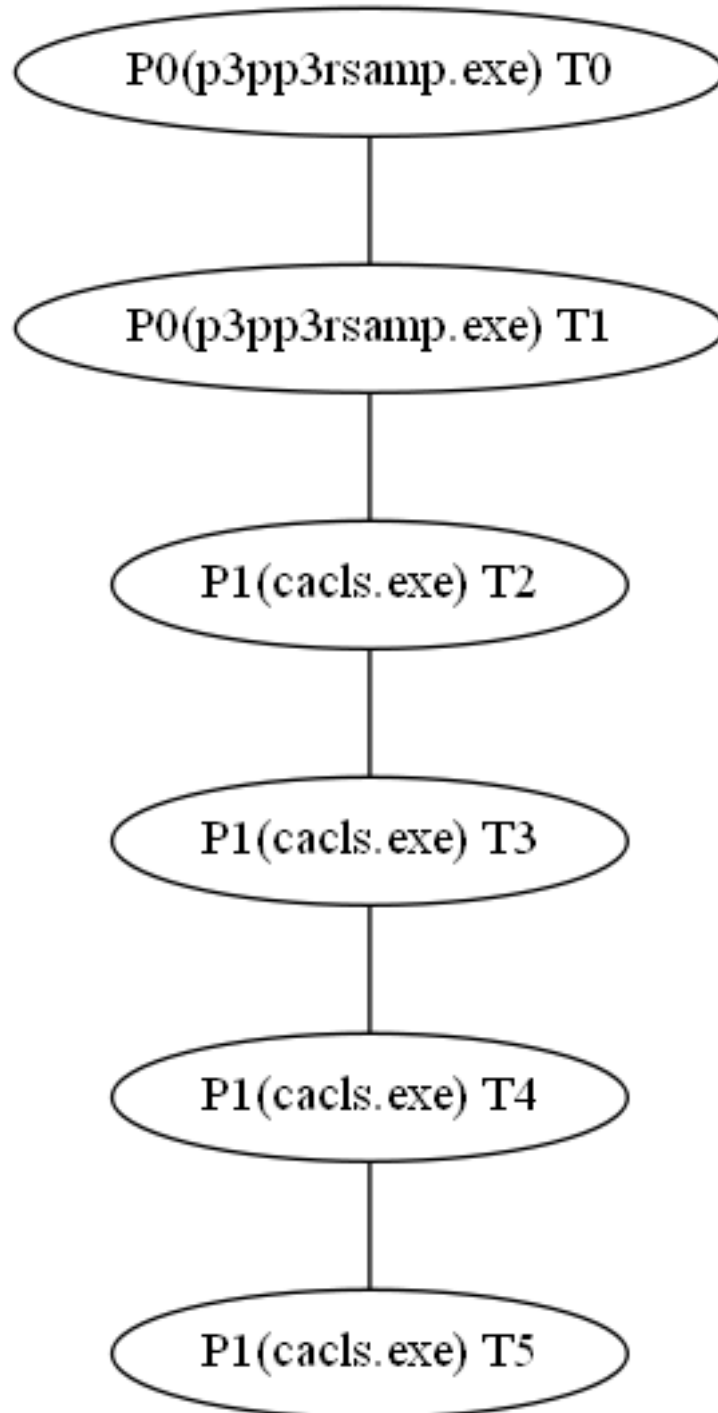
•

Virustotal

- <https://virustotal.com/es/file/7351373a50acbaa4bb3fa622b0573f473289d745ba717551c82abbe398c1c1ff/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\\1Lf9Tn7B 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)
- Thread Create (Thread ID: T5)

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.

- <dpiAware xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- !This program cannot be run in DOS mode.
- <compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
- <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <application xmlns="urn:schemas-microsoft-com:asm.v3">
- C:\Users\p3pp3r\Downloads\p3pp3rsamp.exe
- C:\Windows\regedit.exe
- C:\Windows\System32\cacls.exe
- REG_MULTI_SZ -
- abnormal program termination
- REG_REG_EXPAND_SZ -
- *s@C:\Windows\System32\user32.dll
- \$#"&"%*!\$)14988>2l:1l=77E-./0>+, :eit
- name="Microsoft.Windows.Common-Controls"
- <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}" />
- <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}" />
- name="JR.Inno.Setup"
- <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}" />
- </trustInfo>
- #\$\$',06:17<)-2.1937B25C,.(,,' ;4;J>BM
- LegalCopyright
- <requestedPrivileges>
- type="win32"
- #\$\$',03:8<A+.6-0826A37B,/>+-?&*<@DV`b1
- </windowsSettings>
- <dependency>
- <windowsSettings>
- VS_VERSION_INFO
- <description>Inno Setup</description>
- <requestedExecutionLevel level="asInvoker" uiAccess="false" />
- #\$(+/5:*05%)4*.936D,1@+0?(/@*1@19FJM[
- </dependency>
- GetProcAddress
- </requestedPrivileges>
- PathFileExistsA
- =Tt>Ql;Kb3>R\$<<
- CZz@Ro=Nh8C^,3D
- type="win32" />
- GetDeviceCaps
- processorArchitecture="x86"
- </dependentAssembly>
- <dependentAssembly>
- StringFileInfo
- language=""
- SHAppBarMessage
- commctrl_DragListMsg
- DOMAIN error
- .?AVCCmdTarget@@
- CreateProcessA

- HKEY_CURRENT_USER
- SetWaitableTimer
- - unable to open console device
- ?HKEY_CLASSES_ROOT
- c:\windows\8000
- - not enough space for lowio initialization
- GetStringTypeAGetStringTypeWIsBadCodePtrSetStdHandleLoadLibraryAFreeLibraryGetCommandLineASetFilePointerDeleteFileAGetFileSizeReadFileSetFileAttributesACreateFileAWriteFileGetCurrentDirectoryAGetTickCountLCMapStringAGetModuleFileNameAIsBadReadPtrHeapFreeH
- SystemTimeToFileTime
- Microsoft Visual C++ Runtime Library
- <program name unknown>
- EnumDisplaySettingsA
- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- HKEY_LOCAL_MACHINE
- .?AV_AFX_WIN_STATE@@
- Process32First
- .?AV_AFX_CTL3D_THREAD@@
- BlackMoon RunTime Error:
- .?AVAFX_MODULE_THREAD_STATE@@
- .?AVCMapPtrToPtr@@
- .?AVCTempMenu@@
- program internal error number is %d.
- CMapPtrToPtr
- runtime error
- LocalFileTimeToFileTime
- PreviewPages
- MonitorFromPoint
- TerminateProcess
- .?AV_AFX_THREAD_STATE@@
- - unable to initialize heap
- - not enough space for stdio initialization
- Runtime Error!
- .?AVtype_info@@
- abcdefghijklmnopqrstuvwxyz
- qPaj7i44:JlT
- - not enough space for thread data
- .?AV_AFX_BASE_MODULE_STATE@@
- JanFebMarAprMayJunJulAugSepOctNovDec
- EnumDisplayMonitors
- REG_BINARY -
- ResumeThread
- - unexpected multithread lock error
- - floating point not loaded
- REG_DWORD - DWORD
- - pure virtual function call
- OpenFileMappingA
- __GLOBAL_HEAP_SELECTED
- Software\Microsoft\Windows\CurrentVersion\Run\
- .?AVCWinThread@@
- - not enough space for arguments
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- - not enough space for environment
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory

- Process32Next
- SetThreadContext
- MapViewOfFile
- WriteProcessMemory
- GetThreadContext
- CreateToolhelp32Snapshot
- VirtualAlloc
- RegSetValueExA
- LoadLibraryA
- VirtualProtect
- RegOpenKeyExA
- RtlMoveMemory
- MonitorFromRect
- MonitorFromWindow
- GetModuleHandleA
- RegDeleteValueA
- IsDBCSLeadByte
- RegCreateKeyExA
- RegDeleteKeyA
- RegEnumValueA
- CreateWaitableTimerA
- GetLastActivePopup
- GetSystemMetrics
- ZwUnmapViewOfSection
- GetMonitorInfoA
- RegQueryValueExA
- MsgWaitForMultipleObjects
- GetEnvironmentVariableA
- GetActiveWindow
- RegCreateKeyA
- WaitForSingleObject

Hosts

- 203.205.151.50:http
- google-public-dns-a.google.com:domain
- 192.168.149.192:49159
- 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 192.168.149.192:49159 ---> 203.205.151.50 (users.qzone.qq.com) :80**

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

- **tcp 203.205.151.50 (users.qzone.qq.com) :80 ---> 192.168.149.192:49159**

```
<center><h1>301 Moved Permanently</h1></center>[...]Content-Type: text/html[...]Content-Length: 193[...]Server:
stgw/1.3.10.5_1.13.5[...]<hr><center>stgw/1.3.10.5_1.13.5</center>[...]Date: Thu, 14 Mar 2019 22:25:46
GMT[...]HTTP/1.1 301 Moved Permanently[...]Location:
https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=3351552119[...]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.

- <dpiAware xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- !This program cannot be run in DOS mode.
- <compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
- <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <application xmlns="urn:schemas-microsoft-com:asm.v3">
- C:\Users\p3pp3r\Downloads\p3pp3rsamp.exe
- C:\Windows\regedit.exe
- C:\Windows\System32\cacls.exe
- REG_MULTI_SZ -
- abnormal program termination
- REG_REG_EXPAND_SZ -
- *s@C:\Windows\System32\user32.dll
- \$#"&"%*!\$)14988>2l:1l=77E-./0>+, :eit
- name="Microsoft.Windows.Common-Controls"
- <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}" />
- <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}" />
- name="JR.Inno.Setup"
- <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}" />
- </trustInfo>
- #\$\$',06:17<)-2.1937B25C,.(,,' ;4;J>BM
- LegalCopyright
- <requestedPrivileges>
- type="win32"
- #\$\$',03:8<A+.6-0826A37B,/>+-?&*<@DV`b1
- </windowsSettings>
- <dependency>
- <windowsSettings>
- VS_VERSION_INFO
- <description>Inno Setup</description>
- <requestedExecutionLevel level="asInvoker" uiAccess="false" />
- #\$(+/5:*05%)4*.936D,1@+0?(/@*1@19FJM[
- </dependency>
- GetProcAddress
- </requestedPrivileges>
- PathFileExistsA
- =Tt>Ql;Kb3>R\$<<
- CZz@Ro=Nh8C^,3D
- type="win32" />
- GetDeviceCaps
- processorArchitecture="x86"
- </dependentAssembly>
- <dependentAssembly>
- StringFileInfo
- language=""
- SHAppBarMessage
- commctrl_DragListMsg
- DOMAIN error
- .?AVCCmdTarget@@
- CreateProcessA

- HKEY_CURRENT_USER
- SetWaitableTimer
- - unable to open console device
- ?HKEY_CLASSES_ROOT
- c:\windows\8000
- - not enough space for lowio initialization
- GetStringTypeAGetStringTypeWIsBadCodePtrSetStdHandleLoadLibraryAFreeLibraryGetCommandLineASetFilePointerDeleteFileAGetFileSizeReadFileSetFileAttributesACreateFileAWriteFileGetCurrentDirectoryAGetTickCountLCMapStringAGetModuleFileNameAIsBadReadPtrHeapFreeH
- SystemTimeToFileTime
- Microsoft Visual C++ Runtime Library
- <program name unknown>
- EnumDisplaySettingsA
- - not enough space for _onexit/atexit table
- SunMonTueWedThuFriSat
- HKEY_LOCAL_MACHINE
- .?AV_AFX_WIN_STATE@@
- Process32First
- .?AV_AFX_CTL3D_THREAD@@
- BlackMoon RunTime Error:
- .?AVAFX_MODULE_THREAD_STATE@@
- .?AVCMapPtrToPtr@@
- .?AVCTempMenu@@
- program internal error number is %d.
- CMapPtrToPtr
- runtime error
- LocalFileTimeToFileTime
- PreviewPages
- MonitorFromPoint
- TerminateProcess
- .?AV_AFX_THREAD_STATE@@
- - unable to initialize heap
- - not enough space for stdio initialization
- Runtime Error!
- .?AVtype_info@@
- abcdefghijklmnopqrstuvwxyz
- qPaj7i44:JlT
- - not enough space for thread data
- .?AV_AFX_BASE_MODULE_STATE@@
- JanFebMarAprMayJunJulAugSepOctNovDec
- EnumDisplayMonitors
- REG_BINARY -
- ResumeThread
- - unexpected multithread lock error
- - floating point not loaded
- REG_DWORD - DWORD
- - pure virtual function call
- OpenFileMappingA
- __GLOBAL_HEAP_SELECTED
- Software\Microsoft\Windows\CurrentVersion\Run\
- .?AVCWinThread@@
- - not enough space for arguments
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- - not enough space for environment
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory

- Process32Next
- SetThreadContext
- MapViewOfFile
- WriteProcessMemory
- GetThreadContext
- CreateToolhelp32Snapshot
- VirtualAlloc
- RegSetValueExA
- LoadLibraryA
- VirtualProtect
- z@o{0{1~9C*R
- <assemblyIdentity
- FileDescription
- publicKeyToken="6595b64144ccfldf"
- </compatibility>
- </application>
- \$#"&\'\$\'++/48<A,/4+.311=04?..>-/A+.=PUD
- <application>
- comctl32.dll
- kernel32.dll
- version="1.0.0.0"
- version="6.0.0.0"
- G\\x>Ql9Hb0;0#*9
- advapi32.dll
- ProductVersion
- winspool.drv
- \$\$\$()*%*\'*/77=43<-0500<56D..@.1@,.@_bp
- OpenPrinterA
- RegOpenKeyExA
- RtlMoveMemory
- MonitorFromRect
- MonitorFromWindow
- GetModuleHandleA
- RegDeleteValueA
- IsDBCSLeadByte
- RegCreateKeyExA
- RegDeleteKeyA
- RegEnumValueA
- CreateWaitableTimerA
- GetLastActivePopup
- GetSystemMetrics
- ZwUnmapViewOfSection
- GetMonitorInfoA
- RegQueryValueExA
- MsgWaitForMultipleObjects
- GetEnvironmentVariableA
- GetActiveWindow
- RegCreateKeyA
- WaitForSingleObject
- .?AVCSimpleException@@
- .?AUThreadData@@
- .?AVCException@@
- .PAVCSimpleException@@
- .?AVCHandleMap@@
- .?AVCMemoryException@@
- .PAVCOject@@
- .PAVCException@@

- CTempGdiObject
- AfxOleControl42s
- GAIProcessorFeaturePresent
- .?AVCNotSupportedException@@
- .?AVCGdiObject@@
- AfxFrameOrView42s
- CResourceException
- .?AVCUserException@@
- .?AVCWinApp@@
- - unexpected heap error
- .?AVCObject@@
- AfxMDIFrame42s
- CUserException
- COMDLG32.dll
- .?AVAFX_MODULE_STATE@@
- .?AVCNoTrackObject@@
- .?AVCResourceException@@
- .?AV_AFX_CTL3D_STATE@@
- CMemoryException
- .PAVCMemoryException@@
- CNotSupportedException
- InitCommonControlsEx
- AfxControlBar42s
- .?AVCTempGdiObject@@
- .?AVCTestCmdUI@@
- .?AVCCmdUI@@
- 2015-06-12 06:48:12
- AfxOldWndProc423
- Ezv;Kh0=S&/C
- SFGED3690Y7E589H7SFAT67BEAY8F9ASE768W4H7TY9SER87YGF68SDFBS7A6563
- .?AVCTempWnd@@
- .?AVCTempDC@@
- SFGED5890Y7E589H7SFAT67BEAY8F9ASE768W4H7TY9SER87YGF68SDFBS7A6563
- __MSVCRT_HEAP_SELECT
- -v.a-vxB/v@; 3v

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\\1Lf9Tn7B 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

- Thread T5 (in process P1, cacls.exe)

- Thread' events

- Thread Create (Thread ID: T5)

- Thread T5 (in process P1, cacls.exe) description

- Thread's childs

- 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 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))


```

    . ?AVCCmdTarget@@
    . name="JR.Inno.Setup"
    . CreateProcessA
    . HKEY_CURRENT_USER
    . #$(+/5:*05%)4*.936D,1@+0?(/@*1@19FJM[
    . SetWaitableTimer
    . <requestedPrivileges>
    . - unable to open console device
    . <description>Inno Setup</description>
    . ?HKEY_CLASSES_ROOT
    . PathFileExistsA
    . </requestedPrivileges>
    . CZz@Ro=Nh8C^,3D
    . c:\windows\8000
    . - not enough space for lowio initialization
    . GetStringTypeAGetStringTypeWIsBadCodePtrSetStdHandleLoadLibraryAFreeLibraryGetCommandLineASetFilePointerDeleteFil
    eAGetFileSizeReadFileSetFileAttributesACreateFileAWriteFileGetCurrentDirectoryAGetTickCountLCMapStringAGetModuleFil
    eNameAIsBadReadPtrHeapFreeH
    . SystemTimeToFileTime
    . Microsoft Visual C++ Runtime Library
    . <windowsSettings>
    . name="Microsoft.Windows.Common-Controls"
    . <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}" />
    . <program name unknown>
    . EnumDisplaySettingsA
    . <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}" />
    . - not enough space for _onexit/atexit table
    . type="win32"
    . SunMonTueWedThuFriSat
    . HKEY_LOCAL_MACHINE
    . <dependency>
    . VS_VERSION_INFO
    . ?AV_AFX_WIN_STATE@@
    . </trustInfo>
    . GetProcAddress
    . Process32First
    . GetDeviceCaps
    . ?AV_AFX_CTL3D_THREAD@@
    . BlackMoon RunTime Error:
    . ?AVAFX_MODULE_THREAD_STATE@@
    . ?AVCMapPtrToPtr@@
    . ?AVCTempMenu@@
    . program internal error number is %d.
    . <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}" />
    . </windowsSettings>
    . CMapPtrToPtr
    . SHAppBarMessage
    . runtime error
    . LocalFileTimeToFileTime
    . PreviewPages
    . MonitorFromPoint
    . TerminateProcess
    . ##',06;17<)-2.1937B25C,.(,;>',;4;J>BM
    . $$$',03;8<A+.6-0826A37B,/>+--?&*<@DV`b1
    . ?AV_AFX_THREAD_STATE@@
    . - unable to initialize heap
    . </dependency>

```

- - not enough space for stdio initialization
- Runtime Error!
- =Tt>Ql;Kb3>R\$<<
- .?AVtype_info@@
- abcdefghijklmnopqrstuvwxyz
- qPaj7i44:JlT
- type="win32"/>
- - not enough space for thread data
- </dependentAssembly>
- .?AV_AFX_BASE_MODULE_STATE@@
- JanFebMarAprMayJunJulAugSepOctNovDec
- EnumDisplayMonitors
- REG_BINARY -
- ResumeThread
- LegalCopyright
- - unexpected multithread lock error
- - floating point not loaded
- StringFileInfo
- <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
- REG_DWORD - DWORD
- - pure virtual function call
- OpenFileMappingA
- __GLOBAL_HEAP_SELECTED
- Software\\Microsoft\\Windows\\CurrentVersion\\Run\\
- processorArchitecture="x86"
- .?AVCWinThread@@
- - not enough space for arguments
- <dependentAssembly>
- language="*"
- HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
- - not enough space for environment
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- SetThreadContext
- MapViewOfFile
- WriteProcessMemory
- GetThreadContext
- CreateToolhelp32Snapshot
- VirtualAlloc
- RegOpenKeyExA
- RtlMoveMemory
- MonitorFromRect
- MonitorFromWindow
- GetModuleHandleA
- RegDeleteValueA
- RegSetValueExA
- IsDBCSLeadByte
- RegCreateKeyExA
- RegDeleteKeyA
- RegEnumValueA
- CreateWaitableTimerA
- GetLastActivePopup
- GetSystemMetrics
- ZwUnmapViewOfSection
- LoadLibraryA

- VirtualProtect
- GetMonitorInfoA
- RegQueryValueExA
- MsgWaitForMultipleObjects
- GetEnvironmentVariableA
- GetActiveWindow
- RegCreateKeyA
- WaitForSingleObject

• **Module 2 other strings**

- .?AVCSimpleException@@
- <application>
- .?AUThreadData@@
- FileDescription
- .?AVCException@@
- .PAVCSimpleException@@
- .?AVCHandleMap@@
- version="6.0.0.0"
- .?AVCMemoryException@@
- \$#"&\'\$\'++/48<A,/4+.311=04?..>-/A+.=PUD
- .PAVCOject@@
- .PAVCException@@
- CTempGdiObject
- AfxOleControl42s
- GAIsProcessorFeaturePresent
- .?AVCNotSupportedException@@
- </application>
- .?AVCGdiObject@@
- </compatibility>
- AfxFrameOrView42s
- CResourceException
- .?AVCUserException@@
- G\\x>Q19Hb0;0#*9
- .?AVCWinApp@@
- - unexpected heap error
- winspool.drv
- .?AVCOject@@
- AfxMDIFrame42s
- CUserException
- publicKeyToken="6595b64144ccf1df"
- COMDLG32.dll
- z@o}{0{1~9C*R
- .?AVAFX_MODULE_STATE@@
- .?AVCNoTrackObject@@
- .?AVCResourceException@@
- .?AV_AFX_CTL3D_STATE@@
- kernel32.dll
- ProductVersion
- CMemoryException
- .PAVCMemoryException@@
- comctl32.dll
- <assemblyIdentity
- CNotSupportedException
- InitCommonControlsEx
- AfxControlBar42s

- .?AVCTempGdiObject@@
- .?AVCTestCmdUI@@
- advapi32.dll
- .?AVCCmdUI@@
- version="1.0.0.0"
- 48:12
- \$\$\$()*%*\'/77=43<-0500<56D. .@.1@, .@_bp
- OpenPrinterA
- AfxOldWndProc423
- SFGED3690Y7E589H7SFAT67BEAY8F9ASE768W4H7TY9SER87YGF68SDFBS7A6563
- .?AVCTempWnd@@
- .?AVCTempDC@@
- SFGED5890Y7E589H7SFAT67BEAY8F9ASE768W4H7TY9SER87YGF68SDFBS7A6563
- __MSVCRT_HEAP_SELECT
- -v.a-vxB/v@; 3v
- Ezv;Kh0=S&/C

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.gal

.kr

.kr.gal

ET

step_down.php?key=b308115d7b1f81e2

HTTP/1.1 200 OK

Accept-Ranges: bytes

Content-Type: text/plain

Content-Length:

VBScript

Function MACAddress()

Dim mc,mo

Set mc=GetObject("Winmgmts:").InstancesOf("Win32_NetworkAdapterConfiguration")

For Each mo In mc

If mo.IPEnabled=True Then

MACAddress= mo.MacAddress

Exit For

End If

MACAddress

WinHttp.WinHttpRequest.5.1

Open

Send

responseBody

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

http://127.0.0.1:

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

AddCode

Applications\zipfldr.dll\NoOpenWith

regsvr32 /s zipfldr.dll

zip

Error

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

Line

ConnId

ProxyId

Configs Recovered

In this section there are malware configs recovered by platform plugins