

Forum:[Hack Forums](#)

Thread: [\[MUST READ\] Weird DuckDNS subdomain takeover](#)

QU?CKSILVER - July 20, 2015, 9:06 pm

Today I found out that DuckDNS owners/admins had taken control over a subdomain that I registered on there a year ago.. It had been working ever since and many of my clients are still resolving this subdomain, but guess what? DuckDNS has taken control over my subdomain now for an unknown reason. (I assume it is to check if it's being used for a botnet... Don't know to be honest).

How it all started? Well, basically, my DuckDNS updater had problems updating the subdomain and it was showing the following error:

Okay then... I was wondering why it was happening, so I managed to go to DuckDNS site and surprisingly saw that the registered subdomain was not in the list (deleted)... I tried to add it again, but Oh... BIG SURPRISE. Just look below, lol.

After seeing this crap, I was like "What the heck, how is that even possible? Why would I delete my own subdomain? How come it is now taken by another user?"

Before judging this situation as a TAKEOVER from DuckDNS admins, I managed to resolve the domain above to find out if it was still alive, where it is now pointing to and perform a port scan on it.

Turns out the domain is now pointing to: 192.169.69.25 and it has the port 80 open.

IPWHOIS:

When I saw the port 80 was open, I knew it had to be a webserver running on that IP address and of course, I opened a new tab and went to <http://labrechadera.duckdns.org/> just for curiosity and GUYS, what you're going to see will make you stop using DuckDNS immediately...

Okay, so I guess this is definitely telling me everything I wanted to know... "Modern HoneyPot Network Server"

More info on ThreatStream and their "Modern HoneyNet Framework" project here: Spoiler [\(Click to View\)](#)<https://www.threatstream.com/blog/mhn-modern-honey-network>

DuckDNS is no longer safe for RATs/botnets. BEWARE!! If you still don't trust me, you can just do an HTTP request on the IP mentioned above (which is where my subdomain is currently pointing to) and see it for yourself.

To make a long story short, my subdomain (labrechadera.duckdns.org) was basically taken down by DuckDNS administrators because they want to find out if I was using it for malicious purposes (technically I was) but all I can say is to stop using DuckDNS for Remote Administration

Tools/Botnets, as you could be surprised someday.

?Syria - July 20, 2015, 9:14 pm

I came here for a video! And some one probably just paid them to get ur sub domain and wanted to scare you

eidt:wow they found 10,300,426 infected computers

BahNahNah - July 20, 2015, 9:18 pm

(Jul 20, 2015 09:14 PM)?Syriamanal Wrote: [\[CITE\]](#) I came here for a video! And some one probably just paid them to get ur sub domain and wanted to scare you

eidt:wow they found 10,300,426 infected computers

Its possible that duckdns is cracking down.

OP, how many computers did you have connecting to the DNS?

QU?CKSILVER - July 20, 2015, 9:50 pm

(Jul 20, 2015 09:18 PM)BahNahNah Wrote: [\[CITE\]](#) Its possible that duckdns is cracking down.

OP, how many computers did you have connecting to the DNS?

Well, I must say I have like 10 people resolving that subdomain right now, and they're all from my country (Dominican Republic)

(Jul 20, 2015 09:14 PM)?Syriamanal Wrote: [\[CITE\]](#) I came here for a video! And some one probably just paid them to get ur sub domain and wanted to scare you

eidt:wow they found 10,300,426 infected computers

Why would you need a video? I didn't record anything, just showing proof that DuckDNS is somehow taking over subdomains for investigation.

d4rkito - July 20, 2015, 9:54 pm

Seems curious. This could be an important info for us, thanks!

SiNdicate - July 21, 2015, 12:46 am

Thanks for looking out! You probably saved the asses of a lot of people.

N3wb Gamer - July 22, 2015, 8:44 am

This just happened to me. Does anyone recommend another dns server?

?I??? ??t - July 22, 2015, 8:45 am

my dns got closed too

but when you ping it does to 1.1.1.1(dns is : alienware123.duckdns.org)

QU?CKSILVER - July 22, 2015, 11:08 am

(Jul 22, 2015 08:44 AM)N3wb Gamer Wrote: [\[CITE\]](#) This just happened to me. Does anyone recommend another dns server?

To be honest, I'd recommend to stay away from Free DNS providers, as they might do the same DuckDNS just did in the future.

(Jul 22, 2015 08:45 AM)GSOmega Wrote: [\[CITE\]](#) my dns got closed too

but when you ping it does to 1.1.1.1(dns is : alienware123.duckdns.org)

Your subdomain is pointing to the same IP address of mine:

SIM-2163220 - July 22, 2015, 11:44 am

Just lost over 10k slaves.

Fuck this shit, I lay down this career now.

IAmExploit - July 22, 2015, 2:27 pm

(Jul 22, 2015 11:44 AM)Nea™ Wrote: [\[CITE\]](#) Just lost over 10k slaves.

Fuck this shit, I lay down this career now.

Sorry for your loss, man. :(

Wolf of Wall Street - July 22, 2015, 3:18 pm

(Jul 22, 2015 11:44 AM)Nea™ Wrote: [\[CITE\]](#) Just lost over 10k slaves.

Fuck this shit, I lay down this career now.

omg thats awful ?

duckdns was good for me cause im a newbie and it was easy to use

©Ratatouille™ - July 22, 2015, 4:28 pm

mother fucker lost 1k <http://mediafire.duckdns.org>

Alternative DNS ?

No ip = Ban

DNS exit = Ban

DuckDns = Ban

SiNdicate - July 22, 2015, 10:09 pm

Well, FreeDNS is pretty decent, but it's really the only one i've ever used. No problems with it and I would suggest it.

Armada - July 22, 2015, 11:31 pm

(Jul 22, 2015 11:22 PM)Odinz Wrote: [\[CITE\]](#) Which bot was using this host?

It seems to have more to do with the amount of traffic ging through the domains, not the type of traffic.

I looked in to this earlier.

<https://hackforums.net/showthread.php?tid=4917395>

Armada - July 22, 2015, 11:55 pm

(Jul 22, 2015 11:47 PM)Odinz Wrote: [\[CITE\]](#) I actually think that it's less about the traffic volume (even though the networking logic in 99% of the RATs and Botnets is extremely flawed), but rather about the actual port and the encryption key of the packets (if there is any) that cause the actual suspicions in the first place.

I lost 2 DNS's to this myself, both utilizing SSL tunnels. I debated that myself until I realized even encrypted connections were compromised.

mightyevilcat - July 23, 2015, 1:43 am

Look at their google+ community: plus.google

.com/116877712628428129232/posts/M7K6RT3PAaq

A meany gave them a list of people to ban, OP's dns is in that list. The list is there: comox.hyas

.com/duck/

If you are in that list, sorry for your loss.

Altidore - July 23, 2015, 2:16 am

(Jul 23, 2015 01:43 AM)mightyevilcat Wrote: [\[CITE\]](#) Look at their google+ community: plus.google.com/116877712628428129232/posts/M7K6RT3PAaq

A meany gave them a list of people to ban, OP's dns is in that list. The list is there: comox.hyas.com/duck/

Good find, holy shit now you know what happened, they planned it all in the background, duckdns wasn't (willing to be) ready for the large amount of bad users ?

Indus - July 23, 2015, 6:03 am

i think i should shift to something else

SIM-2212192 - July 27, 2015, 11:30 am

thx 4 the heads up, thread back to the top