Sample: 236cc4758f096952703b8e0b457bf4e5

P3pper Reports - **http://www.peppermalware.com**.

P3pper Twitter - **https://twitter.com/P3pperP0tts**.

This report has been generated automatically by a set of malware analysis tools.

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

Analysis date: 2019-03-15 04:28:11 (p3pperp0tts platform's analysis date)

Exe timestamp: 2016-04-22 14:23:38 (timestamp of the original sample)

Unpacked mods max timestamp: 2016-04-22 14:23:38 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2019-02-28 01:32:06 (date of last time that the sample was analyzed at vt)

Index

Sample

- md5: 236cc4758f096952703b8e0b457bf4e5

AV detections

- Microsoft: TrojanSpy:Win32/Banker
- Kaspersky: Trojan-Banker.Win32.Banbra.tlmx
- Symantec: Backdoor.Graybird
- Malwarebytes:

Source

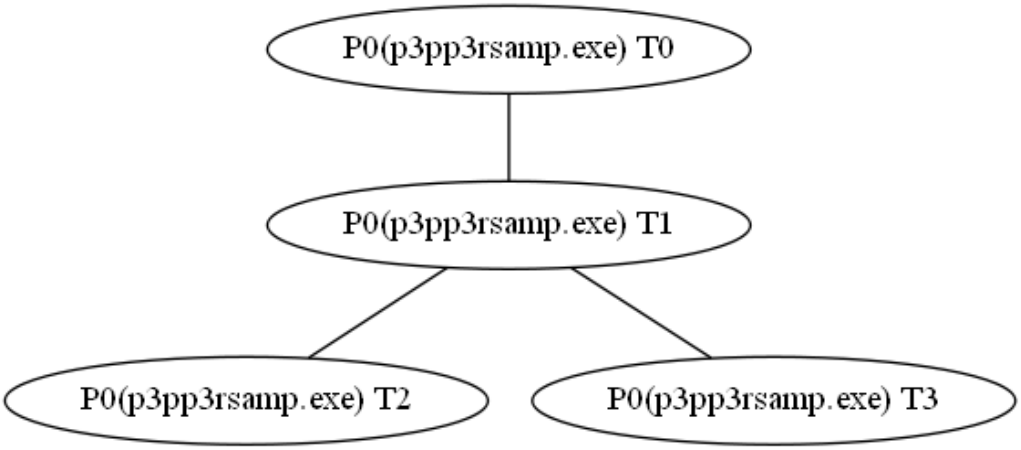
-

Virustotal

- https://virustotal.com/es/file/00eae37eaaee93b8155e6bad95564c3d95d71e7397653ffcbae4f95614ffa723/analysis

Threads tree

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



Most interesting behavior

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

- RegCreateKey (HKCU\\Software\\Microsoft\\Windows Script\\Settings Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\000C29FC2AB3 Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- Thread Create (Thread ID: T1)
- Thread Create (Thread ID: TUNKALIAS)
- Thread Create (Thread ID: T2)
- Thread Create (Thread ID: T3)

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'?>
- Copyright (c) 2010 - 2015 Baidu, Inc. All Rights Reserved.
- /%+I:>]KRp\\io\\o
- IsBadReadPtr
- to~84?>:EhdoWS^}o
- CLSIDFromProgID
- a\\kIIULMW][gi`t`TjPIX=9E73?C?K72
- OriginalFilename
- IIU][g`Tj=9EC?K
- <requestedPrivileges>
- }sqwukiomcage
- JFQ=:Ca^gVS\\]Og
- <9BA:ARFRA2@
- >3$)boxuV[LAal{vUXOB
- PathFileExistsA
- A-@L?OOCY.$4"
- StringFileInfo
- 6BB1A5AC7F04F927A802E0913D2DCF323DC48C7BDF0E747A9E73DB32B4F60EEACA56CFB7DF635E212A8D1404587794A3E348E5E0C898F4B6B5156698609C8CFEA6E855BF
- </requestedPrivileges>
- LCMapStringA
- </trustInfo>
- XBZA-@G8FL?OM@VOCY+!2.$4J@P"
- GetNativeSystemInfo
- program internal error number is %d.
- lixRJ[TM\\KCT:5D
- =:CVS\\eT]E4Oj]u
- $H7DhU^o\\e}jy
- GetUserDefaultLCID
- 3*>D6NRE]LCX
- CLSIDFromString
- GetProcAddress
- 0XJbjUkv_ns_lzky|r
- ww}cag\\Z`JHN
- -&;0YRODu~ch
- -MEj`PrgQnxaw
- &9;c#%U9:ma[
- RunTime Error:
- ?&:S;M2 -eU`SEK
- 997BA5EA600423CD2830F846EB20A1505CD
- l]|VF^4'5.%/;1>KAQNCW-$8
- 7:- m`wzYTCN
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- InternalName
- CreateThread
- d[o?5LOB\\l\\si_lLFK-/0(,1>DKFHPYY_]\\eLKUD6
- TranslateMessage
- MultiByteToWideChar

- tuyTUY%&*~uqj][
- ghr[UfVMaTM\\KDSB=L?:I
- 86$*p~lbHFTZ
- \\Rc]PfXJbUI]QHURNTPNT9:D**6>=GA>GDCMJIS
- sozkgrPLW<-jSClRE]
- \\Qeqdr`RdfZlldunlxfenVU_SJ^SJ^LERFBMB>J:8D)'
- HCL@0AM:IM7C3
- ;9?=3175+)/-#!'%[Y_]SQWUKIOMCAGE{y
- GetLogicalDriveStringsA
- LegalCopyright
- ??3@YAXPAX@Z
- __CxxFrameHandler
- <0B?0E`Oj[JeTE`UH`ec
- Baidu Pinyin MicroKernel Library
- 2?(%nctyZW@M
- VS_VERSION_INFO
- (L<NQ?V`PhSC[L?U@3Yje
- oVd:".jYbsgm,
- licat@on eqr
-)D\t(549"5,.fO
-]pA]HT]\\RY6k
- Copyright (C) 2011
- Wow64DisableWow64FsRedirection
- CoCreateInstance
- WideCharToMultiByte
- RtlMoveMemory
- Wow64RevertWow64FsRedirection
- GetModuleHandleA
- GetCommandLineA
- GetTempPathA
- RtlAllocateHeap
- LeaveCriticalSection
- GetProcessHeap
- RegDisableReflectionKey
- CreateDirectoryA
- LoadLibraryA
- GetSystemWow64DirectoryA
- EnterCriticalSection
- RegSetValueExA
- CreateMutexA
- GetModuleFileNameA
- RegCreateKeyExA
- VirtualAlloc
- RegQueryValueExA
- GetEnvironmentVariableA
- InitializeCriticalSection
- GetUserNameA
- RegOpenKeyExA
- PeekMessageA
- DispatchMessageA
- RegEnableReflectionKey
- DeleteCriticalSection
- LookupAccountNameA
- WaitForSingleObject
- ConvertSidToStringSidW
- ReleaseMutex

Hosts

- 203.205.151.50:http
- google-public-dns-a.google.com:domain
- 192.168.149.224:49159
- 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 192.168.149.224:49159 ---> 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=2218657667 HTTP/1.1

- **tcp 203.205.151.50 (users.qzone.qq.com) :80 ---> 192.168.149.224:49159**

  Date: Fri, 15 Mar 2019 03:11:44 GMT[...]<hr> stgw/1.3.6.2_1.13.5 [...]Content-Type: text/html[...]Location: https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=2218657667[...]Content-Length: 192[...]Server: stgw/1.3.6.2_1.13.5[...] <h1>301 Moved Permanently</h1> [...]HTTP/1.1 301 Moved Permanently[...]Connection: Keep-Alive[...]<body bgcolor="white">[...]<head><title>301 Moved Permanently</title></head>

Full strings list

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

- <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'?>
- Copyright (c) 2010 - 2015 Baidu, Inc. All Rights Reserved.
- /%+I:>]KRp\\io\\o
- IsBadReadPtr
- to~84?>:EhdoWS^}o
- CLSIDFromProgID
- a\\kIIULMW][gi`t`TjPIX=9E73?C?K72
- OriginalFilename
- IIU][g`Tj=9EC?K
- <requestedPrivileges>
- }sqwukiomcage
- JFQ=:Ca^gVS\\]Og
- <9BA:ARFRA2@
- >3$)boxuV[LAal{vUXOB
- PathFileExistsA
- A-@L?OOCY.$4"
- StringFileInfo
- 6BB1A5AC7F04F927A802E0913D2DCF323DC48C7BDF0E747A9E73DB32B4F60EEACA56CFB7DF635E212A8D1404587794A3E348E5E0C898F4B6B5156698609C8CFEA6E855BF
- </requestedPrivileges>
- LCMapStringA
- </trustInfo>
- XBZA-@G8FL?OM@VOCY+!2.$4J@P"
- GetNativeSystemInfo
- program internal error number is %d.
- lixRJ[TM\\KCT:5D
- =:CVS\\eT]E4Oj]u
- $H7DhU^o\\e}jy
- GetUserDefaultLCID
- 3*>D6NRE]LCX
- CLSIDFromString
- GetProcAddress
- 0XJbjUkv_ns_lzky|r
- ww}cag\\Z`JHN
- -&;0YRODu~ch
- -MEj`PrgQnxaw
- &9;c#%U9:ma[
- RunTime Error:
- ?&:S;M2 -eU`SEK
- 997BA5EA600423CD2830F846EB20A1505CD
- l]|VF^4'5.%/;1>KAQNCW-$8
- 7:- m`wzYTCN
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- InternalName
- CreateThread
- d[o?5LOB\\l\\si_lLFK-/0(,1>DKFHPYY_]\\eLKUD6
- TranslateMessage
- MultiByteToWideChar

- tuyTUY%&*~uqj][
- ghr[UfVMaTM\\KDSB=L?:I
- 86$*p~lbHFTZ
- \\Rc]PfXJbUI]QHURNTPNT9:D**6>=GA>GDCMJIS
- sozkgrPLW<-jSClRE]
- \\Qeqdr`RdfZlldunlxfenVU_SJ^SJ^LERFBMB>J:8D)'
- HCL@0AM:IM7C3
- ;9?=3175+)/-#!'%[Y_]SQWUKIOMCAGE{y
- GetLogicalDriveStringsA
- LegalCopyright
- ??3@YAXPAX@Z
- __CxxFrameHandler
- <0B?0E`Oj[JeTE`UH`ec
- Baidu Pinyin MicroKernel Library
- 2?(%nctyZW@M
- VS_VERSION_INFO
- (L<NQ?V`PhSC[L?U@3Yje
- oVd:".jYbsgm,
- licat@on eqr
-)D\t(549"5,.fO
-]pA]HT]\\RY6k
- Copyright (C) 2011
- Wow64DisableWow64FsRedirection
- CoCreateInstance
- WideCharToMultiByte
- RtlMoveMemory
- Wow64RevertWow64FsRedirection
- GetModuleHandleA
- GetCommandLineA
- GetTempPathA
- RtlAllocateHeap
- LeaveCriticalSection
- GetProcessHeap
- RegDisableReflectionKey
- CreateDirectoryA
- LoadLibraryA
- GetSystemWow64DirectoryA
- EnterCriticalSection
- RegSetValueExA
- CreateMutexA
- GetModuleFileNameA
- RegCreateKeyExA
- VirtualAlloc
- RegQueryValueExA
- GetEnvironmentVariableA
- InitializeCriticalSection
- GetUserNameA
- RegOpenKeyExA
- PeekMessageA
- DispatchMessageA
- RegEnableReflectionKey
- DeleteCriticalSection
- LookupAccountNameA
- WaitForSingleObject
- ConvertSidToStringSidW
- ReleaseMutex

• 69B1A5AD7F7AFE27AA76E1903D2CCA3D3FB7897EA60874739F7FDA46CFFC0A9ACF26CEB8A4635D242A8D11005C7293A2E246E694B5E9F5B3B114629C619DF3FDDCEA51BF0FF93D83B602355008911A1A8BB9AC511D4A5FC80FB6C3A48D420329851B672D310E20251304F7F2F42A63AAD7169B43E7A343AD176BAC9E75359A0

• 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F30313233343536373 8393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F7071 72737475767778797A7B7C7D7E7

• 68B1A4DE7F0FFA29A904E091

• AO]Sywek1?-#

• 6FC6A4DC780C

• oleaut32.dll

• *!.;1A2&<,#7

• 68B6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18A03A70F720A9D72DE42B4800F94CB21B4B9A4125A552EFC15755E0497AA9F30E090C8EEF5B3B560669F6191F68ADC9956B6768C39FECC01315F08911C6F8FC3D62F18485FBB0FB0C7AD8B4001588666652A3109202C1205F3F9F32C66A1AA179946E7A344A3161BACEF754F9D0

• A'>I4JWL\\ZS`

• 6EC9DFA07A05FF5CA80DE49A415ACA3B3AB28E03DA7D727A9F7CDF47B5800B9CCF26B4BFA4125E212988100F5C7C90DA9E45E096C8EDF1B6B163659D649C8D89DC9550CD0B8B4088CA72375C0CE71F628FC8D52C1C4B5EC90FC1C2D48D30062C8162672E310E20231300F7F7F02962DAD71C9B47E7D446A0101EAAE975419A7

• CoInitialize

• microkernel.dll

• K1aG9]3-D,#0a^gkpygitigmGEK

• 6BB2A4AD7F7DF95DAA72E1EC4158CB4E39B18C78DF0D0F729E79DE34B5FD0EEFCB53B5BEA4115A532A8A11005807

• Bl]}VF^7*8<1;7-:5*:J?SB8I

• D2!BB3O=0J=3J

• -#3XJb]Lg]NiUH`

• U09GVFdBUkVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cUnVuXA==

• 69C9A5AA7F0EF92FAA04E29C3D26

• ./%6:0=;08+$'

• 68B4A4A97C05FA5BAE07E4EA

• 6BB2A4AD7C79F927AB02E09B3A58CE4B3FB78878DC0A737B

• .com6EC7A4DA7C7A

• B9Fd[e?4>C6D

• C5oNHgnjv302ZTY=3C

• !-\'2,"/I=QB8V

• $-6?HAZSle~w

• 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665C542AFB1071587790A29941E0E5C99EF5B3B36865EB649DF68BDC9951B90B833EF8CD7437290C921F1E8FC8AD5E1F4B5EC90FB6C3A28A43055FFF62675F310C2023

• SvOiVv6|TvY>Rv

• 68B5DFAD7A05FE27AF02E0E83D58CE3239C7880CDC78747C9B7CDE47B4810E9FC850B5BDA36F5F222FFA1075587D90A29E30E19BC8E2F1C1B66962E965E0F6FDDCE855CD08833D8CB70F345C09E5

• 6EC9DFAF7D0CFF5C

• SHGetSpecialFolderPathA

• 69B1A4AD7F0FFA5C

• (@4EE1EBEA17D92A4E98A7816B7BEDC09842FD7DDC49CBA9C674062B7ED1D51AD9FAE36CF0136605CCD620151DA61D224B12C401B7764A93A4FBC82B42757B4D7F79418B1A75726B674BCABCAE9705229832603E665EF278F94FB18DDE379ABF04DE5C5B345EAF64A835E803C989B8CD54E02AB6FA7146C9CF1C0ECC4BE0056

• 6FC9D9DD7878FE29AE0DE49B415D

• 69B6DFAA7A79FA5DAA76E09C3A5DCF48

• K>X6,<?7B0'4:0AK>X+

• 1<p)4n-5q;>{bc

•)aV`KIOZ^cBKO

• 6EC6A4AB7F7FFE29AA0DE09D3A5D

• 6BC3A4A17C78

• @6AB6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18802DC0F74799E0FDE34C9F50A9FCA54B4BCA3145F5F2E8E100F597695D9E342E4E2B39F

• 7ac13b3aa82136afa3090c5137

• FileDescription

• 68B5DFAD7A05

- CoUninitialize
- 68C8A4AC7F05F85DAB02E0913D27
- ProductVersion
- 85"/di~sP]JG
- 6EB6A4A0780C
- QPZ;/E]OgdWoQH]
- #&.B@L8.E@2V&
- 69C9DFDE7A79FF5C
- |yz;8=>7412# %&/,)*
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665D232AFC1102587691AF9E48E19AB2EFF3B0B668659E64E4F682DC9851BF0AFB3DF9B603345C0CE11F638FC8AD5E1E385FC30ECCC2A58A4501288565665A350B25251205F085F32C62A0D7609A46E6D241A1146EABED72469A7
- 68C5A4A17F0FFA5B
- 68C5A4A97F0FFA59AA77E0ED3D5CCE4B
- eZjbUkQJWOLURL]63<87A
- 69B1A4AB7C7AFA2EAA0DE1913F58CE3A3DC4890ADF0C747D9F7F
- 68C8A5A87C78FA2BAB04E0EF3D5ACF483DC38878DC79730A9C7FDF37B4F40FEDCB20B5B6A36E5F5F2EFB1171580791AC9C43E297C8ECF3C3B61466996593F3F9DC9F51BF0B8E
- @68B1A5AA7F04FA26AA70E0903F2DCE4E3DC0880BDC0D730F9B7BDA40CC850E95CA5DB5CAA4135F222AFC1102587595AE9F49E090C8EFF1B6B41565EC64E7F183DCEA50B60D893DF8B772355A0CEB1E688BBFD15B183D5DCE0FC7C3A08A3503598516672B310F20231302F781F42A61DBD6119A35E6D143A0126DD7E408409D
- 6AC1A5AC7C05F927AE07E49A402D
- 69B2A5AD7F0F
- /;=?HLGFO2.9
- 68C3DCAB7F79F95EAB04E1EA3A26
- ??2@YAPAXI@Z
- 6AC5A4A97F0AF959AB04
- kpy8;IgitjirigmdbhGEK
- 68C4DFA97D79F826AB70E0913A5BCE4B3EB0890D
- AB7619FB44BAD8BAAE6EBF113B0873FC
- 6EB5DEDA7C7EFA26AA76E4EA3A26CB4E39B18D03D80E720F9F72DF42B4870A98CA26B5BBA4115F5E2A891504587C91DE9E48E4E2B19EF1B2B66966996195F1FDDDE954CB0F8F398ACB00305F09911A6C8ACDD6501C4D5EC90ECDC3A28D30055F8666625C36002750
- 000C29FC2AB3
- b\\m5)?D8NRI]
- kernel32.dll
- 6AC1A5AC7C05F927AE07E49A402DCB4F3AB78D09D8790E729B7DDB46C9F30BEECE55
- d[oOB\\i_l-/0>DKYY_LKUC5onjvZTY
- 68B3A5AA7C7AFA28AA76
- 68C6A5A87F04FA29
- mgzULarf|qcu8,8
- BVF^<1;5*:B8I
- 6EC7A4AB7F0EFA2AAF03E09A3A5CCF49
- 69B5A4A17F0FF82FAA70E1913A5DCA3B38CD887EDC79727A9E0EDF42B5FD0D94CB21B4BBA46F5E21298F10715C7C94DEE241E5E1
- 68C1DCAC7A05FF27AF02E5ED402CCB4F39B18D0CDB0E0E729B73DC32CFF6089BCD55CEBBA3125E5E2A891075597695AD9C32E0E1C8EDF1B4B568659F60978DF8DC9451CB08823DF9B60233290AE21D6F8FC9D55C1D4C5FC80FC6C3A4F631045B8610665E310E5A2C6F00F085F02D61A1D6119E37E6D144A1166EAC9E75359C7
- MCQ_u{ig=3!/
- jko`aecdhNOS
- 89BDD4493961669 26A226D64B4
- 6EC7A4DA7C7AFE29AB02E1EB3A58
- 6BB5A5AF7C7DFE29AB03E0ED3A5FCE4B3EB78C7BDC0D747D9F7E
- 5bOpG4M9,:=2<,"/"
- advapi32.dll
- 68B3A5A07F04FA5DAA77E1913D27CD493EB5880FDF0A74089F7EDE41B4F30FE9
- N@6BB3A5AB7F04F95EAA75E49B3A5ACF3F3DC5887BDC0B0F7C9E72DF45C9F30E95CB50B5B7
- I9K:$6R=FC.7!
- About BDTool

- BDTool, Version 1.0
- bUkSIZQJWROXOLUMHWRL]51<63<65?87A
- `VfL<N`PhL?U
- .2.Q-,X1.`rk
- 4F93E9EF11AC51389EA2846C7B9DC59F388800DE4EB9ACB171732A09D0D41BDCFFE26DFA13637EB8D322116EA11C254C12C100B4774496DDFBB92B40717C4D0A7E328F6F75006C614EBCB8A497055F9433143A675BF37CF832B58CDF3296BA00DE5D5B475EAF64DC34ED02CDF3CECD50E15CCD807444CDCD1D0EC946E771602
- =VLj[ToYUnsp
- zqlgV]@K")4?
- .'<5BKPYfot}
- [X]^WTQRC@EFOLIJkhmngdabspuv
- 6,=:/C.$5c[f
- VVd]\\f]ZckhqUR[
- {pmfW\\AJ#(5>
- tywtsuRQSLKO;<@!"&
- :9;GKPCIPVX`cbkXW`A@J>0
- \',&1-).% "@5==.<\\H_{c
- %,&1% "=.<{c
- |ungXQJC4=&/
- 4:(&|r`nDJXV79+%
- _:/ <;\t"2!;L
- 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 P0, p3pp3rsamp.exe)
    - Thread T3 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - 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)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - Thread Create (Thread ID: T2)
    - Thread Create (Thread ID: T3)
    - 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)
    - RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\000C29FC2AB3 Type: REG_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
    - 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 T2 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**

- Thread Create (Thread ID: TUNKALIAS)

- **Thread T3 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - 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 P0 (p3pp3rsamp.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 (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 (445))
- 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**
    - 44616e530000000000000000000000007b1c0c0001000000c30f5f0004000000831c0e00010000006f1f040002000000362 60b000100000036260a0002000000c30f5d00150000000000010089000000000000000010000000e81f0b00
  - **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'?>
      - Copyright (c) 2010 - 2015 Baidu, Inc. All Rights Reserved.
      - /%+I:>]KRp\\io\\o
      - IsBadReadPtr
      - to~84?>:EhdoWS^}o
      - CLSIDFromProgID
      - a\\kIIULMW][gi`t`TjPIX=9E73?C?K72
      - OriginalFilename
      - IIU][g`Tj=9EC?K
      - <requestedPrivileges>
      - }sqwukiomcage
      - JFQ=:Ca^gVS\\]Og
      - <9BA:ARFRA2@
      - >3$)boxuV[LAal{vUXOB
      - PathFileExistsA
      - A-@L?OOCY.$4"
      - StringFileInfo
      - 6BB1A5AC7F04F927A802E0913D2DCF323DC48C7BDF0E747A9E73DB32B4F60EEACA56CFB7DF635E212A8D1404587794A3E348E5E0C898F4B6B5156698609C8CFEA6E855BF
      - </requestedPrivileges>
      - LCMapStringA
      - </trustInfo>
      - XBZA-@G8FL?OM@VOCY+!2.$4J@P"
      - GetNativeSystemInfo
      - program internal error number is %d.
      - lixRJ[TM\\KCT:5D
      - =:CVS\\eT]E4Oj]u
      - $H7DhU^o\\e}jy
      - GetUserDefaultLCID
      - 3*>D6NRE]LCX
      - CLSIDFromString
      - GetProcAddress
      - 0XJbjUkv_ns_lzky|r
      - ww}cag\\Z`JHN
      - -&;0YRODu~ch
      - -MEj`PrgQnxaw
      - &9;c#%U9:ma[

- RunTime Error:
- ?&:S;M2 -eU`SEK
- 997BA5EA600423CD2830F846EB20A1505CD
- l]|VF^4'5.%/;1>KAQNCW-$8
- 7:- m`wzYTCN
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- InternalName
- CreateThread
- d[o?5LOB\\l\\si_lLFK-/0(,1>DKFHPYY_]\\eLKUD6
- TranslateMessage
- MultiByteToWideChar
- tuyTUY%&*~uqj][
- ghr[UfVMaTM\\KDSB=L?:I
- 86$*p~lbHFTZ
- \\Rc]PfXJbUI]QHURNTPNT9:D**6>=GA>GDCMJIS
- sozkgrPLW<-jSClRE]
- \\Qeqdr`RdfZlldunlxfenVU_SJ^SJ^LERFBMB>J:8D)'
- HCL@0AM:IM7C3
- ;9?=3175+)/-#!'%[Y_]SQWUKIOMCAGE{y
- GetLogicalDriveStringsA
- LegalCopyright
- ??3@YAXPAX@Z
- __CxxFrameHandler
- <0B?0E`Oj[JeTE`UH`ec
- Baidu Pinyin MicroKernel Library
- 2?(%nctyZW@M
- VS_VERSION_INFO
- (L<NQ?V`PhSC[L?U@3Yje
- oVd:".jYbsgm,
- licat@on eqr
- Wow64DisableWow64FsRedirection
- CoCreateInstance
- WideCharToMultiByte
- RtlMoveMemory
- Wow64RevertWow64FsRedirection
- GetModuleHandleA
- GetCommandLineA
- GetTempPathA
- RtlAllocateHeap
- LeaveCriticalSection
- GetProcessHeap
- RegDisableReflectionKey
- CreateDirectoryA
- LoadLibraryA
- GetSystemWow64DirectoryA
- EnterCriticalSection
- RegSetValueExA
- CreateMutexA
- GetModuleFileNameA
- RegCreateKeyExA
- VirtualAlloc
- RegQueryValueExA
- GetEnvironmentVariableA
- InitializeCriticalSection
- GetUserNameA
- RegOpenKeyExA
- PeekMessageA

- DispatchMessageA
- RegEnableReflectionKey
- DeleteCriticalSection
- LookupAccountNameA
- WaitForSingleObject
- ConvertSidToStringSidW
- ReleaseMutex

- **Module 1 other strings**

- 69B1A5AD7F7AFE27AA76E1903D2CCA3D3FB7897EA60874739F7FDA46CFFC0A9ACF26CEB8A4635D242A8D11005C7293A2E246E694B5E9F5B3B114629C619DF3FDDCEA51BF0FF93D83B602355008911A1A8BB9AC511D4A5FC80FB6C3A48D420329851B672D310E20251304F7F2F42A63AAD7169B43E7A343AD176BAC9E75359A0
- 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F30313233343536373738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7
- 68B1A4DE7F0FFA29A904E091
- AO]Sywek1?-#
- 6FC6A4DC780C
- oleaut32.dll
- *!.;1A2&<,#7
- 68B6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18A03A70F720A9D72DE42B4800F94CB21B4B9A4125A552EFC15755E0497AA9F30E090C8EEF5B3B560669F6191F68ADC9956B6768C39FECC01315F08911C6F8FC3D62F18485FBB0FB0C7AD8B4001588666652A3109202C1205F3F9F32C66A1AA179946E7A344A3161BACEF754F9D0
- A'>I4JWL\\ZS`
- 6EC9DFA07A05FF5CA80DE49A415ACA3B3AB28E03DA7D727A9F7CDF47B5800B9CCF26B4BFA4125E212988100F5C7C90DA9E45E096C8EDF1B6B163659D649C8D89DC9550CD0B8B4088CA72375C0CE71F628FC8D52C1C4B5EC90FC1C2D48D30062C8162672E310E20231300F7F7F02962DAD71C9B47E7D446A0101EAAE975419A7
- CoInitialize
- microkernel.dll
- K1aG9]3-D,#0a^gkpygitigmGEK
- 6BB2A4AD7F7DF95DAA72E1EC4158CB4E39B18C78DF0D0F729E79DE34B5FD0EEFCB53B5BEA4115A532A8A11005807
- 5*:J?SB8I
- D2!BB3O=0J=3J
- -#3XJb]Lg]NiUH`
- U09GVFdBUkVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cUnVuXA==
- 69C9A5AA7F0EF92FAA04E29C3D26
- 0=;08+$'
- 68B4A4A97C05FA5BAE07E4EA
- 6BB2A4AD7C79F927AB02E09B3A58CE4B3FB78878DC0A737B
- .com6EC7A4DA7C7A
- B9Fd[e?4>C6D
- C5oNHgnjv302ZTY=3C
- !-\'2,"/I=QB8V
- $-6?HAZSle~w
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665C542AFB1071587790A29941E0E5C99EF5B3B36865EB649DF68BDC9951B90B833EF8CD7437290C921F1E8FC8AD5E1F4B5EC90FB6C3A28A43055FFF62675F310C2023
- SvOiVv6|TvY>Rv
- 68B5DFAD7A05FE27AF02E0E83D58CE3239C7880CDC78747C9B7CDE47B4810E9FC850B5BDA36F5F222FFA1075587D90A29E30E19BC8E2F1C1B66962E965E0F6FDDCE855CD08833D8CB70F345C09E5
- 6EC9DFAF7D0CFF5C
- SHGetSpecialFolderPathA
- 69B1A4AD7F0FFA5C
- (@4EE1EBEA17D92A4E98A7816B7BEDC09842FD7DDC49CBA9C674062B7ED1D51AD9FAE36CF0136605CCD620151DA61D224B12C401B7764A93A4FBC82B42757B4D7F79418B1A75726B674BCABCAE9705229832603E665EF278F94FB18DDE379ABF04DE5C5B345EAF64A835E803C989B8CD54E02AB6FA7146C9CF1C0ECC4BE0056

- 6FC9D9DD7878FE29AE0DE49B415D
- 69B6DFAA7A79FA5DAA76E09C3A5DCF48
- 0AK>X+
- 1<p)4n-5q;>{bc
-)aV`KIOZ^cBKO
- 6EC6A4AB7F7FFE29AA0DE09D3A5D
- 6BC3A4A17C78
- @6AB6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18802DC0F74799E0FDE34C9F50A9FCA54B4BCA3145F5F2E8E100F597695D9E342E4E2B39F
- 7ac13b3aa82136afa3090c5137
- FileDescription
- 68B5DFAD7A05
- CoUninitialize
- 68C8A4AC7F05F85DAB02E0913D27
- ProductVersion
- 85"/di~sP]JG
- 6EB6A4A0780C
- QPZ;/E]OgdWoQH]
- #&.B@L8.E@2V&
- 69C9DFDE7A79FF5C
- |yz;8=>7412# %&/,)*
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665D232AFC1102587691AF9E48E19AB2EFF3B0B668659E64E4F682DC9851BF0AFB3DF9B603345C0CE11F638FC8AD5E1E385FC30ECCC2A58A4501288565665A350B25251205F085F32C62A0D7609A46E6D241A1146EABED72469A7
- 68C5A4A17F0FFA5B
- 68C5A4A97F0FFA59AA77E0ED3D5CCE4B
- eZjbUkQJWOLURL]63<87A
- 69B1A4AB7C7AFA2EAA0DE1913F58CE3A3DC4890ADF0C747D9F7F
- 68C8A5A87C78FA2BAB04E0EF3D5ACF483DC38878DC79730A9C7FDF37B4F40FEDCB20B5B6A36E5F5F2EFB1171580791AC9C43E297C8ECF3C3B61466996593F3F9DC9F51BF0B8E
- @68B1A5AA7F04FA26AA70E0903F2DCE4E3DC0880BDC0D730F9B7BDA40CC850E95CA5DB5CAA4135F222AFC1102587595AE9F49E090C8EFF1B6B41565EC64E7F183DCEA50B60D893DF8B772355A0CEB1E688BBFD15B183D5DCE0FC7C3A08A3503598516672B310F20231302F781F42A61DBD6119A35E6D143A0126DD7E408409D
- 6AC1A5AC7C05F927AE07E49A402D
- 69B2A5AD7F0F
- /;=?HLGFO2.9
- 68C3DCAB7F79F95EAB04E1EA3A26
- ??2@YAPAXI@Z
- 6AC5A4A97F0AF959AB04
- kpy8;IgitjirigmdbhGEK
- 68C4DFA97D79F826AB70E0913A5BCE4B3EB0890D
- AB7619FB44BAD8BAAE6EBF113B0873FC
- 6EB5DEDA7C7EFA26AA76E4EA3A26CB4E39B18D03D80E720F9F72DF42B4870A98CA26B5BBA4115F5E2A891504587C91DE9E48E4E2B19EF1B2B66966996195F1FDDDE954CB0F8F398ACB00305F09911A6C8ACDD6501C4D5EC90ECDC3A28D30055F8666625C36002750
- 000C29FC2AB3
- b\\m5)?D8NRI]
- kernel32.dll
- 6AC1A5AC7C05F927AE07E49A402DCB4F3AB78D09D8790E729B7DDB46C9F30BEECE55
- d[oOB\\i_l-/0>DKYY_LKUC5onjvZTY
- 68B3A5AA7C7AFA28AA76
- 68C6A5A87F04FA29
- mgzULarf|qcu8,8
- B8I
- 6EC7A4AB7F0EFA2AAF03E09A3A5CCF49
- 69B5A4A17F0FF82FAA70E1913A5DCA3B38CD887EDC79727A9E0EDF42B5FD0D94CB21B4BBA46F5E21298F10715C7C94DEE241E5E1
- 68C1DCAC7A05FF27AF02E5ED402CCB4F39B18D0CDB0E0E729B73DC32CFF6089BCD55CEBBA3125E5E2A891075597695AD9C32E0E1C8EDF1B4B568659F60978DF8DC9451CB08823DF9B60233290AE21D6F8FC9D55C1D4C5FC80FC6C3A4F631045B8610665E310E5A2C6F00F085F02D61A1D6119E37E6D144A1166EAC9E75359C7

- MCQ_u{ig=3!/
- jko`aecdhNOS
- 89BDD449396166926A226D64B4
- 6EC7A4DA7C7AFE29AB02E1EB3A58
- 6BB5A5AF7C7DFE29AB03E0ED3A5FCE4B3EB78C7BDC0D747D9F7E
- =2<,"/"
- advapi32.dll
- 68B3A5A07F04FA5DAA77E1913D27CD493EB5880FDF0A74089F7EDE41B4F30FE9
- N@6BB3A5AB7F04F95EAA75E49B3A5ACF3F3DC5887BDC0B0F7C9E72DF45C9F30E95CB50B5B7
- $6R=FC.7!
- bUkSIZQJWROXOLUMHWRL]51<63<65?87A
- `VfL<N`PhL?U
- .2.Q-,X1.`rk
- 4F93E9EF11AC51389EA2846C7B9DC59F388800DE4EB9ACB171732A09D0D41BDCFFE26DFA13637EB8D322116EA11C254C12C100B4774496DDFBB92B40717C4D0A7E328F6F75006C614EBCB8A497055F9433143A675BF37CF832B58CDF3296BA00DE5D5B475EAF64DC34ED02CDF3CECD50E15CCD807444CDCD1D0EC946E771602
- =VLj[ToYUnsp
- zqlgV]@K")4?
- .'<5BKPYfot}
- [X]^WTQRC@EFOLIJkhmngdabspuv
- /C.$5c[f
- VVd]\\f]ZckhqUR[
- {pmfW\\AJ#(5>
- tywtsuRQSLKO;<@!"&
- 9;GKPCIPVX`cbkXW`A@J>0
- \',&1-).% "@5==.<\\H_{c
- %,&1% "=.<{c
- |ungXQJC4=&/
- (&|r`nDJXV79+%

Module 2 (probably unpacked / injected by the sample)

Module 2 rich signatures

- 44616e530000000000000000000000007b1c0c0001000000c30f5f0004000000831c0e00010000006f1f040002000000362 60b000100000036260a0002000000c30f5d00150000000000010089000000000000000010000 00e81f0b00

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'?>
- Copyright (c) 2010 - 2015 Baidu, Inc. All Rights Reserved.
- /%+I:>]KRp\\io\\o
- IsBadReadPtr
- to~84?>:EhdoWS^}o
- CLSIDFromProgID
- a\\kIIULMW][gi`t`TjPIX=9E73?C?K72
- OriginalFilename
- IIU][g`Tj=9EC?K
- <requestedPrivileges>
- }sqwukiomcage

- JFQ=:Ca^gVS\\]Og
- <9BA:ARFRA2@
- >3$)boxuV[LAal{vUXOB
- PathFileExistsA
- A-@L?OOCY.$4"
- StringFileInfo
- 6BB1A5AC7F04F927A802E0913D2DCF323DC48C7BDF0E747A9E73DB32B4F60EEACA56CFB7DF635E212A8D1404587794A3E348E5E0C898F4B6B5156698609C8CFEA6E855BF
- </requestedPrivileges>
- LCMapStringA
- </trustInfo>
-)D\t(549"5,.fO
- XBZA-@G8FL?OM@VOCY+!2.$4J@P"
- GetNativeSystemInfo
- program internal error number is %d.
- lixRJ[TM\\KCT:5D
- =:CVS\\eT]E4Oj]u
- $H7DhU^o\\e}jy
- GetUserDefaultLCID
- 3*>D6NRE]LCX
- CLSIDFromString
- GetProcAddress
- 0XJbjUkv_ns_lzky|r
- ww}cag\\Z`JHN
- -&;0YRODu~ch
- -MEj`PrgQnxaw
- &9;c#%U9:ma[
- RunTime Error:
- ?&:S;M2 -eU`SEK
- 997BA5EA600423CD2830F846EB20A1505CD
- l]|VF^4'5.%/;1>KAQNCW-$8
- 7:- m`wzYTCN
- <requestedExecutionLevel level='asInvoker' uiAccess='false' />
- InternalName
- CreateThread
- d[o?5LOB\\l\\si_lLFK-/0(,1>DKFHPYY_]\\eLKUD6
- TranslateMessage
- MultiByteToWideChar
- tuyTUY%&*~uqj][
- ghr[UfVMaTM\\KDSB=L?:I
- 86$*p~lbHFTZ
- \\Rc]PfXJbUI]QHURNTPNT9:D**6>=GA>GDCMJIS
-]pA]HT]\\RY6k
- Copyright (C) 2011
- sozkgrPLW<-jSClRE]
- \\Qeqdr`RdfZlldunlxfenVU_SJ^SJ^LERFBMB>J:8D)'
- HCL@0AM:IM7C3
- ;9?=3175+)/-#!'%[Y_]SQWUKIOMCAGE{y
- GetLogicalDriveStringsA
- LegalCopyright
- ??3@YAXPAX@Z
- __CxxFrameHandler
- <0B?0E`Oj[JeTE`UH`ec
- Baidu Pinyin MicroKernel Library
- 2?(%nctyZW@M
- VS_VERSION_INFO
- (L<NQ?V`PhSC[L?U@3Yje

- oVd:".jYbsgm,
- licat@on eqr
- Wow64DisableWow64FsRedirection
- CoCreateInstance
- WideCharToMultiByte
- RtlMoveMemory
- Wow64RevertWow64FsRedirection
- GetModuleHandleA
- GetCommandLineA
- GetTempPathA
- RtlAllocateHeap
- LeaveCriticalSection
- GetProcessHeap
- RegDisableReflectionKey
- CreateDirectoryA
- LoadLibraryA
- GetSystemWow64DirectoryA
- EnterCriticalSection
- RegSetValueExA
- CreateMutexA
- GetModuleFileNameA
- RegCreateKeyExA
- VirtualAlloc
- RegQueryValueExA
- GetEnvironmentVariableA
- InitializeCriticalSection
- GetUserNameA
- RegOpenKeyExA
- PeekMessageA
- DispatchMessageA
- RegEnableReflectionKey
- DeleteCriticalSection
- LookupAccountNameA
- WaitForSingleObject
- ConvertSidToStringSidW
- ReleaseMutex

- **Module 2 other strings**

- 69B1A5AD7F7AFE27AA76E1903D2CCA3D3FB7897EA60874739F7FDA46CFFC0A9ACF26CEB8A4635D242A8D11005C7293A2E246E694B5E9F5B3B114629C619DF3FDDCEA51BF0FF93D83B602355008911A1A8BB9AC511D4A5FC80FB6C3A48D420329851B672D310E20251304F7F2F42A63AAD7169B43E7A343AD176BAC9E75359A0
- 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7
- 68B1A4DE7F0FFA29A904E091
- AO]Sywek1?-#
- 6FC6A4DC780C
- oleaut32.dll
- *!.;1A2&<,#7
- 68B6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18A03A70F720A9D72DE42B4800F94CB21B4B9A4125A552EFC15755E0497AA9F30E090C8EEF5B3B560669F6191F68ADC9956B6768C39FECC01315F08911C6F8FC3D62F18485FBB0FB0C7AD8B4001588666652A3109202C1205F3F9F32C66A1AA179946E7A344A3161BACEF754F9D0
- A'>I4JWL\\ZS`
- 6EC9DFA07A05FF5CA80DE49A415ACA3B3AB28E03DA7D727A9F7CDF47B5800B9CCF26B4BFA4125E212988100F5C7C90DA9E45E096C8EDF1B6B163659D649C8D89DC9550CD0B8B4088CA72375C0CE71F628FC8D52C1C4B5EC90FC1C2D48D30062C8162672E310E20231300F7F7F02962DAD71C

9B47E7D446A0101EAAE975419A7

- CoInitialize
- microkernel.dll
- K1aG9]3-D,#0a^gkpygitigmGEK
- 6BB2A4AD7F7DF95DAA72E1EC4158CB4E39B18C78DF0D0F729E79DE34B5FD0EEFCB53B5BEA4115A532A8A11005807
- 5*:J?SB8I
- D2!BB3O=0J=3J
- -#3XJb]Lg]NiUH`
- U09GVFdBUkVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cUnVuXA==
- About BDTool
- 69C9A5AA7F0EF92FAA04E29C3D26
- 0=;08+$'
- 68B4A4A97C05FA5BAE07E4EA
- 6BB2A4AD7C79F927AB02E09B3A58CE4B3FB78878DC0A737B
- .com6EC7A4DA7C7A
- B9Fd[e?4>C6D
- C5oNHgnjv302ZTY=3C
- !-\'2,"/I=QB8V
- $-6?HAZSle~w
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665C542AFB1071587790A29941E0E5C99EF5B3B36865EB649DF68BDC9951B90B833EF8CD7437290C921F1E8FC8AD5E1F4B5EC90FB6C3A28A43055FFF62675F310C2023
- SvOiVv6|TvY>Rv
- 68B5DFAD7A05FE27AF02E0E83D58CE3239C7880CDC78747C9B7CDE47B4810E9FC850B5BDA36F5F222FFA1075587D90A29E30E19BC8E2F1C1B66962E965E0F6FDDCE855CD08833D8CB70F345C09E5
- 6EC9DFAF7D0CFF5C
- SHGetSpecialFolderPathA
- 69B1A4AD7F0FFA5C
- (@4EE1EBEA17D92A4E98A7816B7BEDC09842FD7DDC49CBA9C674062B7ED1D51AD9FAE36CF0136605CCD620151DA61D224B12C401B7764A93A4FBC82B42757B4D7F79418B1A75726B674BCABCAE9705229832603E665EF278F94FB18DDE379ABF04DE5C5B345EAF64A835E803C989B8CD54E02AB6FA7146C9CF1C0ECC4BE0056
- 6FC9D9DD7878FE29AE0DE49B415D
- 69B6DFAA7A79FA5DAA76E09C3A5DCF48
- 0AK>X+
- 1<p)4n-5q;>{bc
-)aV`KIOZ^cBKO
- 6EC6A4AB7F7FFE29AA0DE09D3A5D
- 6BC3A4A17C78
- @6AB6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18802DC0F74799E0FDE34C9F50A9FCA54B4BCA3145F5F2E8E100F597695D9E342E4E2B39F
- 7ac13b3aa82136afa3090c5137
- FileDescription
- 68B5DFAD7A05
- CoUninitialize
- 68C8A4AC7F05F85DAB02E0913D27
- ProductVersion
- 85"/di~sP]JG
- 6EB6A4A0780C
- QPZ;/E]OgdWoQH]
- #&.B@L8.E@2V&
- 69C9DFDE7A79FF5C
- |yz;8=>7412# %&/,)*
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665D232AFC1102587691AF9E48E19AB2EFF3B0B668659E64E4F682DC9851BF0AFB3DF9B603345C0CE11F638FC8AD5E1E385FC30ECCC2A58A4501288565665A350B25251205F085F32C62A0D7609A46E6D241A1146EABED72469A7
- 68C5A4A17F0FFA5B
- 68C5A4A97F0FFA59AA77E0ED3D5CCE4B
- eZjbUkQJWOLURL]63<87A
- 69B1A4AB7C7AFA2EAA0DE1913F58CE3A3DC4890ADF0C747D9F7F

• 68C8A5A87C78FA2BAB04E0EF3D5ACF483DC38878DC79730A9C7FDF37B4F40FEDCB20B5B6A36E5F5F2EFB1171580791AC9C43E297C8ECF3C3B61466996593F3F9DC9F51BF0B8E
• @68B1A5AA7F04FA26AA70E0903F2DCE4E3DC0880BDC0D730F9B7BDA40CC850E95CA5DB5CAA4135F222AFC1102587595AE9F49E090C8EFF1B6B41565EC64E7F183DCEA50B60D893DF8B772355A0CEB1E688BBFD15B183D5DCE0FC7C3A08A3503598516672B310F20231302F781F42A61DBD6119A35E6D143A0126DD7E408409D
• 6AC1A5AC7C05F927AE07E49A402D
• 69B2A5AD7F0F
• /;=?HLGFO2.9
• 68C3DCAB7F79F95EAB04E1EA3A26
• ??2@YAPAXI@Z
• 6AC5A4A97F0AF959AB04
• kpy8;IgitjirigmdbhGEK
• 68C4DFA97D79F826AB70E0913A5BCE4B3EB0890D
• AB7619FB44BAD8BAAE6EBF113B0873FC
• 6EB5DEDA7C7EFA26AA76E4EA3A26CB4E39B18D03D80E720F9F72DF42B4870A98CA26B5BBA4115F5E2A891504587C91DE9E48E4E2B19EF1B2B66966996195F1FDDDE954CB0F8F398ACB00305F09911A6C8ACDD6501C4D5EC90ECDC3A28D30055F8666625C36002750
• BDTool, Version 1.0
• 000C29FC2AB3
• b\\m5)?D8NRI]
• kernel32.dll
• 6AC1A5AC7C05F927AE07E49A402DCB4F3AB78D09D8790E729B7DDB46C9F30BEECE55
• d[oOB\\i_l-/0>DKYY_LKUC5onjvZTY
• 68B3A5AA7C7AFA28AA76
• 68C6A5A87F04FA29
• mgzULarf|qcu8,8
• B8I
• 6EC7A4AB7F0EFA2AAF03E09A3A5CCF49
• 69B5A4A17F0FF82FAA70E1913A5DCA3B38CD887EDC79727A9E0EDF42B5FD0D94CB21B4BBA46F5E21298F10715C7C94DEE241E5E1
• 68C1DCAC7A05FF27AF02E5ED402CCB4F39B18D0CDB0E0E729B73DC32CFF6089BCD55CEBBA3125E5E2A891075597695AD9C32E0E1C8EDF1B4B568659F60978DF8DC9451CB08823DF9B60233290AE21D6F8FC9D55C1D4C5FC80FC6C3A4F631045B8610665E310E5A2C6F00F085F02D61A1D6119E37E6D144A1166EAC9E75359C7
• MCQ_u{ig=3!/
• jko`aecdhNOS
• 89BDD449396166926A226D64B4
• 6EC7A4DA7C7AFE29AB02E1EB3A58
• 6BB5A5AF7C7DFE29AB03E0ED3A5FCE4B3EB78C7BDC0D747D9F7E
• =2<,"/"
• advapi32.dll
• 68B3A5A07F04FA5DAA77E1913D27CD493EB5880FDF0A74089F7EDE41B4F30FE9
• N@6BB3A5AB7F04F95EAA75E49B3A5ACF3F3DC5887BDC0B0F7C9E72DF45C9F30E95CB50B5B7
• $6R=FC.7!
• bUkSIZQJWROXOLUMHWRL]51<63<65?87A
• `VfL<N`PhL?U
• .2.Q-,X1.`rk
• 4F93E9EF11AC51389EA2846C7B9DC59F388800DE4EB9ACB171732A09D0D41BDCFFE26DFA13637EB8D322116EA11C254C12C100B4774496DDFBB92B40717C4D0A7E328F6F75006C614EBCB8A497055F9433143A675BF37CF832B58CDF3296BA00DE5D5B475EAF64DC34ED02CDF3CECD50E15CCD807444CDCD1D0EC946E771602
• =VLj[ToYUnsp
• zqlgV]@K")4?
• .'<5BKPYfot}
• [X]^WTQRC@EFOLIJkhmngdabspuv
• /C.$5c[f
• VVd]\\f]ZckhqUR[
• {pmfW\\AJ#(5>
• tywtsuRQSLKO;<@!"&
• 9;GKPCIPVX`cbkXW`A@J>0
• \',&1-).% "@5==.<\\H_{c

- / <;\t"2!;L
- %,&1% "=.<{c
- |ungXQJC4=&/
- (&|r`nDJXV79+%
- MS Shell Dlg

Extra Information Recovered

In this section there is additional information recovered by platform plugins

- **DecryptedString**

ScriptControl

Language

VBScript

ExecuteStatement

```
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
```

Run

MACAddress

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;}

JScript

lakwi

Software\\Microsoft\\Internet Explorer\\Main\\Start Page

www.naver.com

0.0.0.0

.com.ows

.kr

.kr.ows

ET

step_down.php?key=9ea8e376b5cd1274

HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: text/plain
Content-Length:

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

ScriptControl

Language

VBScript

ExecuteStatement

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

Run

MACAddress

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;}

JScript

lakwi

Software\\Microsoft\\Internet Explorer\\Main\\Start Page

www.naver.com

0.0.0.0

.com.ows

.kr

.kr.ows

ET

step_down.php?key=9ea8e376b5cd1274

HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: text/plain
Content-Length:

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
```

```
ScriptControl
```

```
Language
```

```
VBScript
```

```
ExecuteStatement
```

```
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
```

```
Run
```

```
MACAddress
```

```
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;}

JScript

lakwi

Software\\Microsoft\\Internet Explorer\\Main\\Start Page

www.naver.com

0.0.0.0

.com.ows

.kr

.kr.ows

ET

step_down.php?key=9ea8e376b5cd1274

HTTP/1.1 200 OK

```
Accept-Ranges: bytes
Content-Type: text/plain
Content-Length:

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