Something is leaking my DNS

Goobi · Feb 11, 2016

G

Goobi
Regular Contributor

Feb 11, 2016 #1

Hello All,

I got a 68U running the latest Merlin and it is solid as rock. Well over a year ago, I started using DNSCrypt along with DNS filtering to ensure all clients connected to the network are forced to us the router's DNS which is using DNSCrypt. I occasionally, run tcpdump against port 53 to make sure nothing is leaking. Here is the exact command I run:

tcpdump -i eth0 dst port 53 or src port 53 -n -x -X -v -e

I typically get nothing showing up which is what I expect. However, over the past couple of weeks, I noticed that the above commands show some leakage but I am unsure of the source. Here is a snip from the tcpdump output:

```
11:14:28.601118 00:01:5c:78:46:46 > My ISP MAC, ethertype IPv4 (0x0800), length 88: (t
os 0x0, ttl 52, id 0, offset 0, flags [DF], proto UDP (17), length 74)
    90.154.145.81.53 > My ISP Address.11304: 40344 ServFail 0/0/0 (46)
        0x0000:  4500 004a 0000 4000 3411 7755 5a9a 9151  E..J..@.4.wUZ..Q
        0x0010:  4ac4 989e 0035 2c28 0036 d10c 9d98 8182  J....5,(.6......
        0x0020:  0001 0000 0000 0000 0c75 6c75 6c65 7077  .........ululepw
        0x0030:  6e6d 6e6b 7a03 7777 7707 7839 396d 6f79  nmnkz.www.x99moy
        0x0040:  7503 6e65 7400 0001 0001                 u.net.....
```

The IP address are random from all over but they always hit my ISP

Note the MAC address I captured (00:01:5c:78:46:46). This MAC appears to come from Apple. This MAC never changes in the dump although the IP addresses do. The port of 53 also remains the same. This MAC is not coming from any of my connected devices, so I don't know how to stop it from sending these requests.

Any ideas on how I can go about preventing this MAC from sending DNS requests to my ISP address? Is there a way to possibly block any attempts from this MAC to my ISP address? Thanks in advance for some guidance.

E

eddiez
Senior Member

Feb 11, 2016 #2

The MAC belongs to Cadant Inc., which is owned by Arris. Arris manufactures modems. So it could be the box the ISP gave you.

http://www.dslreports.com/forum/r25953464-TWC-Cadant-CMTS-wtf-Hudson-Valley-NY

RT-AC68U 384.12_0

C

ColinTaylor
Part of the Furniture

Feb 11, 2016 #3

Have you seen this: http://serverfault.com/questions/74...es-this-packet-come-in-dns-response-127-0-0-1

Looks like it might be our Chinese friends again (x99moyu.net).

UPDATE: Actually that example is a Bulgarian IP!

RT-AX86U Asuswrt-Merlin

martinr

G

Feb 11, 2016 #4

> **eddiez said:**
>
> The MAC belongs to Cadant Inc., which is owned by Arris. Arris manufactures

> Valley-NY

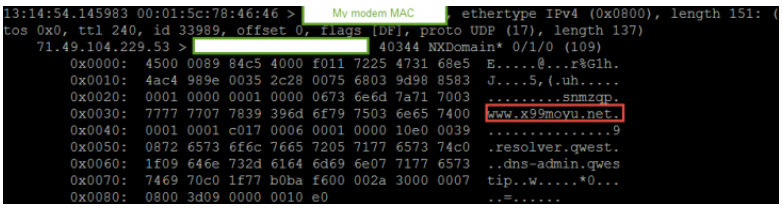
Thanks, I misspoke as the MAC address is associated with Cadant. I have a Arris Motorola modem. However, when I look at the MAC for the modem, it is not the captured MAC in the tcpdump snippet I posted.

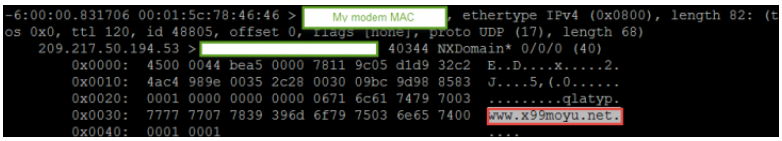
Goobi
Regular Contributor

Feb 11, 2016 #5

> **ColinTaylor said:**
>
> Have you seen this: http://serverfault.com/questions/74...es-this-packet-come-in-dns-response-127-0-0-1
>
> Looks like it might be our Chinese friends again (x99moyu.net).
>
> UPDATE: Actually that example is a Bulgarian IP!

Colin, I think you may be on to something. Here are a couple of more snips that show the dreaded www.x99moyu.net:

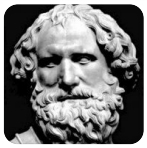




I got about 28 instances of this the last 6 or so hours, so it's not slowing me down or anything, but it is still concerning. The tcpdump also shows my modem MAC as the destination, so it appears they are hitting my modem directly and it appears to end there. No probing of the attached router.

I looked at the link you provided where the situation is explained very well, but I did not note a solution. Is my only option to ask my ISP to generate a new address because the existing one appears to be compromised?

Thanks in advance.



joegreat
Very Senior Member

Feb 11, 2016 #6

> **Goobi said:**
>
> I got a 68U running the latest Merlin and it is solid as rock. Well over a year ago, I started using DNSCrypt along with DNS filtering to ensure all clients connected to

Just an idea: Could it be that some of your clients are not using the router als DNS server (automatic configuraiton), but have set an explicit DNS server on their own (manual setup)?

Is a typical trick for malware/ramsonware to re-direct the traffic to a compromised DNS server...

PS.: Looking into my dnscrypt setup I have also somebody bypassing my setup! It's the Chromcast devices who is using Google's DNS servers (and cannot be changed?).

Last edited: Feb 12, 2016

Main Router: Asus RT-AX88U with Entware 64-bit, OpenVPN, Samba and some Scripts - using 2 USB devices \/
Access Point: Asus RT-AC87U to extend WLAN coverage in a challenging building /\ Using **Merlin's firmware v388.1 and Asus v382_52545 /\ Internet Speed Test: 529 down / 54 up Mbps**

sfx2000

C

ColinTaylor
Part of the Furniture

Feb 12, 2016 #7

> **Goobi said:**
>
> I looked at the link you provided where the situation is explained very well, but I did not note a solution. Is my only option to ask my ISP to generate a new address because the existing one appears to be compromised?

If, as seems likely, you are seeing option #4 in that article, then personally I would just ignore it.

It's nothing to do with you or your network, they've just got some bots in another part of the world that happen to be using your IP as a spoofed return address. As you're not seeing a continuous stream of traffic coming in I would speculate that the bots are just cycling through all the IP's in a given group of networks. It's likely that all the IP's on your ISP's subnet are experiencing the same thing, so changing your IP might not make any difference.

Keep monitoring it for a couple of weeks, you might find that it stops as the bots move onto another group of IP's.

RT-AX86U Asuswrt-Merlin

J

Feb 12, 2016 #8

Google devices will not let you change DNS, nor will Roku devices, Not sure about Amazon but iv seen both Chromecast and Roku boxes ignore DNS settings from a router... Roku will not even let you set a fixed IP

sfx2000
Part of the Furniture

Feb 12, 2016 #9

> **joegreat said:**
>
> Is a typical trick for malware/ramsonware to re-direct the traffic to a compromised DNS server...

This is a strong consideration - time to check PC's to see if someone got a drive-by attack...

--
"How many lights?"

sfx2000
Part of the Furniture

Feb 12, 2016 #10

Also - some apps have DNS hard-coded in the app itself - if I recall, Netflix on Android had this issue for a while (not sure if this is resolved for not) - not a stretch to see if other apps are doing this same dodgy behavior...

--
"How many lights?"

joegreat and Nullity

Nullity
Very Senior Member

Feb 12, 2016 #11

> **sfx2000 said:**
>
> Also - some apps have DNS hard-coded in the app itself - if I recall, Netflix on Android had this issue for a while (not sure if this is resolved for not) - not a stretch to see if other apps are doing this same dodgy behavior...

My Roku & my Samsung Smart-TV (I think) both have hardwired DNS.

I force all DNS queries to my router's dnsmasq instance with NAT port-forwards. I guess this would fail with dnscrypt?

Please correct any obvious misinformation in my posts.
-Not a professional.
Router: pfSense **AP:** Asus RT-N66U (john9527)

ASAT
Senior Member

Feb 13, 2016 #12

> **Goobi said:**
>
> over the past couple of weeks, I noticed that the above commands show some leakage but I am unsure of the source.

How to make a tripwire on the WAN-side of the router. Automatically ban remote hosts that attempt to access invalid services.

Code:

```
/usr/sbin/ipset -N bannedhosts iphash
/usr/sbin/iptables -I INPUT -i eth0 -p tcp -m multiport --ports
/usr/sbin/iptables -I INPUT -i eth0 -p udp -m multiport --ports
/usr/sbin/iptables -I INPUT -m set --match-set bannedhosts src -
/usr/sbin/iptables -I INPUT -m set --match-set bannedhosts dst -
/usr/sbin/iptables -I OUTPUT -m set --match-set bannedhosts src
/usr/sbin/iptables -I OUTPUT -m set --match-set bannedhosts dst
/usr/sbin/iptables -I FORWARD -m set --match-set bannedhosts src
/usr/sbin/iptables -I FORWARD -m set --match-set bannedhosts dst
```

SOURCE: http://www.linuxjournal.com/content/advanced-firewall-configurations-ipset?page=0,2

CiscoX

Goobi
Regular Contributor

Feb 13, 2016 #13

Thanks for all the feedback everyone. I am going to monitor over the next couple of weeks and see if "they" move on to a different pool of IP addresses. As it stands, I see 1-2 requests per hour. If the issue remains, I will give ASAT's suggestion a whirl since it appears as a more proactive approach to try and mitigate this activity. Thanks again everyone!

Nullity
Very Senior Member

Feb 13, 2016 #14

So, you are unsure which client on your network is querying the DNS server for that particular domain? (x99moyu.com)

Does the source IP correspond to your configured DNS servers? If not, it's just standard unsolicited internet scanning crap that I would disregard. Just because you get a response does not mean you issued a request.

The source MAC is always going to be the first hop, since ethernet is point to point. Regarding what company the MAC's OUI corresponds to, my upstream DSLAM has the OUI of a medical or prosthetics device... so I would not pay too much attention to the OUI.

Please correct any obvious misinformation in my posts.
-Not a professional.
Router: pfSense **AP:** Asus RT-N66U (john9527)

ColinTaylor
Part of the Furniture

Feb 14, 2016 #15

Nullity said:

So, you are unsure which client on your network is querying the DNS server for that particular domain? (x99moyu.com)

No that's not what we are saying. Look again at the dumps and then read

to the way scammers use a fake return email address.

RT-AX86U Asuswrt-Merlin

Nullity
Very Senior Member

Feb 14, 2016 #16

> **ColinTaylor said:**
>
> No that's not what we are saying. Look again at the dumps and then read the information I linked to in post #3. It's nothing to do with him or his equipment. He is not querying the DNS server, it's a bot somewhere that is using his (and many others) IP as a return address to hide itself. It's similar to the way scammers use a fake return email address.

There is no DNS leak then? If there is nothing unexpected leaving/leaking from his network, there is no concern, I would assume.

I thought the OP suspected a LAN client was making DNS queries that it should not be making, causing unexpected DNS respones.

Someone could be spoofing his IP like in a DNS Amplification attack.

Ultimately, I just don't see a reason to be concerned, but I could very likely be misinterpreting what's been posted...

Please correct any obvious misinformation in my posts.
-Not a professional.
Router: pfSense **AP:** Asus RT-N66U (john9527)

Nullity
Very Senior Member

Feb 14, 2016 #17

Super... my post is flagged as spam and awaiting mod approval.

Please correct any obvious misinformation in my posts.
-Not a professional.
Router: pfSense **AP:** Asus RT-N66U (john9527)

sfx2000
Part of the Furniture

Feb 14, 2016 #18

> **Nullity said:**
>
> Super... my post is flagged as spam and awaiting mod approval.

Happens...

--

C

ColinTaylor
Part of the Furniture

Feb 14, 2016 #19

> **Nullity said:**
>
> I thought the OP suspected a LAN client was making DNS queries that it should not be making, causing unexpected DNS respones.

That was his initial concern but upon further investigation of the dumps that now seems unlikely.

> Someone could be spoofing his IP like in a DNS Amplification attack.

That's exactly it. Or at least, that's our current theory.

RT-AX86U Asuswrt-Merlin

Nullity

G

Goobi
Regular Contributor

Feb 17, 2016 #20

Hi Guys,

I am here to report back. This has become very interesting and I thank you for your suggestions and feedback. While I originally thought that something from within my network was leaking DNS, a careful look at tcpdump data shows that was not the case. You can see a remote source IP using port 53 and terminating at my cable modem.

I think the working theory of this being a DNS amplification attack is right on. The victim of the attack does appear to be a company called CloudFlare. In particular, it's DNS servers.

If I take a look at one of the dumps, we can see requests for x99moyu.net. If I run dig against this domain name, I get the following:

dig +short x99moyu.net NS

darwin.ns.cloudflare.com

Since neither I or this remote IP (from dump) are owned by Cloudflare, we can reasonably assume that one of these IPs is spoofed. Given the victim of the attack (Cloudflare) and how the attack operates, the address most likely being spoofed here is mine!

I did not like the idea of my IP participating in any attack so after a couple of days of watching these requests trickle in, I decide to try ASAT's suggestion about setting up a tripwire on the WAN side of the router. I modified to log any drops so what I ended up with is:

ipset -N bannedhosts iphash
iptables -I INPUT -i eth0 -p tcp -m multiport --ports 53 -j SET --add-set bannedhosts src
iptables -I INPUT -i eth0 -p udp -m multiport --ports 53 -j SET --add-set bannedhosts src
iptables -I INPUT -m set --match-set bannedhosts src -j logdrop
iptables -I INPUT -m set --match-set bannedhosts dst -j logdrop
iptables -I OUTPUT -m set --match-set bannedhosts src -j logdrop
iptables -I OUTPUT -m set --match-set bannedhosts dst -j logdrop
iptables -I FORWARD -m set --match-set bannedhosts src -j logdrop
iptables -I FORWARD -m set --match-set bannedhosts dst -j logdrop

The bannedhosts ipset shows the following bad actors captured:

210.5.183.234 -->Hong Kong
213.219.84.227 -->Estonia
63.134.200.200 --> Arizona (US)
80.69.147.202 --> Russia
61.35.16.29 --> South Korea
66.86.78.244 --> North Carolina (US)
195.189.29.130 --> Kazakhstan
218.90.188.222 --> China
88.147.150.52 --> Russia
117.141.117.145 --> China
201.40.135.70 --> Brazil

It appears that this x99moyu.net is coming from several sources and not just China but I think they are all related and probably have the same source.

This ipset/iptables combination seems to have resolved the issue from the standpoint that these packets are being dropped as soon as they hit my cable modem.

was wondering if I/we should be taking a more proactive approach to the WAN side of the router in terms of letting your cable modem (or whatever) be susceptible to this kind of activity. Do you think that it would be worth adding more commonly exploited ports to the above iptables so that remote sources trying to access invalid services on my modem are dropped? For example, I don't run a SMTP server, so maybe doing this to port 25 would make sense. The only port I use for remote access is port 1194 for OpenVPN. Would it make sense to try and block all other ports or will that potentially cause more problems than what it is worth?

Thanks in advance for your feedback.

ColinTaylor, joegreat and CiscoX

1 2 Next ▸

You must log in or register to reply here.

Similar threads

Thread starter	Title	Forum	Replies	Date
U	ZenWiFi XT8 (RT-AX95Q) and stable: 388.1_0-gnuton1 - Network Map - Ethernet table lost it's css style/table or something	Asuswrt-Merlin	5	Jan 20, 2023
C	Is there something that I can use to do this with VPN?	Asuswrt-Merlin	15	Oct 10, 2022
E	Is this something to worry about?	Asuswrt-Merlin	3	May 6, 2022
	Something that is not dnsmasq advertising	Asuswrt-	12	Mar 6, 2022

Share:

Latest threads

W Meaning of the word BACKHAUL (re: mesh routers)
Started by wsalopek · Today at 3:30 PM · Replies: 3
ASUS AC Routers & Adapters

A ASUS N66U and OpenVPN woes.
Started by absolute · Today at 2:33 PM · Replies: 3
ASUSWRT - Official

D Reserved IP Addressing when mobile device has Randomised MAC (Android) or Private Wi-Fi Address (iOS)
Started by DrMopp · Today at 12:34 PM · Replies: 2
General Wireless Discussion

openvpn server on RT-AC68U not working

Voxel Custom firmware build for Orbi LBR20 v. 9.2.5.2.37SF-HW
Started by Voxel · Today at 9:04 AM · Replies: 5
NETGEAR AC Wireless

Sign Up For SNBForums Daily Digest

Get an update of what's new every day delivered to your mailbox. Sign up here!

Members online

SomeWhereOverTheRainBow, Sanna1967, ThomsBe, goldcart, Ripshod, whatsup, wsalopek, tabormeister, head, karateca, Markymarc, bartj12, shabbs, paul0363, scottyrick, jdabbs, J23, absolute, DME, Henkan

Total: 472 (members: 26, guests: 446)