NEWS & MEDIA

™ Tweet <0

RESOURCES

Blog



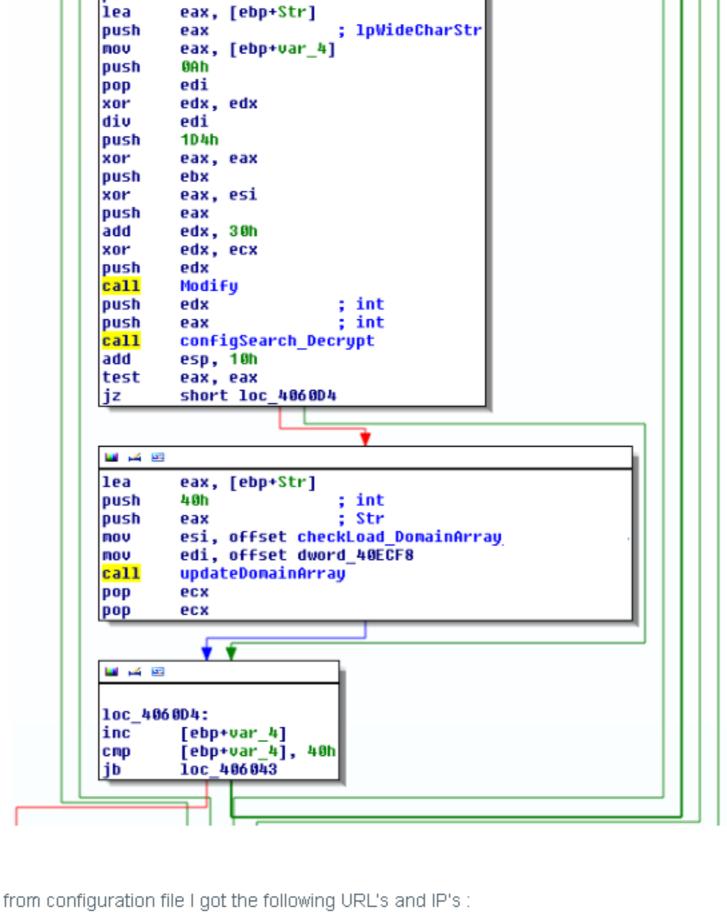
2013.09.10 | By Atinderpal Singh | 2 comments

In November 2012 Necurs malware came in the limelight when Microsoft reported 83000+ infections. After that it was not very active. Some time back it started to show activity again. I started following new samples. As I was analyzing one of the samples I found something that I have never seen in any other malware. I checked some old samples and found that it was doing it for quite some time and had not caught anyone's attention.

Here are the things I am going to discuss in this blog:

- » Domain and IP's in Necurs config file » What is .bit domain?
- » What is Namecoin?
- » What is the use of Decentralized DNS?
- » How to access .bit domains? » IP addresses from configuration
- » How Necurs access .bit domains? (update)
- » Conclusion

loc 406080: ; cchWideChar push



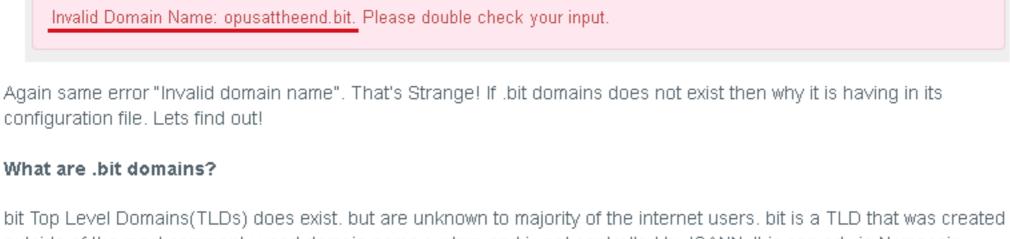
	95.211.195.245	178.63.16.21	
21	in name probably belong to Command ain name" error.	and Control server. I tried Whois look	cup for this domain name
w .is Sear	rch Domain name or IP address	Q Se	earch by Name Server
RROR			×
valid Domain N	ama: magashara hit. Plaasa doubla chack	vour input	

who.is Q, Search Domain name or IP address

Why is it having an invalid domain name in configuration file? Is it by mistake?

ERROR ×

To find out I extracted "opusattheend.bit" domain name from old Necurs sample compiled on 18/10/2009 and tried whois



What is Namecoin?

Probably you all heard of Bitcoin currency. There is one another similar

currency named Namecoin based on exactly the same code as Bitcoin with different blockchain. Bitcoin and Namecoin blockchains are independent and cannot interfere with each other. Namecoin extends Bitcoin to add transaction for registering updating and transferring names. Basically the idea was to develop a decentralized DNS without any trusted third party.



AS no.

A53842

AS3842

AS198203

AS16265

AS46475

Company

RamNodeLLC

RamNodeLLC

LeaseWeb B.V.

RouteLabel V.O.F.

Limestone Networks,

Search by Name Server

How to access .bit domains?

Trade and transact namecoins, the digital currency NMC.

If we try to directly access any .bit domain from browser it wont be able to resolve domain as bit domains are not supported by traditional DNS servers. Then how do we access bit domains?

» Attach values to the names (up to 1023 bytes)

What is the use of Decentralized DNS?

proxy settings for bit domains.

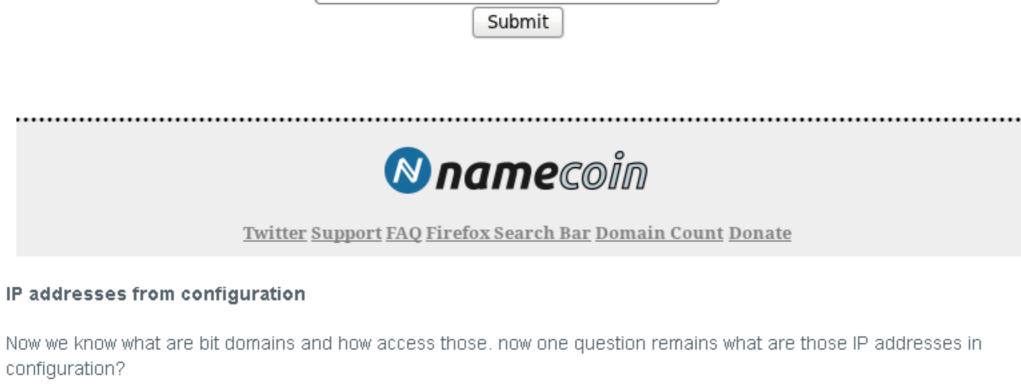
bitse.bit

🛂 bitSE.bit - Your .bit Search Engine 📗 🌩

Accessing bit domains requires a copy of Namecoin blockchain or a supporting public DNS server or a proxy. For details methods of accessing bit domains visit dot-bit website. At the time of writing 83516 no of .bit domains were registered.

page:

8 ∨ Google



Your .bit Search Engine

176.56.238.160 176.56.238.160 lw177.ua-hosting.com.ua 95.211.195.245 60-48-31-64.31.48.60

to .bit TLD is specified in parameters:

🜃 🅰 😐

rndm

call

xor div

MOV

🜃 🎿 🔤

push

MOV

lea

push

push

push

push

push

mov

xor

MOV

call

test

jnz

1ea

loc_40152B:

edi

eax

eax 0C8h

esi

ebx, ebx

eax, eax 1oc 4016C1

DnsQuery_W

IP

192.249.59.89

192.184.89.74

64.static.reverse.lstn.net Inc. DE, Germany Hetzner Online AG dotbit.me 178.63.16.21 AS24940 dns.dot-bit.org OVH Systems 178.32.31.41 FR, France AS16276

🜃 🅰 😐 ; ".bit" offset Str2 push ; Str1 push eax ds:_wcsicmp call pop ecx pop ecx test eax, eax short loc_4062B1 jnz

eax, [ebp+Args]

ecx

ecx, ecx

eax, edi

ResolveDomainName

If domain contains .bit ResolveDomainName is called to resolve it by calling DnsQuery_W with IP for DNS server belonging

; lpCriticalSection

🜃 🅰 🖭

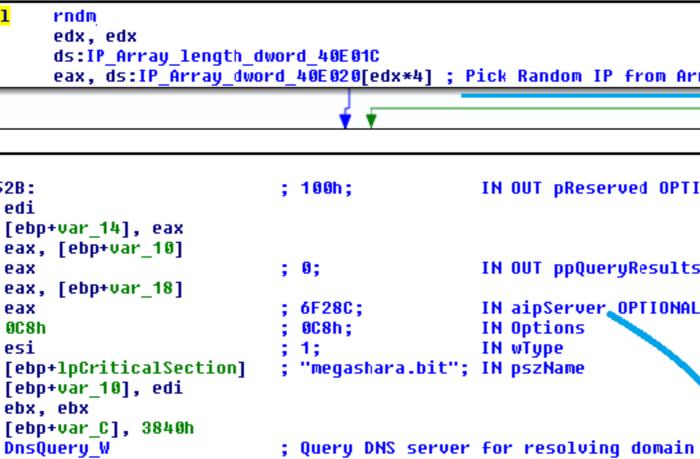
1ea

push call

pop xor

cmp

setnz



aipServers [in] Specifies the DNS servers to which the query should be sent. If this is NULL, default DNS servers for the local computer are used. This parameter is optional. Windows Embedded CE supports a maximum of one server listed in this parameter. Address Hex dump ASCII 0006F28C 01 00 00 00 B2 20 1F 29 00 00 00 00 40 38 00 00 ■...² ■)....@8.. ชชช6⊦29℃ 00 00 00 0<mark>0 00 เร ช ช ช ช 50 50 00 5</mark>0 62 40 00ù∎..ù∎.\b@. 0006F2AC BC F4 50 00 00 00 00 10 50 30 00 3C FB 06 00 ¼ô∎.....⊪P6.<û∎. 0006F2BC <mark>69 00</mark> 74 00 74 00 70 00 3A 00 2F 00 2r 29 6D 00 h.t.t.p.:././.m. 0006F2CC 1 00 e.g.a.s.h.a.r.a. 6 00 ..b.i.t...∎|..6. 0006F2DC 172.32.31.41 -> dns.dot-bit.org 6 00 a∎.Pdw'|..6.∎K6. 0006F2EC 0006F2FC 0 00 a∎.@ Ø.....8... 0006F30C 00 00 00 00 30 E2 09 00 EA 76 92 7C 00 00 08 000â..êv'|..**≡**. 0006F31C 01 00 00 00 71 00 00 00 F8 50 36 00 A8 4B 36 00 ■...q...øP6."K6. 0006F32C 01 00 00 00 58 D5 09 00 00 00 08 00 68 00 00 00 ■...XÕ....■.h... 0006F33C 00 00 00 00 E0 01 00 00 02 00 00 00 2C F4 06 00à■...■...,ô■.

» Very easy to register and update domain.

Other malwares are likely to adopt similar techniques to resist Command server takedowns by Authorities.

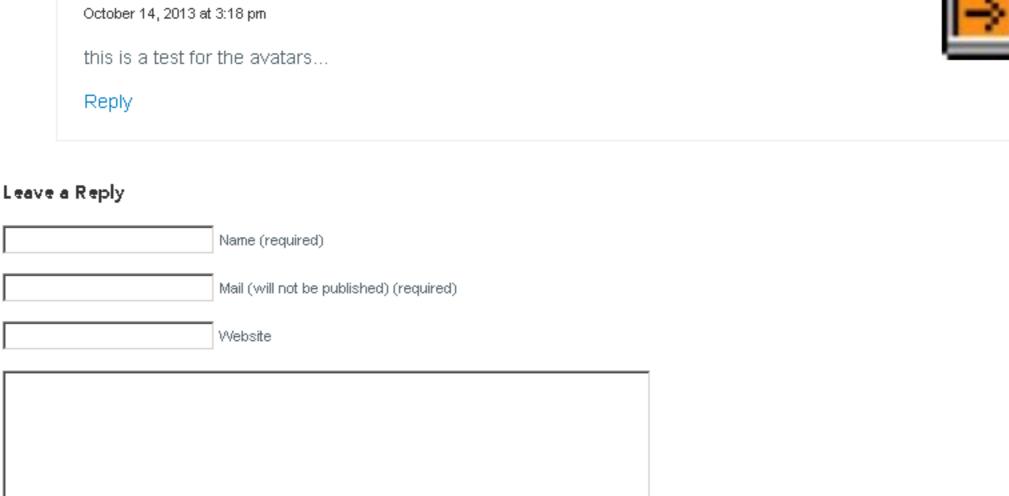
Reply

Very informative article thank you for posting

2 Responses to "Necurs – C&C Domains Non-Censorable"

Doug Heinsdorf says:

September 17, 2013 at 1:28 am



Submit Comment

THREAT PROTECTION

» Automated Malware

» Advanced Targeted

Analysis

Attacks

» Build vs. Buy

norman*shark* N Copyright Norman Shark I Sitemap

PRODUCTS &

» In the News » Press Releases » Events » Press Kit » Blog



NEWS & MEDIA SUPPORT

NORMAN SHARK VIEW WEBINAR **OUR BLOG** "In today's climate of persistent threats,

© @ ②

COMPANY

REQUEST DEMO

Actionable Intelligence for Malware Defense.

SUPPORT

in Share

network defense alone is no longer enough. In order to protect networks from the proliferation of targeted attacks and unknown threats, analysts need dynamic malware

intelligence

capabilities that allow them to respond quickly in the event of an incursion."

Domain and IP's from configuration files megashara.bit 192.249.59.89 192.184.89.74 64.31.48.60

176.56.238.160 178.32.31.41

After decryption from configuration file I got the following URL's and IP's :

Domain and IP's in Necurs config file Necurs decrypts Domain names from its configuration file using following code:

This deci and got "

ER Invalid Domain Name: megashara.bit. Please double check your input.

lookup for this:

configuration file. Lets find out! What are .bit domains? outside of the most commonly used domain name system and is not controlled by ICANN. It is served via Namecoin infrastructure. For registering and configuring .bit domains visit dot-bit website.

project for distributed domain name system was announced in November 2010. And first version of Namecoin was released in April 2011. namecoin It allows us to:

such as ICANN or any other ISP's DNS service. So Development of Dot-P2P

- system. That means DNS servers cannot be updated or seized by authorities. Once a domain is registered only the owner of domain can update the DNS data. That means theoretically Censorship is impossible.
- One simple way to access these domains is to install foxyproxy plugin in Firefox and visit this link to automatically configure.

Those IP addresses belong to DNS servers related to bit Top Level Domain.

Host

atl-dns-dotbit.synapse-axon.net

sea-dns-dotbit.synapse-axon.net

To test your settings you can visit http://bitse.bit/ (bit search engine) from browser. If properly configured you will see this File Edit View History Bookmarks Tools Help @REMnux

Country

US, United States

US, United States

NL, Netherlands

NL, Netherlands

US, United States

How Necurs access .bit domains? Then question arises if .bit domains cannot be accessed by normal means then how Necurs connects to these. Does it change proxy settings or it changes DNS settings of host? No it doesn't. It simply passes DNS server IP to Windows API 'DnsQuery_W' as parameter to resolve domain. Here is how: Before trying to connect it checks if domain name contains .bit in it:

> eax, ds:IP_Array_dword_40E020[edx*4] ; Pick Random IP from Array IN OUT preserved OPTIONAL IN OUT ppQueryResults OPTIONAL IN aipServer_OPTIONAL

Attempts to specify multiple DNS servers result in failure. At the the time of writing "megashara.bit" was not resolving. Conclusion » Necurs uses .bit domains as these are decentralized Cannot be taken down by traditional methods such as taking over or seizing DNS servers. Once domain name is registered cannot be sink-holed, only owner of domain can transfer domain to someone else.

studioactiv8 says:

» Very cost efficient only 0.01 NMC to register and 0 NMC to update domain names.

» Virtually impossible to track as domain owner information to available.

Notify me of new posts by email.

Notify me of follow-up comments by email.

SOLUTIONS » Featured Research » Products » Datasheets » Technology » Case Studies » Solutions » Whitepapers

» Videos

RESOURCES

» Manuals

COMPANY

» Careers

» Company Overview » Management Team