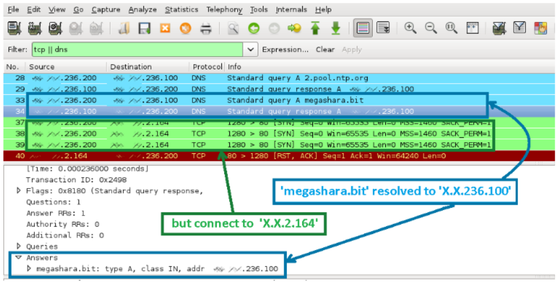
Necurs C&C – Part-2

| By Atinderpal Singh | 0 comments

In Part 1 of this post i discussed what is decentralized domain name system and how Necurs is using it to avoid take-down. Then i got busy with other regular work and did not do further analysis. but recently i got some time and did some further analysis that i will share in this blog post.

Necurs is using decentralized top level domain '.bit' that makes take-down of Necurs C&C theoretically impossible but it is not true in reality, it is still dependent on Namecoin DNS servers in its configuration file to resolve domain names. Whose records can be altered to point to sinkhole and can be used to take-down this botnet. And that Domain history can be analyzed to get list of IP addresses pointed by that domain at any time. Those IP's can be used for further analysis and as evidence during take-down.

Don't get excited just yet. Necurs has some more tricks up to its Sleeve. Even if you manage to get list of IP addresses pointed by some C&C domain of Necurs it wont lead you anywhere or may mislead you. As DNS server returned IP and contacted IP is different.



The IP with which Necurs tries to communicate where did it came from is it hard-coded?

Why it did not contact resolved IP?

This is another trick of Necurs to conceal its Command server infrastructure and make analysis difficult. Necurs does not directly contacts to IP address returned by DNS. It checks its configuration file and if option is specified it modifies IP returned using Rotation and shift operations and contacts modified IP. Following code is used to manipulate returned IP to get real IP of C&C server:

```
pusn    eqi
push    0F6E2C493h
push    0F6F91281h
mov     esi, [ebp+edx*4+bitResolvedIP_var_118]
mov     [ebp+bitResolvedIP_var_8], esi
call    cmdSearch               ; ManipulateIP?
add     esp, 0Ch
test    eax, eax
jz      loc_4016A1
```

Yes No

```
ManipulateIP_:
push    edi
push    514BB920h
push    48028C4Eh
call    cmdSearch               ; Count 5
mov     ecx, eax                ; returned value
imul    eax, 988355h
imul    ecx, 980A0Bh
shr     ecx, 08h
add     ecx, 9CE283Ah
xor     ecx, eax
mov     bl, cl
mov     edx, esi                ; esi=ResolvedIP
add     esp, 0Ch
rol     edx, 3
shl     bl, 2
mov     al, dl
sub     al, bl
sub     al, 5Ch
ror     al, 3
mov     [ebp+var_3], al
mov     eax, ecx
imul    ecx, 58860h
rol     eax, 5
movzx   esi, dl
xor     eax, esi
sub     ecx, eax
mov     esi, ecx
mov     ecx, edx
shr     ecx, 8
movzx   eax, cl
mov     ebx, esi
imul    esi, 8679Eh
rol     ebx, 3
imul    ebx, eax
add     ebx, esi
mov     eax, edx
shr     eax, 10h
mov     [ebp+var_1], al
mov     [ebp+var_2], cl
mov     eax, ebx
shr     eax, 6
rol     al, cl
mov     cl, [ebp+var_1]
sub     cl, al
mov     al, [ebp+var_1]
add     al, 29h
ror     cl, 5
imul    bl
movzx   esi, cl                 ; esi = CL 00 00 00(CL.X.X.X)
mov     cl, dl
shr     cl, 1
shr     edx, 18h
ror     dl, cl
mov     ecx, ebx
rol     ecx, 1
xor     cl, al
sub     dl, cl
sub     dl, bl
movzx   eax, dl
shl     eax, 8                  ; eax = 00  00  EAX 00
or      esi, eax                ; esi = CL  EAX 00  00 (CL.EAX.X.X)
mov     al, [ebp+var_2]
sub     al, 1Fh
shl     esi, 8                  ; esi = 00  EAX CL  00 (00.CL.EAX.X)
movzx   eax, al
or      esi, eax                ; esi = 00  EAX CL  AL[var_2-0x1F](AL.CL.EAX.X)
movzx   eax, [ebp+var_3]
shl     esi, 8                  ; esi = EAX CL  AL  00 (X.AL.XL.EAX)
or      esi, eax                ; esi = EAX CL  AL  var_3 (var_3.AL.CL.EAX)
ror     esi, 3
mov     [ebp+bitResolvedIP_var_8], esi
```

```
loc_4016A1:
cmp     [ebp+bitResolvedIP_var_8], edi
jz      short loc_4016C1
```

This is image caption — Resolved IP modification

So for sinkholing or taking over DNS server requires knowledge of this feature. This is not the only method it uses to communicate to C&C it also has DGA (Domain Generation Algorithm) as a fallback mechanism. DGA and Communication with server will be covered in subsequent blog when i get more time to work on Necurs 😀

Leave a Reply

Logged in as Atinderpal Singh. Log out »

Submit Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.