Blog

Necurs – C&C Domains Non-Censorable

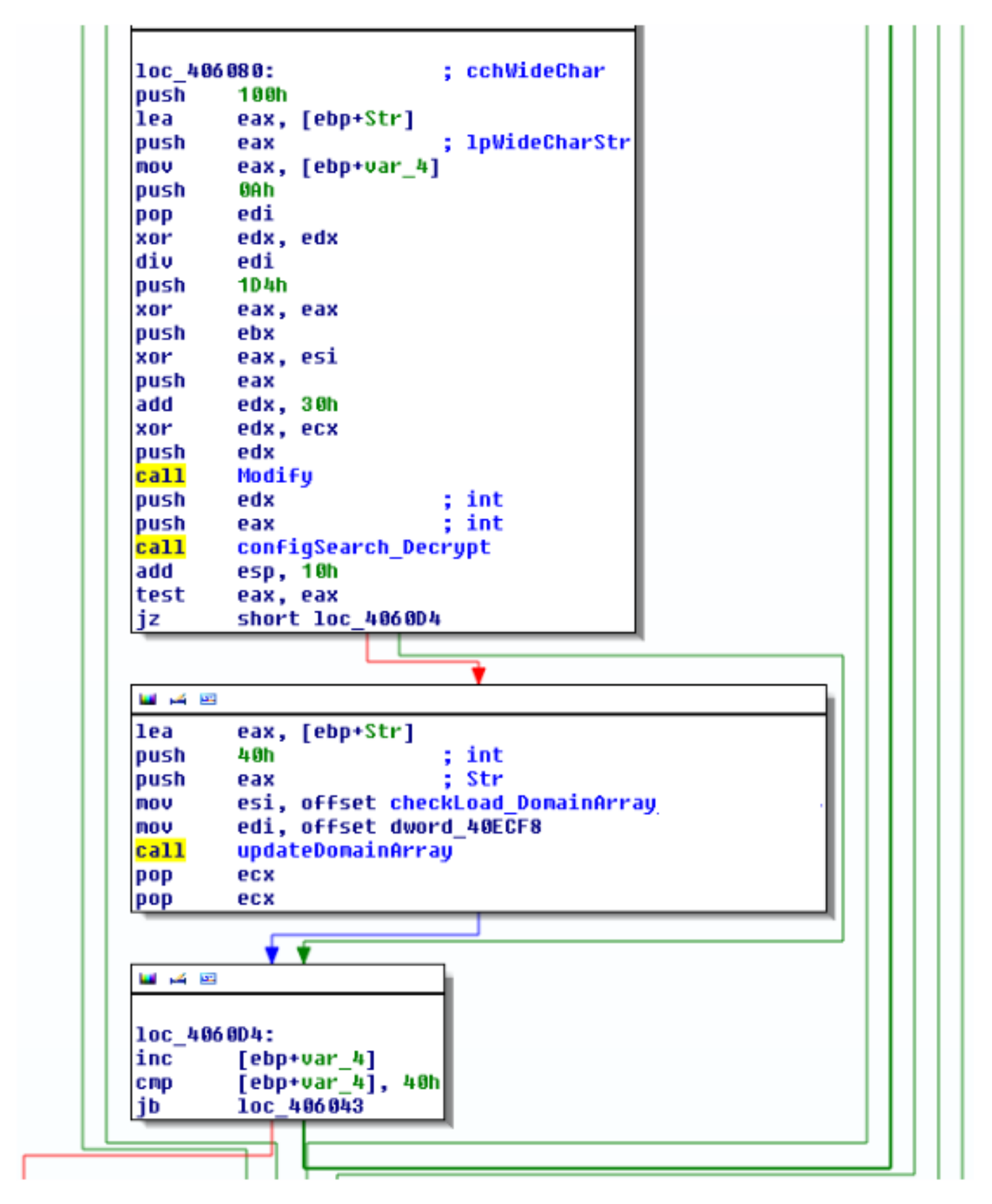
2013.09.10 | By Atinderpal Singh | 2 comments

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

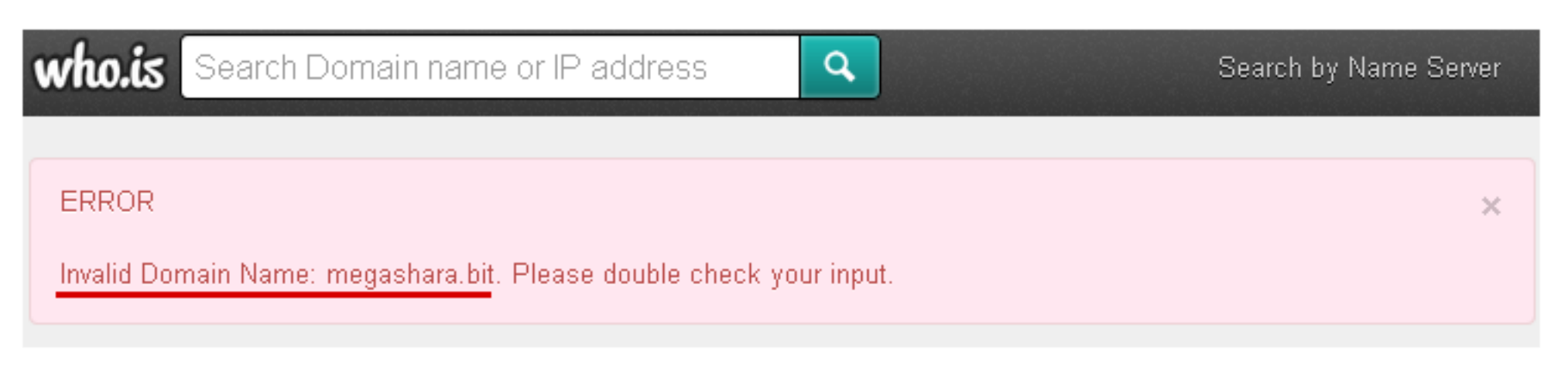
Necurs decrypts Domain names from its configuration file using following code:



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

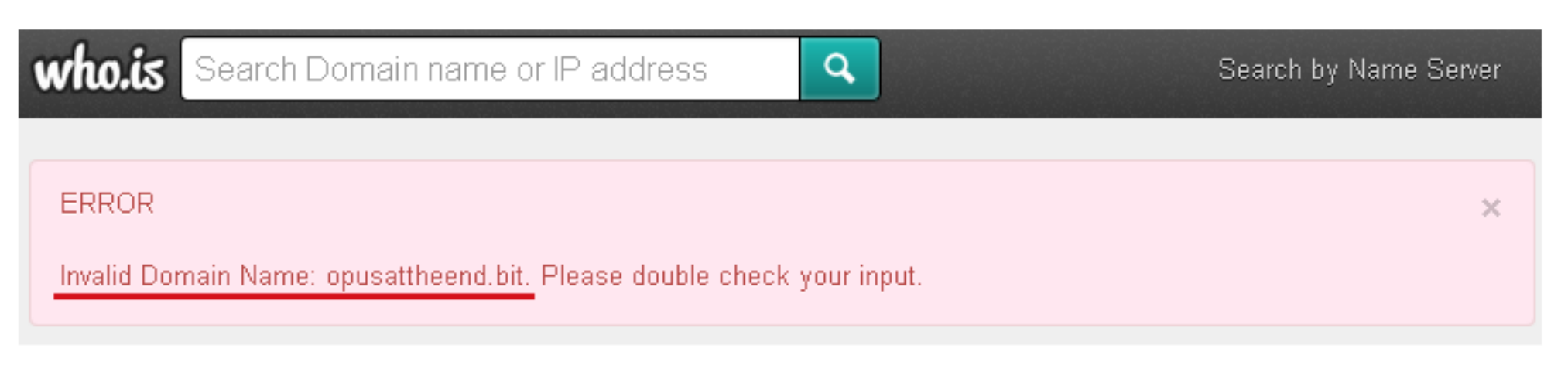
Domain and IP's from configuration files	
megashara.bit	192.249.59.89
192.184.89.74	64.31.48.60
176.56.238.160	178.32.31.41
95.211.195.245	178.63.16.21

This decrypted domain name probably belong to Command and Control server. I tried Whois lookup for this domain name and got "Invalid Domain name" error.



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

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



Again same error "Invalid domain name". That's Strange! If .bit domains does not exist then why it is having in its configuration file. Lets find out!

What are .bit domains?

bit Top Level Domains(TLDs) does exist. but are unknown to majority of the internet users. bit is a TLD that was created 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.

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 such as ICANN or any other ISP's DNS service. So Development of Dot-P2P project for distributed domain name system was announced in November 2010. And first version of Namecoin was released in April 2011.
It allows us to:

» Securely register and transfer arbitrary names, no possible censorship!
» Attach values to the names (up to 1023 bytes)
» Trade and transact namecoins, the digital currency NMC.

What is the use of Decentralized DNS?

Decentralized DNS means TLD's are not owned by any single entity and DNS lookup tables are shared on a peer-to-peer 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.

How to access .bit domains?

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?

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.

One simple way to access these domains is to install foxyproxy plugin in Firefox and visit this link to automatically configure proxy settings for bit domains.

To test your settings you can visit http://bitse.bit/ (bit search engine) from browser. If properly configured you will see this page:

IP addresses from configuration

Now we know what are bit domains and how access those. now one question remains what are those IP addresses in configuration?

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

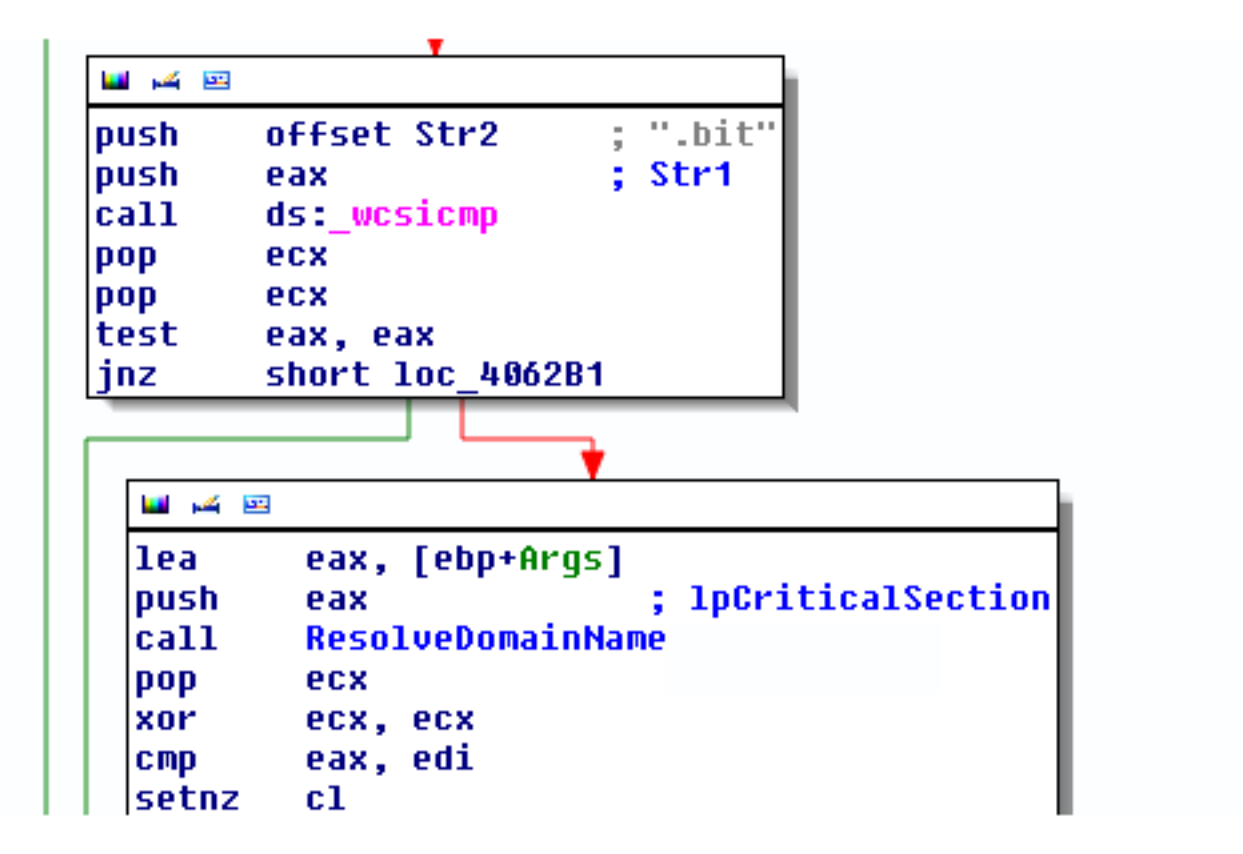
IP	Host	Country	Company	AS no.
192.249.59.89	atl-dns-dotbit.synapse-axon.net	US, United States	RamNode LLC	AS3842
192.184.89.74	sea-dns-dotbit.synapse-axon.net	US, United States	RamNode LLC	AS3842
176.56.238.160	176.56.238.160	NL, Netherlands	RouteLabel V.O.F.	AS198203
95.211.195.245	lw177.ua-hosting.com.ua	NL, Netherlands	LeaseWeb B.V.	AS16265
64.31.48.60	60-48-31-64.static.reverse.lstn.net	US, United States	Limestone Networks, Inc.	AS46475
178.63.16.21	dotbit.me	DE, Germany	Hetzner Online AG	AS24940
178.32.31.41	dns.dot-bit.org	FR, France	OVH Systems	AS16276

How Necurs access .bit domains?

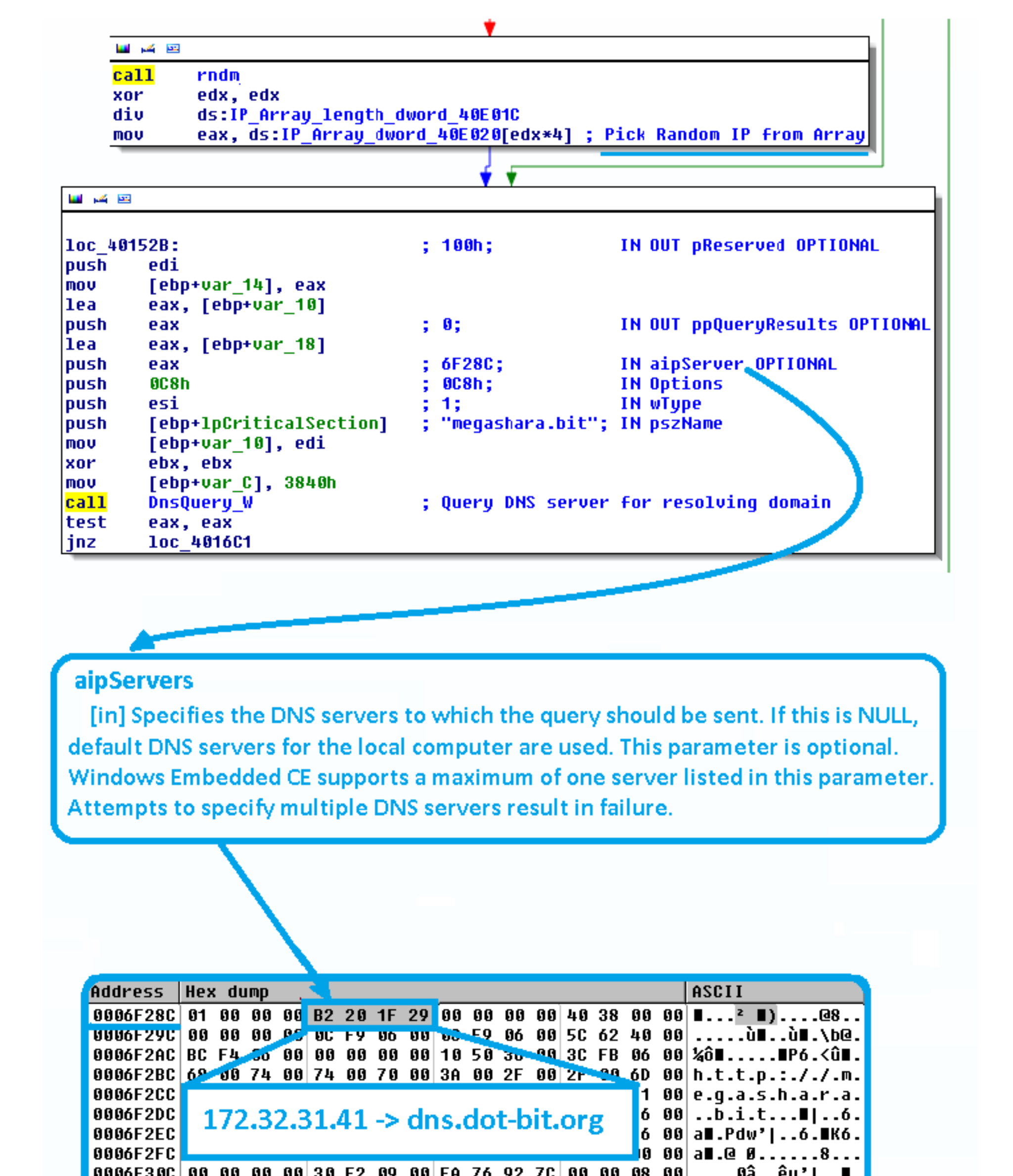
Then question arises if .bit domains cannot be accessed by normal means then how Necurs connects to these. Does it change proxy settings or it changes DNS settings of host? No it doesn't.

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:



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



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.
» Very easy to register and update domain.
» 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.
» Other malwares are likely to adopt similar techniques to resist Command server takedowns by Authorities.

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

Doug Heinsdorf says:
September 17, 2013 at 1:28 am

Very informative article thank you for posting.

Reply

studioactiv8 says:
October 14, 2013 at 3:18 pm

this is a test for the avatars...

Reply

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.