RESOURCES

## norman**shark**

#### Actionable Intelligence for Malware Defense.

SUPPORT

in Share

**NEWS & MEDIA** 

▼Tweet <0
</p>

COMPANY

REQUEST DEMO

VIEW

OUR BLOG

"In today's climate of

persistent threats, network defense

alone is no longer enough. In order to

the proliferation of

analysts need

intelligence

dynamic malware

them to respond

an incursion."

protect networks from

targeted attacks and unknown threats,

capabilities that allow

quickly in the event of

WEBINAR

TRY
NORMAN SHARK

# Blog » Necurs C&C - Part-2

Blog

THREAT PROTECTION



#### Necurs C&C - Part-2

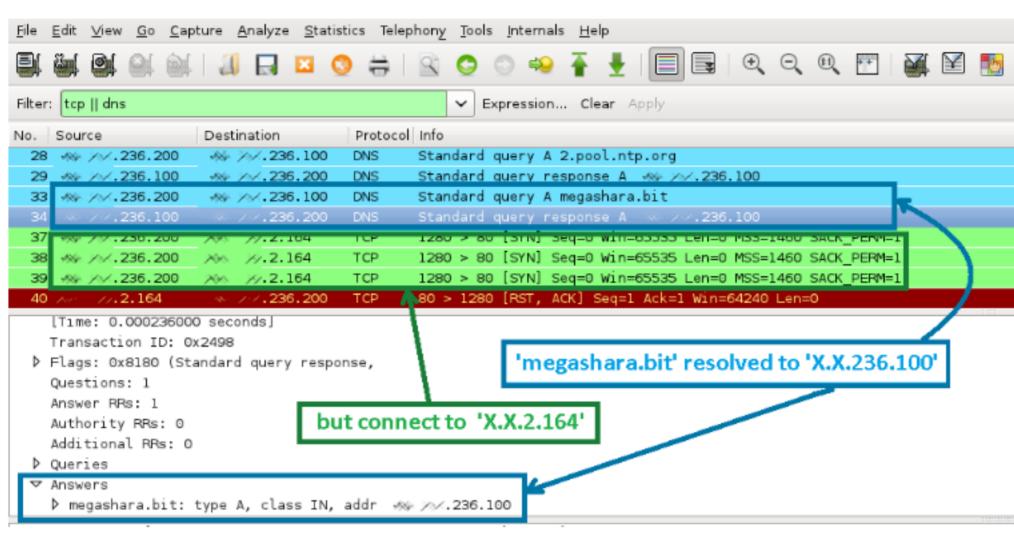
PRODUCTS & SOLUTIONS

| 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
        ea1
        0F6E2C493h
push
        0F6F91281h
push
        esi, [ebp+edx*4+bitResolvedIP_var_118]
MOV
        [ebp+bitResolvedIP var_8], esi
mov
call
        cmdSearch
                                  ; ManipulateIP?
        esp, OCh
add
test
        eax, eax
        1oc_4016A1
jΖ
                                                  Yes
                                                                    No
         🜃 🅰 🖭
        |ManipulateIP_:
                 edi
        push
                 5148B920h
        push
                 48028C4Eh
        push
                                           ; Count 5
        call
                 cmdSearch
                                           ; returned value
        mov
                 ecx, eax
        imul
                 eax, 988355h
        imul
                 ecx, 9BOABh
        shr
                 ecx, OBh
                 ecx, 9CE283Ah
        add
        xor
                 ecx, eax
                 b1, c1
        MOV
                                           : esi=ResolvedIP
        mov
                 edx, esi
                 esp, OCh
        add
                 edx, 3
        rol
                 b1, 2
        shl
                 al, dl
        mov
                 al, bl
        sub
                 al, 5Ch
        sub
                 al, 3
        ror
                 [ebp+var_3], al
        mov
        mov
                 eax, ecx
        imul
                 ecx, 5B860h
        rol
                 eax, 5
                 esi, dl
        MOVZX
        xor
                 eax, esi
                 ecx, eax
        sub
                 esi, ecx
         mov
                 ecx, edx
        mov
        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
                 [ebp+var_2], cl
         mov
                 eax, ebx
        mov
        shr
                 eax, 6
        rol
                 al, cl
        mov
                 cl, [ebp+var_1]
        sub
                 cl, al
        mov
                 al, [ebp+var_1]
        add
                 al, 29h
                 cl, 5
        ror
        imul
                 b1
                                           ; esi = CL 00 00 00(CL.X.X.X)
        MOVZX
                 esi, cl
                 cl, dl
        mov
                 cl, 1
        shr
                 edx, 18h
        shr
        ror
                 dl, cl
        mov
                 ecx, ebx
         rol
                 ecx, 1
        xor
                 cl, al
        sub
                 dl, cl
         sub
                 d1, b1
         MOVZX
                 eax, dl
        sh1
                 eax, 8
                                           ; eax = 00 00 EAX 00
                                           ; esi = CL EAX 00 00 (CL.EAX.X.X)
        or
                 esi, eax
        mov
                 al, [ebp+var_2]
         sub
                 al, 1Fh
                                           ; esi = 00 EAX CL 00 (00.CL.EAX.X)
        shl
                 esi, 8
         MOVZX
                 eax, al
                                           or
                 esi, eax
         MOVZX
                 eax, [ebp+var_3]
        sh1
                 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
                 [ebp+bitResolvedIP_var_8], esi
        mov
                                🜃 🅰 🖭
                               loc_4016A1:
                               cmp
                                       [ebp+bitResolvedIP_var_8], edi
                                       short loc_4016C1
```

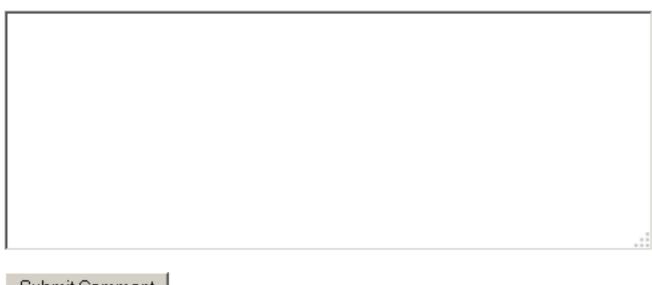
### This is image caption

## 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 »



jΖ

## Submit Comment

- Notify me of follow-up comments by email.
- Notify me of new posts by email.

THREAT PROTECTION PRODUCTS &

norman*shark* Copyright Norman Shark I sitemap

» Automated Malware Analysis

» Build vs. Buy

» Advanced Targeted Attacks

» Products » Technology

SOLUTIONS

» Solutions

» Datasheets » Case Studies » Whitepapers

» Videos

» Featured Research

RESOURCES

**NEWS & MEDIA** » In the News

» Press Releases » Events

» Press Kit » Blog

**O (1) (2)** 

COMPANY

**SUPPORT** 

» Manuals

» Careers

» Company Overview » Management Team