

Forum:[Hack Forums](#)

Thread: [DNS warning \(not the usual warning\)](#)

Alison Wonderland - September 23, 2015, 10:12 pm

So I have seen a few people offering to create DNS or made new DNS services

Just a heads up that this will give them ability to steal your clients if they are so inclined

best way to make it so they cant would be to make your clients have a password for encrypted connection

I know babylon has this feature but I am not sure what other RAT's do.

So just take care in what DNS you use.

I personally would reccomend

[A?mªĐa](#) as a trustworthy DNS source

Ive seen him around alot and he looks the most legit in this regard IMO

and his dns service <https://hackforums.net/showthread.php?tid=4995393>

but in the most part its a good idea to buy a cheap domain name and use that to forward your DNS

Just a heads up as I was recently asked if this were possible to do, so I figure more of you wont know about this

Armada - September 23, 2015, 10:42 pm

(Sep 23, 2015 10:12 PM)Alison Wonderland Wrote: [\[CITE\]](#) So I have seen a few people offering to create DNS or made new DNS services

Just a heads up that this will give them ability to steal your clients if they are so inclined

best way to make it so they cant would be to make your clients have a password for encrypted connection

I know babylon has this feature but I am not sure what other RAT's do.

Absolutely true.

- But I would like to point out how much of a pain in the ass that entire concept would be.

Firstly I would need to jack someones DNS I have given out to (Ok, easy being I control this aspect) Then point it to an IP I connect with.

Open ALL the ports, so I can see which ones are getting hits on.

And then. (Drum roll please) I gotta figure out what everything is (Which port is running which software\protocol), likely by packet sniffing.

Oh, and all this has to be done before the real DNS owner decides to ping their own DNS assignment and figure out the IP# has been changed. ?

(Sep 23, 2015 10:12 PM)Alison Wonderland Wrote: [\[CITE\]](#) I personally would reccomend [A?mªĐa](#) as a trustworthy DNS source

Ive seen him around alot and he looks the most legit in this regard IMO

and his dns service <https://hackforums.net/showthread.php?tid=4995393>

I appreciate the recommendation, on this note, For all the reasons I listed above. For me to do ANY such thing, well yea. Just reading the steps I listed out, seems like too much a pain in the ass for me to bother even considering.

- I can be a VERY lazy person at times... keep your bots, I can get my own lol.

(Sep 23, 2015 10:12 PM)Alison Wonderland Wrote: [\[CITE\]](#) but in the most part its a good idea to buy a cheap domain name and use that to forward your DNS

This is a decent solution for some users, but one of the largest problems with domain registration for these uses is simple. The registrars don't like tolerating this stuff much either. Big surprise, right?

Larger or more serious users will encounter problems with this, by registrar domain seizure. - Then everyone loses their bots, and government or "others" control them. ?

This however is a risk ran REGARDLESS. We have all seen domains that have come and been seized by authorities.

Good advice overall.

Especially with users who are offering DNS services. ?

I personally think it would be a total pain in the ass to do something like you suggested, HOWEVER . This has happened before, it can, and will again... Users are always advised to either do it themselves (or learn to, always the best way) or use someone they trust.

vanphi89 - September 23, 2015, 10:44 pm

can you sell me 5 DNS subdomain? It is enough for me

Cecilia - September 23, 2015, 10:59 pm

(Sep 23, 2015 10:44 PM)vanphi89 Wrote: [\[CITE\]](#) can you sell me 5 DNS subdomain? It is enough for me

Check this out little guy: <https://hackforums.net/showthread.php?tid=4996047>

Easy :)

Alison Wonderland - September 23, 2015, 11:56 pm

well to put it simply

have a all port opened connection

computer/OS/Program that listens on every port and captures every packet received on said ports if the packets aren't encrypted using a special key then they are generic and can be deciphered to which rat they are with relatively easy

It's a fair bit of work but it's not impossible or improbable

vanphi89 - September 24, 2015, 2:06 am

(Sep 23, 2015 10:59 PM)LaPanthere Wrote: [\[CITE\]](#) Check this out little guy:

<https://hackforums.net/showthread.php?tid=4996047>

Easy :)

what is your skype

can you help me via team viewer.

I use Oronze RAT but i will lose slave if IP changed :(

Cecilia - September 24, 2015, 2:37 am

(Sep 24, 2015 02:06 AM)vanphi89 Wrote: [\[CITE\]](#) what is your skype

can you help me via team viewer.

I use Oronze RAT but i will lose slave if IP changed :(

The entire point is for the RAT to use the DNS hostname and you change the IP that hostname resolves to when your ip changes.

Alison Wonderland - September 24, 2015, 2:39 am

(Sep 24, 2015 02:37 AM)LaPanthere Wrote: [\[CITE\]](#) The entire point is for the RAT to use the DNS hostname and you change the IP that hostname resolves to when your ip changes.
you might offer less autistic dns services
but that doesnt mean the users are less autistic

Cecilia - September 24, 2015, 2:42 am

(Sep 24, 2015 02:39 AM)Alison Wonderland Wrote: [\[CITE\]](#) you might offer less autistic dns services
but that doesnt mean the users are less autistic
I cannot agree more with you, HF skids are still skids :)
?

y B Z - September 24, 2015, 11:05 am

(Sep 23, 2015 10:12 PM)Alison Wonderland Wrote: [\[CITE\]](#) So I have seen a few people offering to create DNS or made new DNS services
Just a heads up that this will give them ability to steal your clients if they are so inclined
best way to make it so they cant would be to make your clients have a password for encrypted connection
I know babylon has this feature but I am not sure what other RAT's do.

So just take care in what DNS you use.

I personally would reccomend

[A?mªĐa](#) as a trustworthy DNS source

Ive seen him around alot and he looks the most legit in this regard IMO

and his dns service <https://hackforums.net/showthread.php?tid=4995393>

but in the most part its a good idea to buy a cheap domain name and use that to forward your DNS

Just a heads up as I was recently asked if this were possible to do, so I figure more of you wont know about this

Imao00 thats what im saying like why have someone else be your host when you can make your own

Mr. Robot - September 24, 2015, 11:10 am

Can vouch for A?mªĐa - we see each other around a fair amount.

Also it's much easier to RAT one computer and use it as a host for other clients using a dns anyways :P

y B Z - September 24, 2015, 11:18 am

(Sep 24, 2015 11:10 AM)Mr. Robot Wrote: [\[CITE\]](#) Can vouch for A?mªĐa - we see each other around a fair amount.

Also it's much easier to RAT one computer and use it as a host for other clients using a dns anyways :P

True bot why pay someone for hosting when you can buy your own without the middle man

Armada - September 24, 2015, 11:23 am

(Sep 24, 2015 11:18 AM)y B Z Wrote: [\[CITE\]](#) True bot why pay someone for hosting when you can buy your own without the middle man
Your posts make my eyes bleed.....?

(Sep 23, 2015 10:42 PM)A?mªĐa Wrote: [\[CITE\]](#) This is a decent solution for some users, but one of the largest problems with domain registration for these uses is simple. The registrars don't like tolerating this stuff much either. Big surprise, right?

Larger or more serious users will encounter problems with this, by registrar domain seizure. - Then everyone loses their bots, and government or "others" control them. ?

y B Z - September 24, 2015, 11:28 am

(Sep 24, 2015 11:23 AM)A?mªĐa Wrote: [\[CITE\]](#) Your posts make my eyes bleed.....?

Long story short. Your reselling hosting why would someone buy from you ? Its like me selling a ovh for 25% more when they can buy straight from ovh for cheaper ...

SIM-2502833 - September 24, 2015, 11:32 am

(Sep 23, 2015 10:42 PM)A?mªĐa Wrote: [\[CITE\]](#) Absolutely true.

- But I would like to point out how much of a pain in the ass that entire concept would be.

Firstly I would need to jack someones DNS I have given out to (Ok, easy being I control this aspect) Then point it to an IP I connect with.

Open ALL the ports, so I can see which ones are getting hits on.

And then. (Drum roll please) I gotta figure out what everything is (Which port is running which software\protocol), likely by packet sniffing.

Oh, and all this has to be done before the real DNS owner decides to ping their own DNS assignment and figure out the IP# has been changed. ?

I appreciate the recommendation, on this note, For all the reasons I listed above. For me to do ANY such thing, well yea. Just reading the steps I listed out, seems like too much a pain in the ass for me to bother even considering.

- I can be a VERY lazy person at times... keep your bots, I can get my own lol.

This is a decent solution for some users, but one of the largest problems with domain registration for these uses is simple. The registrars don't like tolerating this stuff much either. Big surprise, right?

Larger or more serious users will encounter problems with this, by registrar domain seizure. - Then everyone loses their bots, and government or "others" control them. ?

This however is a risk ran REGARDLESS. We have all seen domains that have come and been seized by authorities.

Good advice overall.

Especially with users who are offering DNS services. ?

I personally think it would be a total pain in the ass to do something like you suggested, HOWEVER . This has happened before, it can, and will again... Users are always advised to either do it themselves (or learn to, always the best way) or use someone they trust.

I believe LL can't be jacked, because they only connect to managers that have the license they sign up for :)

y B Z - September 24, 2015, 11:39 am

(Sep 24, 2015 11:32 AM)MrMcShroom Wrote: [\[CITE\]](#) I believe LL can't be jacked, because they only connect to managers that have the license they sign up for :)

Yea Nanocore & LL stubs connect to the license only but this can be spoofed

SIM-2502833 - September 24, 2015, 11:40 am

(Sep 24, 2015 11:39 AM)y B Z Wrote: [\[CITE\]](#) Yea Nanocore & LL stubs connect to the license only but this can be spoofed

I feel like no one would ever take the time to do that :)

Although I confess I wasn't aware it could be spoofed without cracking the entire program, and it's possible that the license is checked on KFC's servers, not the LL control panel.

y B Z - September 24, 2015, 12:18 pm

(Sep 24, 2015 11:40 AM)MrMcShroom Wrote: [\[CITE\]](#) I feel like no one would ever take the time to do that :)

Although I confess I wasn't aware it could be spoofed without cracking the entire program, and it's possible that the license is checked on KFC's servers, not the LL control panel.

yea but lets say someone was holding 5k bots. You wouldnt do everything you could to get them?

Armada - September 24, 2015, 2:06 pm

(Sep 24, 2015 11:28 AM)y B Z Wrote: [\[CITE\]](#) Long story short. Your reselling hosting why would someone buy from you ? Its like me selling a ovh for 25% more when they can buy straight from ovh for cheaper ...

You clearly don't understand the service being provided.

Go do what your suggesting, I will wait for the post complaining your domain got jacked up.

Alison Wonderland - September 24, 2015, 5:15 pm

(Sep 24, 2015 11:32 AM)MrMcShroom Wrote: [\[CITE\]](#) I believe LL can't be jacked, because they only connect to managers that have the license they sign up for :)

I wasnt aware the clients and managers were linked like that

that actually sounds like a terrible idea

if that gets seized it will be 100000x worse than the blackshades arrests

SIM-2502833 - September 24, 2015, 5:20 pm

(Sep 24, 2015 05:15 PM)Alison Wonderland Wrote: [\[CITE\]](#) I wasnt aware the clients and managers were linked like that

that actually sounds like a terrible idea

if that gets seized it will be 100000x worse than the blackshades arrests

Only if it gets checked on KFC's servers.

Otherwise, it's probably not a huge deal, there's probably just in the client builder a code that says essentially 'Check the manager, if the ID of the manager is NOT (MD5 hash of your license username) Then do NOT connect'

Making it rough to locate someone, or at least, this would work in theory.

Talk to KFC to see how he did it :)

#Skyline - September 24, 2015, 5:47 pm

Nobody should be trusting a 3rd party DNS provider if anything, users should just create their own DNS. I understand projects have been developed by users here, they are amazing services for the community, don't get me wrong, but still, users are putting there trust into you users here to make sure your services are secure.

Armada - September 24, 2015, 6:11 pm

(Sep 24, 2015 05:20 PM)MrMcShroom Wrote: [\[CITE\]](#) Only if it gets checked on KFC's servers.

Otherwise, it's probably not a huge deal, there's probably just in the client builder a code that says essentially 'Check the manager, if the ID of the manager is NOT (MD5 hash of your license username) Then do NOT connect'

Making it rough to locate someone, or at least, this would work in theory.

Talk to KFC to see how he did it :)

Does not quite work that way with LL.

But close. In fact the binary includes a mutex string which is unique to the controller, as it is generated off of the HWID.

Not only is this used to determine the correct controller, but also is the reason you can't double infect the same machine twice with the same controllers binary.

But yea Allison, I tend to agree, this method has its own draw backs as the mutex is system unique every binary if "finger printed" with the controllers ID so to speak.

SIM-2502833 - September 24, 2015, 6:41 pm

(Sep 24, 2015 06:11 PM)A?mªĐa Wrote: [\[CITE\]](#) Does not quite work that way with LL.

But close. In fact the binary includes a mutex string which is unique to the controller, as it is generated off of the HWID.

Not only is this used to determine the correct controller, but also is the reason you can't double infect the same machine twice with the same controllers binary.

But yea Allison, I tend to agree, this method has its own draw backs as the mutex is system unique every binary if "finger printed" with the controllers ID so to speak.

The question is do stubs use KFC's servers to verify or do they use just that HWID generated string?

Can someone who gains cotnrol of the license servers know what slaves someone has?

That's when I would reconsider using LL in entirety.

Alison Wonderland - September 24, 2015, 7:00 pm

Well im going to have to say LL is not good then with that sort of thing.
fingerprints on a per stub basis sounds like a bad idea

Armada - September 24, 2015, 7:01 pm

(Sep 24, 2015 06:41 PM)MrMcShroom Wrote: [\[CITE\]](#) The question is do stubs use KFC's servers to verify or do they use just that HWID generated string?

Can someone who gains cotnrol of the license servers know what slaves someone has?

That's when I would reconsider using LL in entirety.

I don't believe this is the case. KFC would need to confirm this however.

Even if the licensing server does keep HWID, the mutex string is not the HWID but an encrypted string/algorithm based off of the HWID.

So no, if the licensing server was compromised they would not know the # of binaries each person controls.

That is unless the controllers report these type of statistics to the licensing server, which I find unlikely. It is unnecessary logging at that point.

If Luminosity were to be compromised the authorities would push an update with the backdoor coded or bound to it.

Why change a method that works? Look at how many people got nailed with Shades with this same technique.

SIM-2502833 - September 24, 2015, 7:06 pm

(Sep 24, 2015 07:01 PM)A?mªDa Wrote: [\[CITE\]](#) I don't believe this is the case. KFC would need to confirm this however.

Even if the licensing server does keep HWID, the mutex string is not the HWID but an encrypted string/algorithm based off of the HWID.

So no, if the licensing server was compromised they would not know the # of binaries each person controls.

That is unless the controllers report these type of statistics to the licensing server, which I find unlikely. It is unnecessary logging at that point.

If Luminosity were to be compromised the authorities would push an update with the backdoor coded or bound to it.

Why change a method that works? Look at how many people got nailed with Shades with this same technique.

I agree, but I feel like KFC would try to prevent that from happening. (Really that's just me trying to have any sort of hope in the world)

We should have some sort of code where all update logs will have some sort of word that lets us know it's by KFC, some sort of obscure word he uses in each log, so we can know that "Ok, either the FBI knows we do the code word thing, or this is a legit update." It would make me feel safer, although it probably wouldn't help at all. XD

Armada - September 24, 2015, 7:39 pm

(Sep 24, 2015 07:06 PM)MrMcShroom Wrote: [\[CITE\]](#) I agree, but I feel like KFC would try to prevent that from happening. (Really that's just me trying to have any sort of hope in the world)

We should have some sort of code where all update logs will have some sort of word that lets us know it's by KFC, some sort of obscure word he uses in each log, so we can know that "Ok, either the FBI knows we do the code word thing, or this is a legit update." It would make me feel safer, although it probably wouldn't help at all. XD

Nope, first thing they would do is buy the product legitimately thus getting any sort of code word as well.

Let's be realistic here, the FBI cyber crime division likely has 2-3 agents trolling this site at any given point in time of the day.

SIM-2502833 - September 24, 2015, 7:42 pm

(Sep 24, 2015 07:39 PM)A?mªDa Wrote: [\[CITE\]](#) Nope, first thing they would do is buy the product legitimately thus getting any sort of code word as well.

Let's be realistic here, the FBI cyber crime division likely has 2-3 agents trolling this site at any

given point in time of the day.

Probably, which is kinda funny. I always enjoy seeing antivirus warning people about hackers, then posting screenshot of morons on HF. This reminded me of that. XD

xxleonderpxx - September 24, 2015, 7:43 pm

(Sep 24, 2015 07:39 PM)A?mªDa Wrote: [\[CITE\]](#) Let's be realistic here, the FBI cyber crime division likely has 2-3 agents trolling this site at any given point in time of the day.

That's a scary thought tbh, but probably true.

Armada - September 24, 2015, 7:45 pm

(Sep 24, 2015 07:42 PM)MrMcShroom Wrote: [\[CITE\]](#) Probably, which is kinda funny. I always enjoy seeing antivirus warning people about hackers, then posting screenshot of morons on HF. This reminded me of that. XD

Pretty much, McAfee recently published a "warning" of a new site where users could generate their own Crypto lockers

-including the link to the generator website. Derp ???

SIM-2502833 - September 24, 2015, 7:47 pm

(Sep 24, 2015 07:45 PM)A?mªDa Wrote: [\[CITE\]](#) Pretty much, McAfee recently published a "warning" of a new site where users could generate their own Crypto lockers

-including the link to the generator website. Derp ???

We legitimately need a compilation of these articles all in one thread. 'HF's Impression ion the internet' XDDD

Armada - September 24, 2015, 7:57 pm

(Sep 24, 2015 07:43 PM)xxleonderpxx Wrote: [\[CITE\]](#) That's a scary thought tbh, but probably true.

We are talking about an agency which sets up hacker and other illegal site for the sole purpose of data collection. You think they would not willingly use readily available sites and services as well?

It's not likely true, it certainly is true.

And I am willing to bet most of them are respected or notable members as well.

Alison Wonderland - September 24, 2015, 8:01 pm

I was more thinking along the lines of
if the userbase were compromised
and the controllers and computers could be seized

then the Fingerprint could be pulled off of the computer and then used against them when
more infected machines are found out.

Thats if the user was using it illegally that is.

Armada - September 24, 2015, 8:21 pm

(Sep 24, 2015 08:01 PM)Alison Wonderland Wrote: [\[CITE\]](#) I was more thinking along the lines of
if the userbase were compromised

and the controllers and computers could be seized

then the Fingerprint could be pulled off of the computer and then used against them when
more infected machines are found out.

Thats if the user was using it illegally that is.

This is possible, but that would be end game at that point anyways, if the authorities have your controller, your likely facing the same charges regardless. Only real difference might be between

one count of computer system breach/unauthorized access compared to ten thousand of those charges. Which is unlikely, usually these type of criminal charges are dealt with together, so sentencing would likely be similar anyways.

Alison Wonderland - September 24, 2015, 9:07 pm

(Sep 24, 2015 08:21 PM)A?mªDa Wrote: [\[CITE\]](#) This is possible, but that would be end game at that point anyways, if the authorities have your controller, your likely facing the same charges regardless. Only real difference might be between one count of computer system breach/unauthorized access compared to ten thousand of those charges. Which is unlikely, usually these type of criminal charges are dealt with together, so sentencing would likely be similar anyways.

But even accidental breach of corporate companies can make the charge much much more severe, and it happens