PassiveDNS

An assessment of Non-Authorized Domain Name Resolution provided by DNS Resolution Service Provider

Zhang Zaifeng, **litao3rd**

Dec 8, 2021 • 8 min read

Summary

In a previous article, we disclosed that the Specter botnet uses api. github[.]com and other white domains to provide C2 services as a way to evade detection by security products based on signature and threat intelligence matching. The botnet can do this because the Domain Name Resolution provider have no check for customer to claim any DNS names.

We were wondering what the overall situation is, so we measured and evaluated this phenomenon, i.e., whether domain name registrars/hosts, public cloud providers, and other providers that provide domain name registration and resolution services (collectively referred to as resolution service providers) are able to return correct responses to DNS requests for domains not served by them.

This article provides an analysis of this phenomenon.

Data Selection and Evaluation Methodology

Domains Under Test

Tested domains: Alexa top500. they were chosen because

1. These domains use their own DNS servers, and they do not use resolution services provided by external resolution providers. So if these domains can be resolved by NS servers of external resolution service providers, they are most likely to be unauthorized.
2. It is common practice that these domains are on various security whitelists because of their well-known operations. In fact, the use of DNS traffic to rank domain names more accurately reflect the popularity of domain names. 360netlab's DNSMon system can calculate the popularity of domain names in the large network

The NS servers

The test NS server: that is, the resolution provider. Extracted from 360netlab's passiveDNS library, **18,469** NS servers that were active in the last six months and provided resolution services for more than 500 independent second-level domain names.

Test Method

The domain name under test will be tried to resolve through the test NS server one by one (UDP/53), if the DNS return result of the test server is NOERROR (regardless of whether there is a real RDATA return), the server under test is considered to provide resolution of the domain name under test.

Evaluation Results

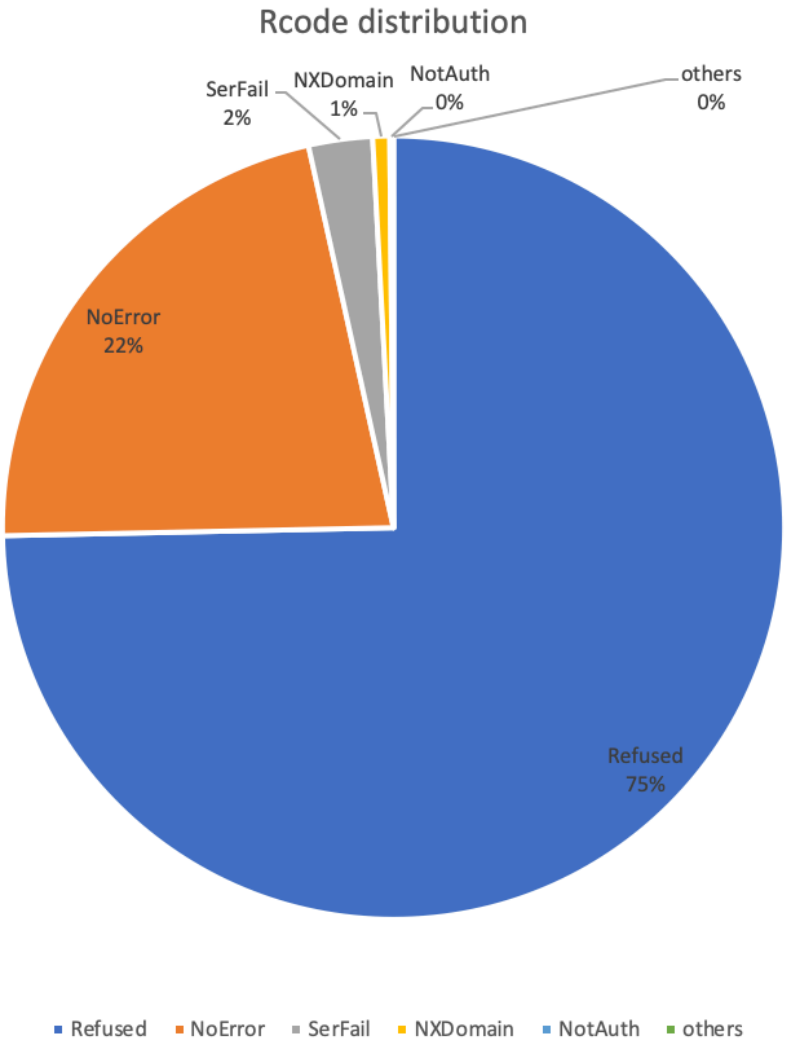
Overall resolution situation

At the time of test, of the 18,469 NS servers, 18,154 were able to resolve to an address, accounting for 98.29% of the total. There are 17,792 servers that can resolve to the address and have a response, accounting for 96.33% of the total. Even though we screened the NS servers with resolution records in the past six months, 3.67% of the servers were inactive at the time of the test, so we can see

that the infrastructure of NS service providers is in constant change.
The following article uses the data of 17,792 NSs as the basis for analysis.

In terms of the number of resolutions, the response rate of 17,792 NS servers is 70.12% ~(6237860/(17,792*500)), which means that 30% of requests are lost when the servers are active, generally due to server timeouts.

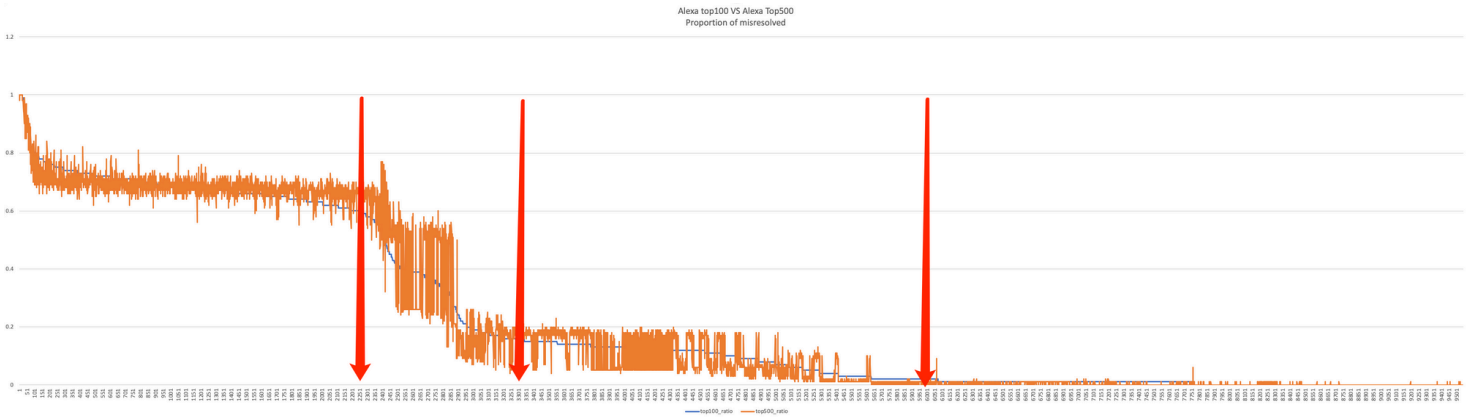
Among all responses, the percentage of Rcode for Refuse is 75, and the percentage of NOERROR is about 22%. The specific distribution of the following chart



In terms of NS servers, 17,792 NS servers, the return of NOERROR record of NS servers are 9544, accounting for about 53.64%.

In terms of NS server secondary domain, 17792 NS corresponds to 4149 secondary domains, of which there are 1687 secondary domains that return NOERROR records, accounting for about 40.66% of the total. That is to say, *in our selected test servers about 40% of NS servers will return a domain name resolution that is not their own customers*.

Based on experience, if such resolution records are added by individual users, it is guessed that the higher ranked domains are more likely to be added and resolved. So we counted the percentage of resolution of Alexa Top100 and the percentage of resolution of all tested domains (i.e. Alexa Top500) for each tested server that returned NOERROR. We sorted the resolution success rate of Alexa Top100 domains by resolution server. The statistical curves are shown below.



From the graph, it is obvious that these 9544 servers can be divided into 4 groups, namely

- NS servers ranked from 1 to 2250 have a resolution rate of more than 60% for top100 and top500 domain names
- NS servers ranking 2250-3300 have a rapid decline from 60% to less than 20% of the domain names under test
- NS servers ranked 3300-6000 are slowly decreasing from 20% to about 2%.
- NS servers ranked after 6000 occasionally have a small amount of resolution, the proportion of basic in about 1%.

In addition, it can be seen from the graph that there is no significant difference in the proportion of tested domains in Alexa Top100 and Top500. This may be due to the fact that there is little difference in the perception of users between the top 100 and 500 domains in Alexa.

Analysis of resolution results

Another perspective on this data is the resolution results. Where exactly do these NS servers resolve these popular domains to.
In the returned results, about 20.92% of the data on the second-level domain is not configured with a valid DNS record with a NOERROR returns, such cases are mostly for the detection of the domain name is configured with the corresponding NS server, but not configured for other types of records.

The domains with IPs

In the return results which have DNS A records, the geographic location of the resolved IPs is mainly concentrated in the United States, followed by China and Russia, and the Top 10 distribution is as follows:

```
 4378 United_States
  579 China
  395 Russian_Federation
  350 United_Kingdom
  216 CLOUDFLARE.COM
  213 Netherlands
  212 Germany
  209 Japan
  195 Republic_of_Korea
  123 Singapore
```

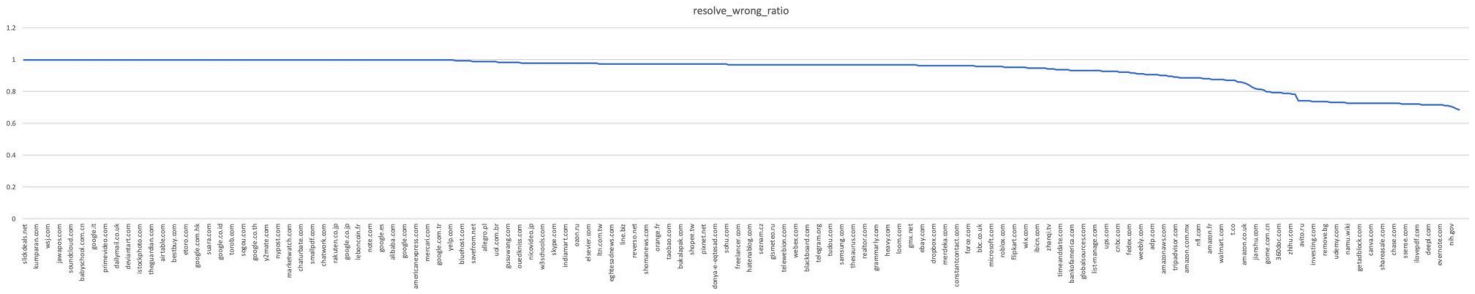
It is worth mentioning that about 3% of the many returned A records are reserved or private addresses, and the most popular of these addresses is 127.0.0.1. The top 10 addresses are as follows:

```
33093 127.0.0.1
  856 10.10.34.35
  425 192.168.3.3
  154 10.10.10.10
   69 10.10.34.36
   52 10.152.68.117
   45 10.10.34.34
   42 192.168.1.1
   27 127.0.0.11
   22 0.0.0.0
```

Error rate of resolution results

We compared the results from non-authorized resolution service providers with the correct resolution results and found that 80% of the domain names (i.e. 400) had an error rate of 90% or more, and the best case domain name error rate was as high as 68%, which is a quite high.

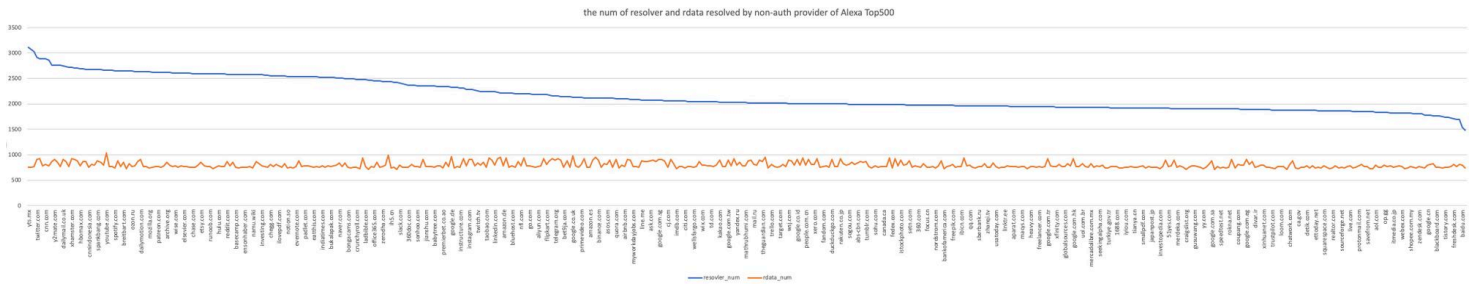
Different domain name resolution error rate curves are as follows.



Domain name perspective

How many NSs do the top500 domains resolve on? What is the distribution of the percentage

Among the 500 domains, the least resolved domain name is express.dhl, with 1483 NS servers resolving it, and the most resolved is yts.mx, with 3114 NS servers resolving it. However, from the results of their resolution, the number of rdata resolved by different domains is relatively stable, mostly around 800. **It can be seen that it is very common but very surprising for popular domains to be added to various non-authorized resolvers**. The specific distribution is as follows.



Case Study

Why so many popular domain names are added to be resolved by non-authorized NS servers? Let's take yts.mx and mozilla.org as examples to see what is going on here.

yts.mx

yts.mx was chosen for analysis because it is the domain name that resolved by most NS servers in our test.

yts.mx is a P2P movie downloads site, and is ranked No. 462 in the Alexa data we used. We can see there are 2886 non-authorized resolving servers that can resolve yts.mx, and only 73 of the NS servers are giving us correct results, the incorrect resolution rate of 97.47%, and within them, the top NS servers are:

```
2020-02-02 01:34:09     2021-12-05 18:55:33     2552    yts.mx  NS      erin.ns.cloudflare.com
2020-02-02 01:34:09     2021-12-05 18:55:33     2552    yts.mx  NS      eric.ns.cloudflare.com
```

Most of this list are IT infrastructure service providers offering domain name registration, web service hosting, hosting services, etc. Not surprisingly cloudns mentioned in our last article is listed.

Looking at the IPs that resolved incorrectly, they point to a total of 750 IP addresses, aggregating to 149 network segments. The top10 of these segments and the usage of these segments are analyzed as follows.

CIDR/24	resolver_num	resolver_owner	function
217.70.184	520	gandi.net	parking/redirecting
209.99.64	451	register.com worldnic.com ztomy.com	parking/redirecting
50.87.144	244	hostgator.com	default page
192.185.4	215	hostgator.com	default page
198.57.247	168	hostgator.com	default page
208.91.197	163	active-dns.com aloojamiento.com bigrock.com bigrock.in bluehost.com ctctdns.com ctctdns.net dns.mn domainesia.com domainmonger.com gatordns.com gatordns.net gatordns.org genious.net guzelhosting.com heberjahiz.com hostgator.in indiacyberspace.com kheweul.net launchpad.com mitsu.in monovm.com mysafedns.com orderbox-dns.com	parking/redirecting
108.167.189	113	hostgator.com	default page

127.0.0	65		loopback
3.64.163	54	dan.com dan.hosting undeveloped.com	parking/reselling
192.254.250	42	hostgator.com	default page

mozilla.org

mozilla.org was chosen because mozilla.org is the official website of the Firefox browser and is well known to the public and it is ranked 182 by Alexa. We dug in our passiveDNS.cn and could see mozilla.org has been using akamai as their resolver since 2014.

```
2014-08-19 18:46:40     2021-12-03 09:10:03     5590898 mozilla.org     NS      ns5-65.akam.net
2014-08-19 18:46:40     2021-12-03 09:10:03     5590905 mozilla.org     NS      ns4-64.akam.net
2014-08-19 18:46:40     2021-12-03 09:10:03     5590905 mozilla.org     NS      ns7-66.akam.net
2014-08-19 18:46:40     2021-12-03 09:10:03     5590920 mozilla.org     NS      ns1-240.akam.net
```

Its resolution results have changed a little bit over time, after November 2020, it has been using amazon's service.

```
2020-11-04 01:43:42     2021-12-03 10:43:49     160143606       mozilla.org     A       44.235.246.155
2020-11-04 01:43:42     2021-12-03 10:43:49     160140246       mozilla.org     A       44.236.72.93
2020-11-04 01:43:42     2021-12-03 10:43:49     160143623       mozilla.org     A       44.236.48.31
2018-05-15 23:15:34     2021-01-30 15:08:29     976954654       mozilla.org     A       63.245.208.195
2014-08-05 21:39:30     2018-05-17 16:02:33     9988032 mozilla.org     A       63.245.215.20
```

However, in our test data, there are 2,624 NS servers capable of resolving mozilla.org, with 735 resolved IP addresses.

The top 10 resolvers are as follows.

```
846 hostgator.com
520 gandi.net
369 register.com
 83 orderbox-dns.com
 70 worldnic.com
 51 dan.hosting
 47 hostgator.mx
 33 ztomy.com
 30 cloudns.net
 16 zoneedit.com
```

This entry on this list is very similar to the yts.mx example.

Except akam.net and cloudflare.com, only 62 NS servers can correctly return the A records. In other words, **70% of the non-authorized NS servers are returning the wrong IPs**.

In terms of incorrectly resolved IPs, 730 incorrect IPs (5 IPs were correctly resolved) were aggregated to 153 CIDR/24 segments, with top10 segments accounting for 75.9% of the total incorrectly resolved volume. We analyzed in detail the CIDR/24 segments of the Top10 incorrectly resolved, and found that they are mainly registered by domain name registrars/resolvers, and the final resolution destination IPs are used for domain name parking, redirection and domain name sale purposes. The specific results are shown in the following chart:

CIDR/24	resolver_num	resolver_owner	function
209.99.64	366	register.com	parking/redirecting
50.87.144	235	hostgator.com	default page
192.185.4	201	hostgator.com	default page
198.57.247	181	hostgator.com	default page
		active-dns.com aloojamiento.com bigrock.com bigrock.in bluehost.com ctctdns.com ctctdns.net dns.mn domainesia.com domainmonger.com gatordns.org genious.net guzelhosting.com heberjahiz.com hostgator.in indiacyberspace.com kheweul.net launchpad.com mitsu.in monovm.com mysafedns.com orderbox-dns.com regway.com resellerclub.com sibername.com	
208.91.197	152	spiritdomains.com	parking/redirecting
108.167.189	116	hostgator.com	default page
		alphadnszone.com anycast.vn cloudns.net compra.eu compra.nl compra.uk creatium.io dandydns.com dcsix.net dnslink.com freshcloud.pro mijnhostingpartner.nl netsample.com perfectdns.com register.to s-dns.de v-dns.de	
127.0.0	69	weblium.com	None

3.64.163	48	ns3.dan.hosting	parking/reselling
192.254.250	43	hostgator.com	default page

accountsupport.com
apollohosting.com
bizland.com
bluedomino.com
domain.com
dot5hosting.com
dotster.com
easycgi.com
ehost.com
fatcow.com
globat.com
hostcentric.com
ipage.com
ipower.com
mydomain.com
nameresolve.com
netfirms.com
powweb.com
purehost.com
readyhosting.com
startlogic.com
verio.com

We can see from the above two cases that these non-authorized resolution service is mainly from domain name registration/resolution provider registration, and the parking, redirection and domain name sales.

Security challenge

When a malicious actor can register arbitrary, especially well known DNS domains, it brings real problems, as we disclosed in our previous blog, there are botnets out there using this “feature” to make their C2 look totally legit.

From defense perspective, The DNS based security detection needs to be expanded to look at both the domain name and the DNS servers used by the domain name, as well as whether the resolution results are consistent with the real results.

俄乌危机中的数字证书：吊销、影响、缓解

商业数字证书签发和使用情况简介(删减版)

解析服务提供商对非授权域名解析情况的评估

See all 27 posts →

公有云网络安全威胁情报（202111）：云上多个资源对外发起攻击

1 概述 2021年11月，360网络安全研究院 Anglerfish蜜罐（以下简称“蜜罐系统”）共监测到全球53745个云服务器发起的网络会话9016万次，与10月份的数据相比略有下降，IP数量下降7.7%，会话数量下降2.1%。本月我们发现了涉及政府、事业单位、新闻媒体等多个行业的单位的8个云服务器IP地址在互联网上发起扫描和攻击。 2 云服务器攻击总体情况 11月22...

Dec 9, 2021 · 14 min read

解析服务提供商对非授权域名解析情况的评估

概要 在之前的文章中，我们披露了Specter僵尸网络序利用api[.]github.com等白域名提供C2服务，以此来逃避基于签名和威胁情报匹配的安全产品的检测。其具体原理经过分析之后，发现其利用了某些域名注册/托管商(cloudns)的权威DNS服务器在解析非其客户域名方面的漏洞。 我们对此现象，即域名注册/托管商，公有云提供商等能够提供域名注册和解析...

Dec 6, 2021 · 16 min read