

PassiveDNS

解析服务提供商对非授权域名解析情况的评估



Zhang Zaifeng, litao3rd

Dec 6, 2021 • 16 min read

概要

在[之前的文章](#)中，我们披露了Specter僵尸网络利用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服务的供应商（以下统称为解析服务提供商）对非自己服务域名的DNS请求是否能够返回正确应答的情况，进行了系统的测量和评估。

这篇文章对此现象进行了分析。

数据选择及评估方法

被测域名

被测试域名：Alexa top500。选择他们作为被测域是因为：

1. 这些域名都会使用自己专有的DNS服务器，他们并不会使用外部的解析服务提供商提供的解析服务。所以如果这些域名可以被外部的解析服务提供商的NS服务器解析，那么大概率是非授权的。
2. 这些域名本身也因为其庞大而知名的业务，会被加入到各种白名单中。一些出于探测目的的人也更容易随手添加一些知名网站，而干坏事的人微了躲避检测黑名单检测，也愿意使用这些白域名。

其实使用DNS流量对域名进行排名更能精确的反应域名的流行度。36onetlab的DNSMon系统可以按照域名在DNS流量中出现的时间跨度，频次，解析稳定性等多维度来计算域名在大网的流行程度，并按天更新排名。我们没有使用它作为被测域名也是出于大众对域名排名的认知。

其实如果要躲避的检测话，白名单域名中的CDN业务或者其他类似的后台功能自动出发的流行域名也是非常合适的选择。

测试服务器

测试的NS服务器：即解析提供商。从36onetlab的passiveDNS库中提取，在最近半年活跃且为超过500个独立的二级域名提供解析服务的NS服务器，**18469**个。

测试方法

将被测域名逐个通过测试服务器尝试解析（UDP/53），如果测试服务器的DNS返回结果为NOERROR（无论是否有真实的RDATA的返回），则认为被测服务器提供了对被测域名的解析。

可能存在的误差

主要来自于数据误差，产生的原因是链路劫持。

为了覆盖最广泛的情况，我们采用udp/53的方式来收集测试数据。尽管我们已经采用了最大的努力来排除劫持的可能，考虑到较为复杂的链路环境，仍可能有少量的数据存在DNS解析结果被劫持的可能。

因为我们已经排除了最常见的劫持情况，所以即使可能有少量的劫持并不影响整体的结论。

评估结果

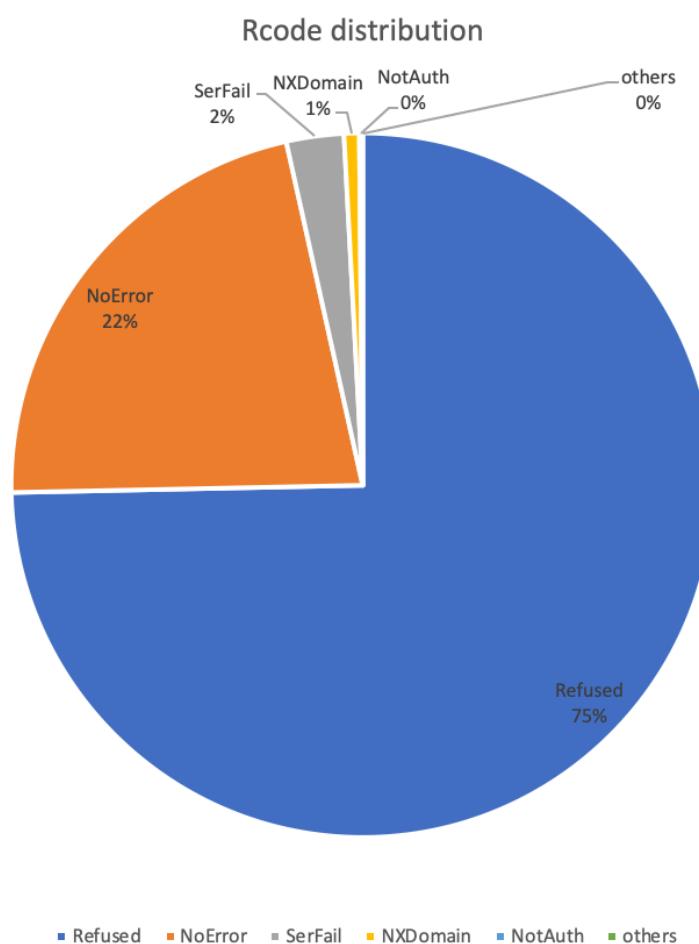
整体的解析情况

在18469个NS服务器中，能解析到地址的有18154个整体占比98.29%。在能解析到地址并且有响应的服务器有17792个，占总数的96.33%。尽管筛选的是近半年有解析记录的NS服务器，在仍有3.67%的服务器在做测试的时候处在不活跃的状态，

由此可见NS服务提供商的基础设施处在不停的变动之中。

下文以这17792个NS的数据作为分析基础。

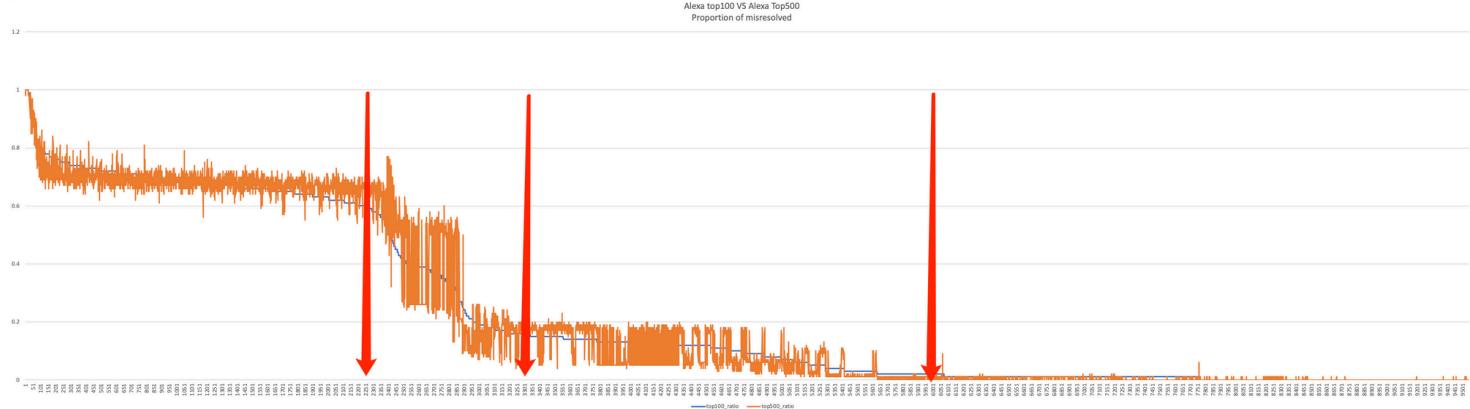
- 在解析数量方面，17792个NS服务器的响应率为70.12% ~ $(6237860/(17792*500))$ ，也就是说30%的请求在服务器活跃的情况下丢失了，一般都是服务器超时导致的。
- 在所有的响应中，Rcode为Refuse的比例为75，NOERROR的比例大约为22%。具体分布如下图



- 在NS服务器方面，17792个NS服务器中，返回NOERROR记录的NS服务器有9544个，占比约为53.64%。
- 在NS服务器的二级域方面，17792个NS对应4149个二级域，其中有返回NOERROR记录的二级域有1687个，约占总数的40.66%左右。也就是说在我们选定的测试服务器中大概有40%的NS服务器会返回非自己客户的域名解析。

根据经验，如果这种解析记录是由用户个人添加的话，猜测排名越高的域名被添加和解析的可能性越大。所以我们对每一个返回NOERROR的被测服务器都统计了其Alexa Top100的解析占比以及全部的被测域名的解析（即Alexa Top500）占比。我

们按照解析服务器对Alexa Top100域名的解析成功率进行排序。其统计曲线如下所示：



从图中可以明显的看到这9544个服务器可以分为4组，即

- 排名在1~2250的NS服务器对top100和top500的域名解析比例都在60%以上
- 排名在2250~3300的NS服务器对被测域名的解析离开快速的从60%下降到不足20%
- 排名在3300~6000的NS服务器解析比例从20%缓慢的下降到2%左右
- 排名在6000之后的NS服务器则偶有少量的解析，比例基本在1%左右。

另外从图中也可以看出来，被测域名处在Alexa Top100和Top500的比例没有显著的差异。这可能的原因是Alexa排名靠前的域名无论是100还是500对用户的感知差异不大。

解析结果的分析

另外一个对这个数据分析的角度是从其解析结果来看。这些NS服务器到底将这些流行域名解析到了哪里。

经过统计，在返回的结果中，大约有20.92%的数据在二级域上没有配置有效的DNS记录，但是返回为NOERROR，此种情况多数是针对被探测域名配置了对应的NS服务器，但是没有配置其他类型的记录所致。

解析出的IP的情况

在配置了解析记录的数据中，解析到的IP地理位置主要集中在美国，接下来是中国和俄罗斯。Top10的分布如下：

```
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
```

值的一提的是，在众多的解析记录中，有大约3%做有的解析结果为保留地址或者私有地址，在众多的此类地址中，最让人喜爱的仍然是`127.0.0.1`。Top10的地址如下：

```
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
```

记录添加人是谁？

如果解析服务商可以对目标域名提供解析，那么添加这种解析记录的人是谁？从探测的数据中，我们发现大量的解析服务提供商对不同被测域名解析的结果是相同的。我们利用这个特点，统计了NS服务器和其解析结果rdata相同的情况下，能够映射到不同的域名的数量，如果此数量超过20，则认为是解析商自己添加的。以此为标准，我们发现 2944 个解析器，占总解析器的16.55%。如果将接这些解析器聚合到二级域，那么占总二级域的7%左右。

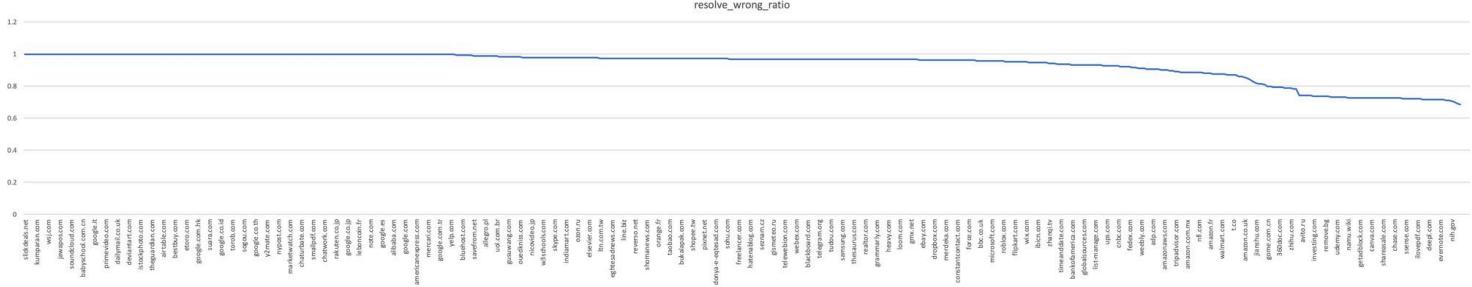
注：此处的添加人的角色判定过程是一个猜测。现在有很多注册商允许用户批量添加域名，那么在批量添加的情况下，上面计算过程使用的阈值就显得比较低了，猜测为注册商自己添加的结论也就不成立了。

我们此处假设整个添加过程仍然是个人测试性为主导，并没有使用解析商提供的批量功能。

解析结果的错误率

解析服务商对这些域名的解析可能是非授权的，不过也有可能存在解析结果和权威解析服务器返回相同结果的可能。我们对非授权的解析服务商解析的结果与正确的解析结果做了对比，发现80%的域名（即400个）的解析结果错误率在90%以上，最好情况的域名错误解析率也高达**68%**，这个比例高的有点让人吃惊。

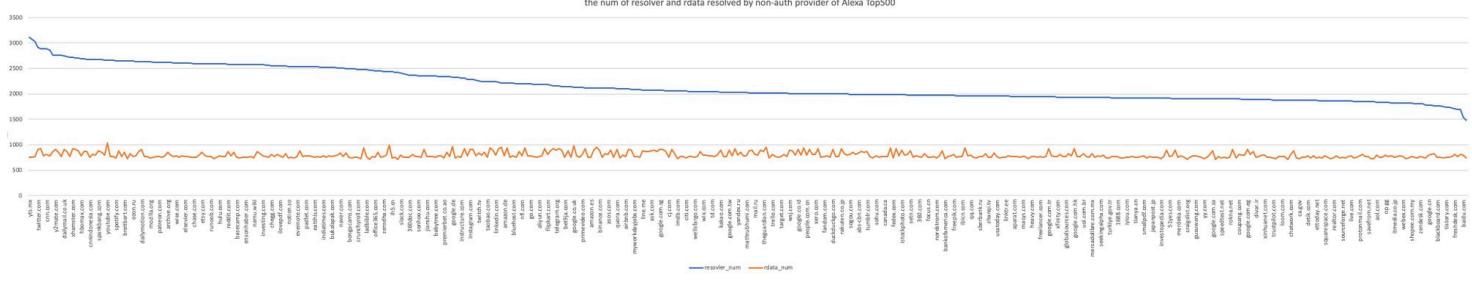
不同域名解析错误率曲线如下：



域名角度

top500域名在多少个NS上有解析？占比分布怎么样

500个域名中，最少被解析的域名为express.dhl，有1483个NS服务器可以解析它，最多的则为yts.mx，有3114个NS服务器可以解析它。不过从他们解析的结果来看，不同的域名解析的rdata个数比较稳定，大多都在800左右。可见对流行域名来说，被添加到各种非授权的解析商是非常普遍但是让人非常吃惊的事情。具体分布如下图：



案例分析

为什么这么多流行域名会加入被非授权的NS服务器解析。从整体上无法深入细节来查看，我们以yts.mx 和mozilla.org为例来看看具体的情况。

yts.mx

选择yts.mx分析是因为它是我们本次测试中，解析NS服务器最多的一个域名。yts.mx是通过p2p协议工具使用BitTorrents等工具下载电影的网站，在我们使用的Alexa数据中排名462。通过passiveDNS.cn来查看，其从2020年4月开始，一直使用cloudflare作为其解析商。

```
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
```

因为本次测试中，因为包含了cloudflare的NS服务器，而yts.mx的官方解析商也是cloudflare，在排除掉cloudflare之后，仍有2886个非授权解析服务器可以解析yts.mx，这个数量仍然可以排在我们本次测试的TOP5。

在2886个非授权解析服务器中，仅有73个可以解析到正确的结果，错误解析率高达**97.47%**，这个比例是让人吃惊的。

从非授权解析服务器来看其涵盖的二级域名有383个，主要是域名注册商。头部的10个解析器的二级域名如下：

```
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
```

这个列表中大多都是提供域名注册，web服务托管，主机服务等IT基础服务提供商。不出所料我们上一篇文章中提到的cloudns在列。

从解析错误的IP来看，2886个非授权解析服务器，共解析到750个IP地址，聚合到了149个网段。其中top10的网段及这些网段的用途分析如下：

CIDR/24	resolver_num	resolver_owner	function
217.70.184	520	gandi.net	parking/redirecting
		register.com worldnic.com	
209.99.64	451	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
		active-dns.com aloojamiento.com bigrock.com bigrock.in bluehost.com ctctdns.com ctctdns.net dns.mn domainesia.com domainmonger.co m gatordns.com gatordns.net gatordns.org genious.net guzelhosting.com heberjahiz.com hostgator.in indiacyberspace.c om kheweul.net launchpad.com mitsu.in monovm.com mysafedns.com	
208.91.197	163	orderbox-dns.com	parking/redirecting
108.167.189	113	hostgator.com	default page
127.0.0	65		

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

mozilla.org

选择mozilla.org是因为mozilla.org是火狐浏览器的官方网站，在我们使用的Alexa排名182，为大众所熟知。mozilla.org的权威NS服务器通过passiveDNS.cn来查看，其从2014年开始就一直使用akamai作为其解析商没有变过。

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

其解析结果随着时间有变动，但是2020年11月之前使用自己的服务，之后则非常稳定的使用amazon的服务。

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	

但是在实际网络中，能够解析mozilla.org的NS服务器多达2624个，解析的IP地址有735个。

头部的10个解析器的二级域名如下：

```
831 hostgator.com
633 cloudflare.com
366 register.com
79 orderbox-dns.com
75 akam.net
50 hostgator.mx
45 dan.hosting
33 cloudns.net
14 hostgator.co
13 zoneedit.com
```

和yts.mx类似，这个列表中大多都是提供域名注册，web服务托管，主机服务等IT基础服务提供商。同样不出所料我们上一篇文章中提到的cloudns也在列。

另一个值得关注的点是 akam.net 自身也有75个服务器提供对mozilla.org的解析，不过所有的服务器解析结果是相同且正确的。也就是说akamai提供的权威解析器可以交叉解析其托管域名。

除此之外，cloudflare的解析看起来可能也是对的。为什么是可能？因为我们发现从passiveDNS数据来看从2016年4月份开始，一直到2021年11月份，www.mozilla.org 使用了cloudflare的CDN服务，其CNAME记录是cloudflare.net，从2021年11月开始逐步切换到了amazon。不过 mozilla.org的ns服务器从未使用过cloudflare的解析器。

2021-11-11 06:04:44	2021-12-03 15:12:41	1572161 www.mozilla.org CNAME www.mozorg.moz.works
2016-04-08 23:45:11	2021-11-19 19:44:25	285033534 www.mozilla.org CNAME www.mozilla.org.cdn.cloudflare.net

从解析结果来看，除掉akam.net以及cloudflare.com之外，仅有62个解析器可以正确的将解析结果返回。也就是说**70%**的非授权解析器解析结果是错误的，这个比例也同样让人吃惊。

在解析的错误IP方面，730个错误IP（有5个IP是正确的解析结果），聚合到了153个CIDR/24网段，其中top10网段占总错误解析量的75.9%。我们详细分析了错误解析的Top10的CIDR/24网段，发现主要是域名注册/解析商注册，最终解析目的IP是用于域名停靠、重定向以及域名出售等目的，基本都是域名注册商的赚钱的基本手段。具体结果见下图：

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 ctcdns.com ctcdns.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 sibernetname.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 WebHost4Life.com yourhostingaccount.com	
66.96.162	39	yourwebhosting.com	default page

从以上两个案例来看，目前提供这种非授权解析服务的主要是域名注册/解析商注册，最终解析目的IP是用于域名停靠、重定向以及域名出售等目的，基本都是域名注册商的赚钱的基本手段。

安全检测

首先这种现象为什么没有引起关注？需要说明的是尽管它广泛存在，但是流量整体比较少，整体流量少是因为入口流量少，大多数的DNS流量走的公共DNS服务器，所以除非在特定网络环境下，否则此种现象很难被注意到。

其次解析服务提供商对非授权域名的解析在安全方面带来了不少的挑战。新的DNS安全检测角度，需要扩展，既要看域名，也要看域名使用的DNS服务器，同时还要看解析结果是否和真实的解析结果一致。

NS服务器角度

在传统的检测方法中，一般对DNS服务器一般会忽略。在APT组织海莲花的攻击行为中，就曾经出现过特定域名只有特定的NS服务器才可以解析的情况。

因此小众的DNS是很值得关注的。这里说的小众就是指其请求客户端少，请求域名数量少。尤其是在网络等级较高的环境中，客户端直接和小众的DNS服务器通信的情况就值得做进一步的分析了。

流量侧角度

1. 从流量中筛选出小众的DNS服务器
2. 筛选出网络内DNS服务器与客户端
3. 针对客户端与小众DNS服务器的流量进行检查
4. 检查结果和大众解析结果进行比对
5. 如果存在差异，需要结合其他维度的数据做进一步分析

结论

1. 组织内网要规范使用DNS服务器，对于组织内的非递归服务器之外的其他DNS请求的目标地址要做严格的检查和筛选
2. 域名解析提供商广泛的解析非自己客户的域名
3. 提供这种业务的主力是域名注册商，目的（猜测）是为了拉拢客户或者提升流量
4. 业界没有统一的标准来规范此类解析行为
5. 已经出现恶意程序使用这种方式逃避检测
6. 对基于签名和威胁情报简单匹配的安全产品存在较大的挑战



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)

Name



Share

Best Newest Oldest

Be the first to comment.

[Subscribe](#)[Privacy](#)[Do Not Sell My Data](#)

— 360 Netlab Blog - Network Security Research Lab at 360 —

PassiveDNS



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)

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

PassiveDNS

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

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

DDoS

EwDoor僵尸网络，正在攻击美国AT&T用户

背景介绍 2021年10月27日，我们的BotMon系统发现有攻击者正通过CVE-2017-6079漏洞攻击Edgewater Networks设备，其payload里有比较罕见的mount文件系统指令，这引起了我们的兴趣，经过分析，我们确认这是一个全新的僵尸网络家族，基于其针对Edgewater产商、并且有Backdoor的功能，我们将它命名为EwDoor。最初捕获的EwDoor使用了常见的...

[See all 27 posts →](#)



Dec 8,
2021

8 min
read



Dec 1,
2021

18 min
read