Sample: 11fb2f435a7c525640575cd571b83513

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 00:57:10 (p3pperp0tts platform's analysis date)

Exe timestamp: 2016-03-31 08:01:46 (timestamp of the original sample)

Unpacked mods max timestamp: 2016-03-31 08:01:46 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2016-04-09 15:02:04 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: 11fb2f435a7c525640575cd571b83513

AV detections

- Microsoft: VirTool:Win32/Injector.HY
- Kaspersky: Trojan-Banker.Win32.Banbra.tlfl
- Symantec:
- Malwarebytes: Trojan.Banker.NVR

Source

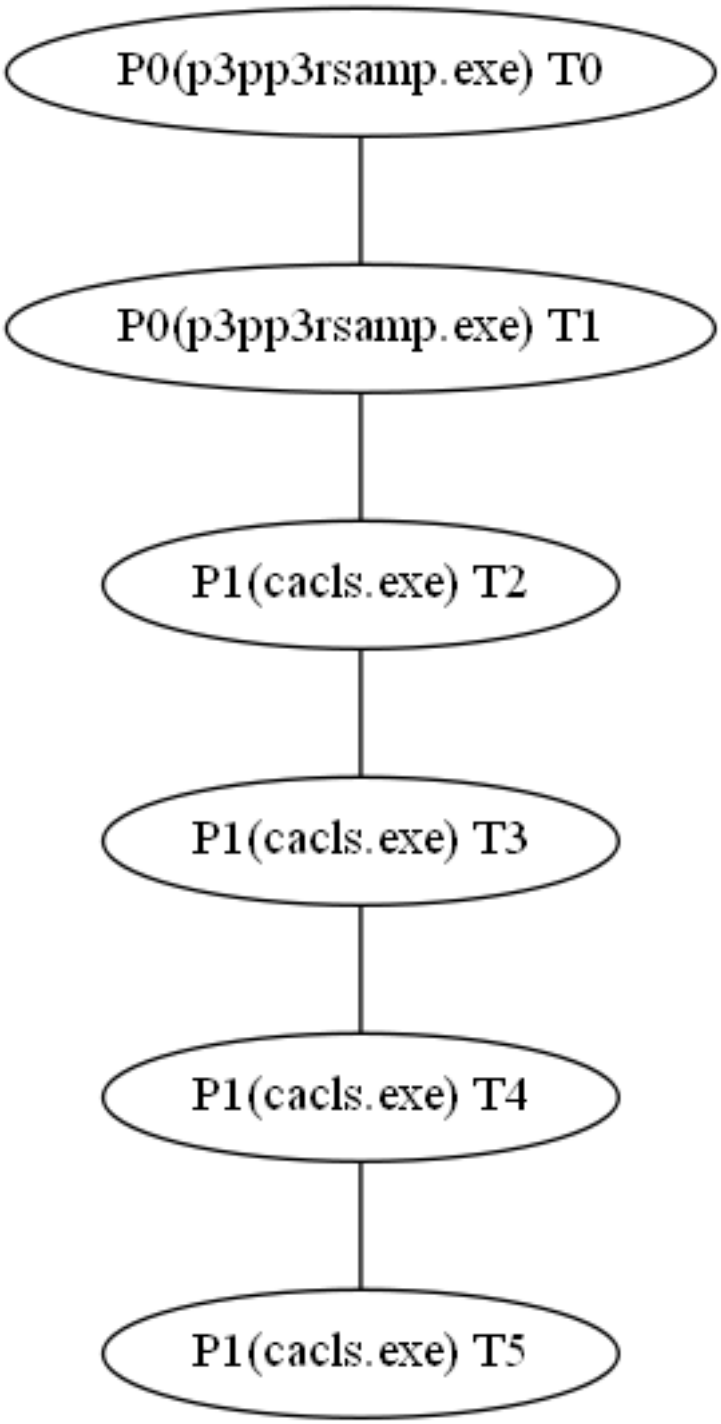
-

Virustotal

- https://virustotal.com/es/file/09a5dc4f9544f7bbc898d205f1e14518606e158f4a7c7126d7eb604ec9ec5c74/analysis

Threads tree

The following tree represents sample's threads. T<index> is an alias for sample's threads (numeration is done in the order of threads creation). P<index> is an alias for processes owning sample's threads.



Most interesting behavior

The following list it's a collection of the most interesting events captured. This list is ordered by the score assigned to the event. In the section "Threads behavioural information" it's possible to find all the actions performed by each sample's thread ordered chronologically.

- Process Create (C:\\Windows\\system32\\cacls.exe PID: P1, Command line: C:\\Windows\\System32\\cacls.exe)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\5jNh7p11 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: T4)
- Thread Create (Thread ID: TUNKALIAS)
- Thread Create (Thread ID: T5)

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.

- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
- !This program cannot be run in DOS mode.
- <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
- REG_REG_EXPAND_SZ -
- REG_MULTI_SZ -
- Photoshop Plugin Utilities
- TerminateProcess
- CloseDesktop
- HKEY_LOCAL_MACHINE
- CreateProcessA
- HKEY_CURRENT_USER
- Adobe Photoshop CC 2015
- OriginalFilename
- Adobe Systems, Incorporated
- IsBadReadPtr
- StringFileInfo
- GetCurrentProcessId
- LCMapStringA
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- CryptGetHashParam
- CryptDestroyHash
- REG_BINARY -
- VS_VERSION_INFO
- GetWindowLongA
- GetProcAddress
- Process32First
- CryptCreateHash
- BlackMoon RunTime Error:
- SwitchDesktop
- program internal error number is %d.
- SetWaitableTimer
- </trustInfo>
- </requestedPrivileges>
- OpenDesktopA
- TranslateMessage
- GetVolumeInformationA
- <requestedPrivileges>
- PathFileExistsA
- HKEY_CLASSES_ROOT
- PathRemoveBlanksA
- ResumeThread
- SetFileAttributesA
- ??3@YAXPAX@Z
- LegalCopyright
- __CxxFrameHandler
- REG_DWORD - DWORD
- OpenFileMappingA
- InternalName
- GetLocalTime
- Copyright 2015 Adobe Systems Inc.

- 732A4C67797E747F67634C28202020B66195FEC
- Hide Unlinked Events
- Auto Arrange
- contextEntityEventNode
- contextEntityGraphNode
- Clear All Event Links
- Auto Arrange All Events
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- SetThreadContext
- WriteProcessMemory
- GetThreadContext
- VirtualAlloc
- RtlMoveMemory
- ZwUnmapViewOfSection
- GetModuleHandleA
- GetCommandLineA
- GetCurrentDirectoryA
- CryptHashData
- RegDeleteKeyA
- CreateWaitableTimerA
- RegOpenKeyExA
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- LoadLibraryA
- RegDeleteValueA
- RegSetValueExA
- GetDiskFreeSpaceExA
- RegEnumValueA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA
- RegQueryValueExA
- MsgWaitForMultipleObjects
- GetEnvironmentVariableA
- DispatchMessageA
- RegCreateKeyA
- WaitForSingleObject

Hosts

- 203.205.151.50:http
- google-public-dns-a.google.com:domain
- 192.168.149.196:49159
- 203.205.151.50:80

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.

- **tcp 192.168.149.196:49159 ---> 203.205.151.50:80**

  GET /fcg-bin/cgi_get_portrait.fcg?uins=2135988505 HTTP/1.1[...]Host: users.qzone.qq.com[...]Connection: Keep-Alive[...]User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36

- **tcp 203.205.151.50:80 ---> 192.168.149.196:49159**

  <h1>301 Moved Permanently</h1> [...]Location: https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=2135988505[...]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 [...]HTTP/1.1 301 Moved Permanently[...]Connection: Keep-Alive[...]<body bgcolor="white">[...]<head><title>301 Moved Permanently</title></head>[...]Date: Thu, 14 Mar 2019 23:43:23 GMT

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.

- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
- !This program cannot be run in DOS mode.
- <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
- REG_REG_EXPAND_SZ -
- REG_MULTI_SZ -
- Photoshop Plugin Utilities
- TerminateProcess
- CloseDesktop
- HKEY_LOCAL_MACHINE
- CreateProcessA
- HKEY_CURRENT_USER
- Adobe Photoshop CC 2015
- OriginalFilename
- Adobe Systems, Incorporated
- IsBadReadPtr
- StringFileInfo
- GetCurrentProcessId
- LCMapStringA
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- CryptGetHashParam
- CryptDestroyHash
- REG_BINARY -
- VS_VERSION_INFO
- GetWindowLongA
- GetProcAddress
- Process32First
- CryptCreateHash
- BlackMoon RunTime Error:
- SwitchDesktop
- program internal error number is %d.
- SetWaitableTimer
- </trustInfo>
- </requestedPrivileges>
- OpenDesktopA
- TranslateMessage
- GetVolumeInformationA
- <requestedPrivileges>
- PathFileExistsA
- HKEY_CLASSES_ROOT
- PathRemoveBlanksA
- ResumeThread
- SetFileAttributesA
- ??3@YAXPAX@Z
- LegalCopyright
- __CxxFrameHandler
- REG_DWORD - DWORD
- OpenFileMappingA
- InternalName
- GetLocalTime
- Copyright 2015 Adobe Systems Inc.

- 732A4C67797E747F67634C28202020B66195FEC
- Hide Unlinked Events
- Auto Arrange
- contextEntityEventNode
- contextEntityGraphNode
- Clear All Event Links
- Auto Arrange All Events
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- SetThreadContext
- WriteProcessMemory
- GetThreadContext
- VirtualAlloc
- RtlMoveMemory
- ZwUnmapViewOfSection
- GetModuleHandleA
- GetCommandLineA
- GetCurrentDirectoryA
- CryptHashData
- RegDeleteKeyA
- CreateWaitableTimerA
- RegOpenKeyExA
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- LoadLibraryA
- RegDeleteValueA
- RegSetValueExA
- GetDiskFreeSpaceExA
- RegEnumValueA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA
- RegQueryValueExA
- MsgWaitForMultipleObjects
- GetEnvironmentVariableA
- DispatchMessageA
- RegCreateKeyA
- WaitForSingleObject
- 532A4C47797E747F67634C43696364757D23224C7371737C633E756875EA6314C3D
- FileDescription
- ProductVersion
- 7371737C633E75687559869F521
- 523867828109165
- f7a3789aht9c7afba934672b
- "@0123456789ABCDEF
- 4668096668889
- 199065834101
- 16.0.0 (2015.0.0 x001 x003)
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CEB0D823E8
- kernel32.dll

- advapi32.dll
- 58267256898179
- Show Linked Events
- RENDERCONTROL
- Show All Events
- Delete Entity
- contextEntityGraphEditor
- MS Shell Dlg

Threads behaviour

In this section it's possible to find information about sample's threads, such as the actions performed by each sample's thread ordered chronologically.

- **Thread T0 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T1 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create (Thread ID: T1)
- **Thread T1 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T2 (in process P1, cacls.exe)
  - **Thread' events**
    - Process Create (C:\\Windows\\system32\\cacls.exe PID: P1, Command line: C:\\Windows\\System32\\cacls.exe)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\5jNh7p11 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: T4)
    - 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 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 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 (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**
    - 44616e530000000000000000000000007b1c0c0001000000831c0e00020000006f1f040002000000e81f0a0002000000000000010062000000c30f5d000d00000036260b00450000000000000000001000000e81f0b00
  - **Module 1 strings**
    - **Module 1 most interesting strings**
      - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
      - <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
      - !This program cannot be run in DOS mode.
      - <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
      - REG_REG_EXPAND_SZ -
      - REG_MULTI_SZ -
      - Photoshop Plugin Utilities
      - TerminateProcess
      - CloseDesktop
      - HKEY_LOCAL_MACHINE
      - CreateProcessA
      - HKEY_CURRENT_USER
      - Adobe Photoshop CC 2015
      - OriginalFilename
      - Adobe Systems, Incorporated
      - IsBadReadPtr
      - StringFileInfo
      - GetCurrentProcessId
      - LCMapStringA
      - <requestedExecutionLevel level='asInvoker' uiAccess='false' />
      - CryptGetHashParam
      - CryptDestroyHash
      - REG_BINARY -
      - VS_VERSION_INFO
      - GetWindowLongA
      - GetProcAddress
      - Process32First
      - CryptCreateHash
      - BlackMoon RunTime Error:
      - SwitchDesktop
      - program internal error number is %d.
      - SetWaitableTimer
      - </trustInfo>
      - </requestedPrivileges>
      - OpenDesktopA
      - TranslateMessage
      - GetVolumeInformationA
      - <requestedPrivileges>
      - PathFileExistsA
      - HKEY_CLASSES_ROOT

- PathRemoveBlanksA
- ResumeThread
- SetFileAttributesA
- ??3@YAXPAX@Z
- LegalCopyright
- __CxxFrameHandler
- REG_DWORD - DWORD
- OpenFileMappingA
- InternalName
- GetLocalTime
- Copyright 2015 Adobe Systems Inc.
- 732A4C67797E747F67634C28202020B66195FEC
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- SetThreadContext
- WriteProcessMemory
- GetThreadContext
- VirtualAlloc
- RtlMoveMemory
- ZwUnmapViewOfSection
- GetModuleHandleA
- GetCommandLineA
- GetCurrentDirectoryA
- CryptHashData
- RegDeleteKeyA
- CreateWaitableTimerA
- RegOpenKeyExA
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- LoadLibraryA
- RegDeleteValueA
- RegSetValueExA
- GetDiskFreeSpaceExA
- RegEnumValueA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA
- RegQueryValueExA
- MsgWaitForMultipleObjects
- GetEnvironmentVariableA
- DispatchMessageA
- RegCreateKeyA
- WaitForSingleObject

- **Module 1 other strings**

- 532A4C47797E747F67634C43696364757D23224C7371737C633E756875EA6314C3D
- FileDescription
- ProductVersion
- 7371737C633E75687559869F521
- 523867828109165

- f7a3789aht9c7afba934672b
- "@0123456789ABCDEF
- 4668096668889
- 199065834101
- 16.0.0 (2015.0.0 x001 x003)
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657EE7B84889B
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CEB0D823E8
- kernel32.dll
- advapi32.dll
- 58267256898179
- No strings found

Module 2 (probably unpacked / injected by the sample)

Module 2 rich signatures

- 44616e530000000000000000000000007b1c0c0001000000831c0e00020000006f1f040002000000e81f0a0002000000000000010062000000c30f5d000d00000036260b00450000000000000000001000000e81f0b00

Module 2 strings

Module 2 most interesting strings

- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
- !This program cannot be run in DOS mode.
- <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
- REG_REG_EXPAND_SZ -
- REG_MULTI_SZ -
- Photoshop Plugin Utilities
- TerminateProcess
- CloseDesktop
- HKEY_LOCAL_MACHINE
- CreateProcessA
- HKEY_CURRENT_USER
- Adobe Photoshop CC 2015
- OriginalFilename
- Adobe Systems, Incorporated
- IsBadReadPtr
- StringFileInfo
- GetCurrentProcessId
- LCMapStringA
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- CryptGetHashParam
- CryptDestroyHash
- REG_BINARY -
- VS_VERSION_INFO
- GetWindowLongA
- GetProcAddress
- Hide Unlinked Events
- Process32First
- CryptCreateHash
- BlackMoon RunTime Error:
- SwitchDesktop

- Auto Arrange
- program internal error number is %d.
- SetWaitableTimer
- </trustInfo>
- </requestedPrivileges>
- OpenDesktopA
- TranslateMessage
- contextEntityEventNode
- GetVolumeInformationA
- <requestedPrivileges>
- PathFileExistsA
- HKEY_CLASSES_ROOT
- PathRemoveBlanksA
- ResumeThread
- SetFileAttributesA
- contextEntityGraphNode
- ??3@YAXPAX@Z
- LegalCopyright
- Clear All Event Links
- __CxxFrameHandler
- REG_DWORD - DWORD
- OpenFileMappingA
- Copyright 2015 Adobe Systems Inc.
- InternalName
- GetLocalTime
- Auto Arrange All Events
- 732A4C67797E747F67634C28202020B66195FEC
- MapViewOfFile
- VirtualAllocEx
- VirtualProtectEx
- ReadProcessMemory
- Process32Next
- CreateToolhelp32Snapshot
- SetThreadContext
- WriteProcessMemory
- GetThreadContext
- VirtualAlloc
- RtlMoveMemory
- ZwUnmapViewOfSection
- GetModuleHandleA
- GetCommandLineA
- GetCurrentDirectoryA
- CryptHashData
- RegDeleteKeyA
- CreateWaitableTimerA
- RegOpenKeyExA
- CryptAcquireContextA
- CryptReleaseContext
- GetProcessHeap
- LoadLibraryA
- RegDeleteValueA
- RegSetValueExA
- GetDiskFreeSpaceExA
- RegEnumValueA
- PeekMessageA
- GetModuleFileNameA
- RegCreateKeyExA

- RegQueryValueExA
- MsgWaitForMultipleObjects
- GetEnvironmentVariableA
- DispatchMessageA
- RegCreateKeyA
- WaitForSingleObject

- **Module 2 other strings**

- Show Linked Events
- 532A4C47797E747F67634C43696364757D23224C7371737C633E756875EA6314C3D
- FileDescription
- ProductVersion
- 7371737C633E75687559869F521
- 523867828109165
- f7a3789aht9c7afba934672b
- "@0123456789ABCDEF
- 4668096668889
- RENDERCONTROL
- 199065834101
- Show All Events
- 16.0.0 (2015.0.0 x001 x003)
- 585B55494F5C5F53515C4F5D515358595E554C435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657EE7B84889B
- 435F5644475142554C5D7973627F637F76644C47797E747F67634C53656262757E6446756263797F7E4C42657E4CEB0D823E8
- kernel32.dll
- Delete Entity
- advapi32.dll
- contextEntityGraphEditor
- 58267256898179
- MS Shell Dlg

Extra Information Recovered

In this section there is additional information recovered by platform plugins

- **DecryptedString**

http://

/ca.php

?m=

&h;=

&o;=

e772ab66f0aad2ef

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.ggg

.kr

.kr.ggg

ET

step_down.php?key=15b8e0491dca8778

```
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