PassiveDNS

被拦截的伊朗域名的快速分析

Zhang Zaifeng
Jun 25, 2021 • 10 min read

伊朗新闻网站被美国阻断的事成为了最近的新闻热点，报道的主要内容是：

> *美国司法部查封36个伊朗的新闻网站，其中许多网站与伊朗的“虚假信息活动”有关。这些网站首页通知显示，根据美国法律，这些网站已被美国政府查封，通知上还附有美国联邦调查局和美国商务部产业安全局的印徽。*

到底哪些新闻站被拦截了，我们查询了几个新闻源都没有给出全部被拦截的网站列表。
其实这种从域名角度做拦截的手段，总是会在大网的DNS/whois数据中留下踪迹。我们利用这些网络基础数据分析出了32+2个被拦截的伊朗新闻网站的域名，其中的2个域名是在今年3月和4月份被拦截的；通过技术分析，也确认这些修改是直接通过注册局进行的改动。被拦截的域名的详细列表见文末。

分析

我们拿其中被拦截的域名之一alalamtv.net 来做一个分析(见相关新闻报道)。

DNS记录

从该域名出发，我们利用PassivedDNS记录可以看到，其NS服务器和IP地址在6月23号的凌晨3点40开始发生了变化，无论NS服务器还是IP地址都切换到了亚马逊的服务器。

2021-06-23 10:29:21	2021-06-23 18:25:10	47	alalamtv.net	A	13.32.123.72
2021-06-23 10:29:21	2021-06-23 18:25:10	47	alalamtv.net	A	13.32.123.71
2021-06-23 10:29:21	2021-06-23 18:25:10	47	alalamtv.net	A	13.32.123.17
2021-06-23 10:29:21	2021-06-23 18:25:10	47	alalamtv.net	A	13.32.123.90
2021-06-23 10:34:09	2021-06-23 17:30:29	45	alalamtv.net	A	99.84.238.113
2021-06-23 10:34:09	2021-06-23 17:30:29	45	alalamtv.net	A	99.84.238.146
2021-06-23 10:34:09	2021-06-23 17:30:29	45	alalamtv.net	A	99.84.238.177
2021-06-23 10:34:09	2021-06-23 17:30:29	45	alalamtv.net	A	99.84.238.209
2021-06-23 11:05:56	2021-06-23 17:09:43	35	alalamtv.net	A	13.226.214.118
2021-06-23 11:05:56	2021-06-23 17:09:43	35	alalamtv.net	A	13.226.214.97
2021-06-23 11:05:56	2021-06-23 17:09:43	35	alalamtv.net	A	13.226.214.26
2021-06-23 11:05:56	2021-06-23 17:09:43	35	alalamtv.net	A	13.226.214.9
2021-06-23 10:37:42	2021-06-23 16:52:56	27	alalamtv.net	A	13.225.149.31
2021-06-23 10:37:42	2021-06-23 16:52:56	27	alalamtv.net	A	13.225.149.60
2021-06-23 10:37:42	2021-06-23 16:52:56	27	alalamtv.net	A	13.225.149.109
2021-06-23 10:37:42	2021-06-23 16:52:56	27	alalamtv.net	A	13.225.149.16
2021-06-23 12:55:31	2021-06-23 16:18:36	2	alalamtv.net	NS	ns-388.awsdns-48.com
2021-06-23 12:55:31	2021-06-23 16:18:36	2	alalamtv.net	NS	ns-1900.awsdns-45.co.uk
2021-06-23 12:55:31	2021-06-23 16:18:36	2	alalamtv.net	NS	ns-1088.awsdns-08.org
2021-06-23 12:55:31	2021-06-23 16:18:36	2	alalamtv.net	NS	ns-977.awsdns-58.net
2021-06-23 03:40:39	2021-06-23 15:04:50	7	alalamtv.net	A	65.8.17.114
2021-06-23 03:40:39	2021-06-23 15:04:50	7	alalamtv.net	A	65.8.17.94
2021-06-23 03:40:39	2021-06-23 15:04:50	7	alalamtv.net	A	65.8.17.14
2021-06-23 03:40:39	2021-06-23 15:04:50	7	alalamtv.net	A	65.8.17.76
2021-06-23 13:56:47	2021-06-23 14:03:14	2	alalamtv.net	A	13.227.73.28
2021-06-23 13:56:47	2021-06-23 14:03:14	2	alalamtv.net	A	13.227.73.129
2021-06-23 13:56:47	2021-06-23 14:03:14	2	alalamtv.net	A	13.227.73.111
2021-06-23 13:56:47	2021-06-23 14:03:14	2	alalamtv.net	A	13.227.73.4
2019-06-08 22:04:53	2021-06-22 14:17:54	261	alalamtv.net	NS	ns3.alalamtv.net
2021-04-09 04:11:24	2021-06-22 14:17:54	12	alalamtv.net	NS	ns1
2021-04-09 04:11:24	2021-06-22 14:17:54	12	alalamtv.net	NS	ns2
2020-04-23 19:19:37	2021-06-22 14:12:25	55	alalamtv.net	MX	mxb.irib.ir
2020-04-23 19:19:37	2021-06-22 14:12:25	55	alalamtv.net	MX	mxa.irib.ir
2018-12-17 11:06:01	2021-06-22 11:52:22	11916	alalamtv.net	A	192.99.38.90

whois记录

先说结论：通过对不同域名的whois数据来看，并比对了同一域名在注册局和注册商（注册局和注册商的解释见下）返回的whois数据，推出是由对应的注册局绕过来域名拥有者和注册商直接对域名的解析信息作的修改。

下面是具体的技术分析细节。

whois数据分析

在介绍利用whois数据分析被拦截的域名之前，先对域名注册流程，注册过程中涉及到的相关实体和whois数据的相关信息做一下简单介绍。

> *注册人*
> *注册域名的个人或者单位，是域名所有者。*
> *注册商*
> *注册商是是一个商业实体或组织，它们由互联网名称与数字地址分配机构（ICANN）或者一个国家性的国家代码顶级域名（ccTLD）域名注册局委派，以在指定的域名注册数据库中管理互联网域名，向公众提供此类服务。并负责提供DNS解析、域名变更过户、域名续费等操作。比如国内的阿里云或者国外的Godday就是域名注册商。*
> *注册局*
> *注册局是顶级域名下注册的域名的数据库的操作者。比如 .com/.net的域名注册局为Verisign公司，.cn域名的域名注册局为cnnic。注册局维护自己负责的顶级域名的数据库。*
> *域名注册的流程*
> *一般的域名注册流程是域名注册人向注册商提出注册申请，注册商将注册信息（域名注册人，注册时间，过期时间等等）传给注册局，注册局将必要信息同步到顶级域名数据库。这样你的域名就可以在互联网上解析，被人访问到了。*
> *以360的域名360.cn为例： 注册人（北京奇虎科技有限公司) --> 注册商（厦门易名科技股份有限公司） --> 注册局（中国互联网信息中心CNNIC）*
> *什么是域名的Whois数据*
> *Whois数据就是记录了一个域名在注册时的基本信息（如域名所有人、联系方式，域名注册商、域名注册日期，过期日期，当前域名的状态和域名当前所使用的DNS*

服务器等等）。whois数据的查询是对公众开放的，可以用来查询域名是否已经被注册以及刚才提到的注册域名的详细信息。

从哪里获取域名的whois数据

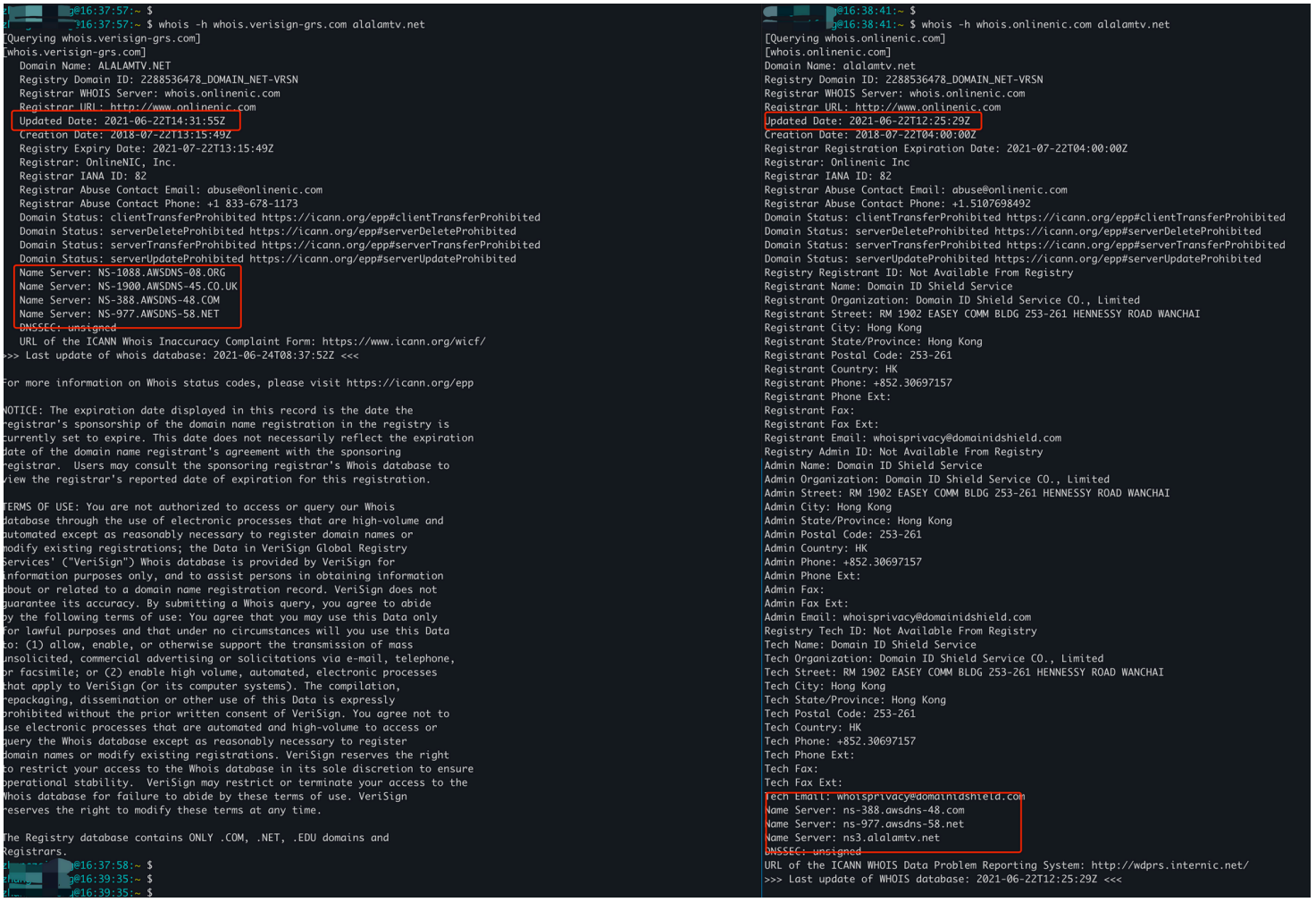
一个域名的whois数据可以从注册该域名的注册商获得，也可以从负责该域名顶级域的注册局处获得。一般来说注册商的whois数据会更完整，注册局的信息则更能反应域名解析的当前状态。对普通人来说，现在很多公司/机构都有查询域名状态的接口。搜索“whois查询”就能查到很多提供whois查询服务的网站。

接下来我们看一下这些域名的whois记录有没有什么变化，果然在6月22号的14点有过一次更新，结合whois的历史记录，变更的正式NS服务器地址，应该就是在这个时间点开始，域名的解析发生了变化。

```
========== 2021-06-24 12:48:04 ==========
alalamtv.net    domainname              alalamtv.net
alalamtv.net    createddate             2018-07-22 04:00:00
alalamtv.net    updateddate             2021-06-22 14:31:55
alalamtv.net    expiresdate             2021-07-22 13:15:49
alalamtv.net    status                  clientTransferProhibited | serverDeleteProhibited | serverTransferProhibited | serverUpdateProhibited
alalamtv.net    registrant_email        whoisprivacy@domainidshield.com
alalamtv.net    registrant_name         Domain ID Shield Service
alalamtv.net    registrant_organization Domain ID Shield Service CO., Limited
alalamtv.net    registrant_address      RM 1902 EASEY COMM BLDG 253-261 HENNESSY ROAD WANCHAI
alalamtv.net    registrant_city         Hong Kong
alalamtv.net    registrant_state        Hong Kong
alalamtv.net    registrant_postalcode   253-261
alalamtv.net    registrant_country      HONG KONG
alalamtv.net    registrant_telephone    +852.30697157
alalamtv.net    admin_email             whoisprivacy@domainidshield.com
alalamtv.net    admin_name              Domain ID Shield Service
alalamtv.net    admin_organization      Domain ID Shield Service CO., Limited
alalamtv.net    admin_address           RM 1902 EASEY COMM BLDG 253-261 HENNESSY ROAD WANCHAI
alalamtv.net    admin_city              Hong Kong
alalamtv.net    admin_state             Hong Kong
alalamtv.net    admin_postalcode        253-261
alalamtv.net    admin_country           HONG KONG
alalamtv.net    admin_telephone         +852.30697157
alalamtv.net    tech_email              whoisprivacy@domainidshield.com
alalamtv.net    tech_name               Domain ID Shield Service
alalamtv.net    tech_organization       Domain ID Shield Service CO., Limited
alalamtv.net    tech_address            RM 1902 EASEY COMM BLDG 253-261 HENNESSY ROAD WANCHAI
alalamtv.net    tech_city               Hong Kong
alalamtv.net    tech_state              Hong Kong
alalamtv.net    tech_postalcode         253-261
alalamtv.net    tech_country            HONG KONG
alalamtv.net    tech_telephone          +852.30697157
alalamtv.net    registrarname           Onlinenic Inc
alalamtv.net    whoisserver             whois.onlinenic.com
alalamtv.net    nameservers             ns-388.awsdns-48.com | ns-977.awsdns-58.net | ns3.alalamtv.net
alalamtv.net    first_seen              2021-06-24 12:48:04
========== 2021-01-31 12:31:22 ==========
alalamtv.net    domainname              alalamtv.net
alalamtv.net    createddate             2018-07-22 04:00:00
alalamtv.net    updateddate             2021-01-30 11:54:55
alalamtv.net    expiresdate             2021-07-22 13:15:49
alalamtv.net    status                  clientTransferProhibited
alalamtv.net    registrant_email        whoisprivacy@domainidshield.com
alalamtv.net    registrant_name         Domain ID Shield Service
alalamtv.net    registrant_organization Domain ID Shield Service CO., Limited
alalamtv.net    registrant_address      RM 1902 EASEY COMM BLDG 253-261 HENNESSY ROAD WANCHAI
alalamtv.net    registrant_city         Hong Kong
alalamtv.net    registrant_state        Hong Kong
alalamtv.net    registrant_postalcode   253-261
alalamtv.net    registrant_country      HONG KONG
alalamtv.net    registrant_telephone    +852.30697157
alalamtv.net    admin_email             whoisprivacy@domainidshield.com
alalamtv.net    admin_name              Domain ID Shield Service
alalamtv.net    admin_organization      Domain ID Shield Service CO., Limited
alalamtv.net    admin_address           RM 1902 EASEY COMM BLDG 253-261 HENNESSY ROAD WANCHAI
alalamtv.net    admin_city              Hong Kong
alalamtv.net    admin_state             Hong Kong
alalamtv.net    admin_postalcode        253-261
alalamtv.net    admin_country           HONG KONG
alalamtv.net    admin_telephone         +852.30697157
alalamtv.net    tech_email              whoisprivacy@domainidshield.com
alalamtv.net    tech_name               Domain ID Shield Service
alalamtv.net    tech_organization       Domain ID Shield Service CO., Limited
alalamtv.net    tech_address            RM 1902 EASEY COMM BLDG 253-261 HENNESSY ROAD WANCHAI
alalamtv.net    tech_city               Hong Kong
alalamtv.net    tech_state              Hong Kong
alalamtv.net    tech_postalcode         253-261
alalamtv.net    tech_country            HONG KONG
alalamtv.net    tech_telephone          +852.30697157
alalamtv.net    registrarname           Onlinenic Inc
alalamtv.net    whoisserver             whois.onlinenic.com
alalamtv.net    nameservers             ns1.alalamtv.net | ns2.alalamtv.net | ns3.alalamtv.net
alalamtv.net    first_seen              2021-01-31 12:31:22
```

上面的whois记录看，有两点值得说明：

1. NS服务器从whois记录和DNS记录中看到的不一致。因为whois信息在注册商和注册局可能存在不一致。我们分别查看了该域名在注册商（onlinenic.com）和注册局（verisign-grs.com）的whois信息（左边为注册局，左边为注册商），如下：



可以看到：

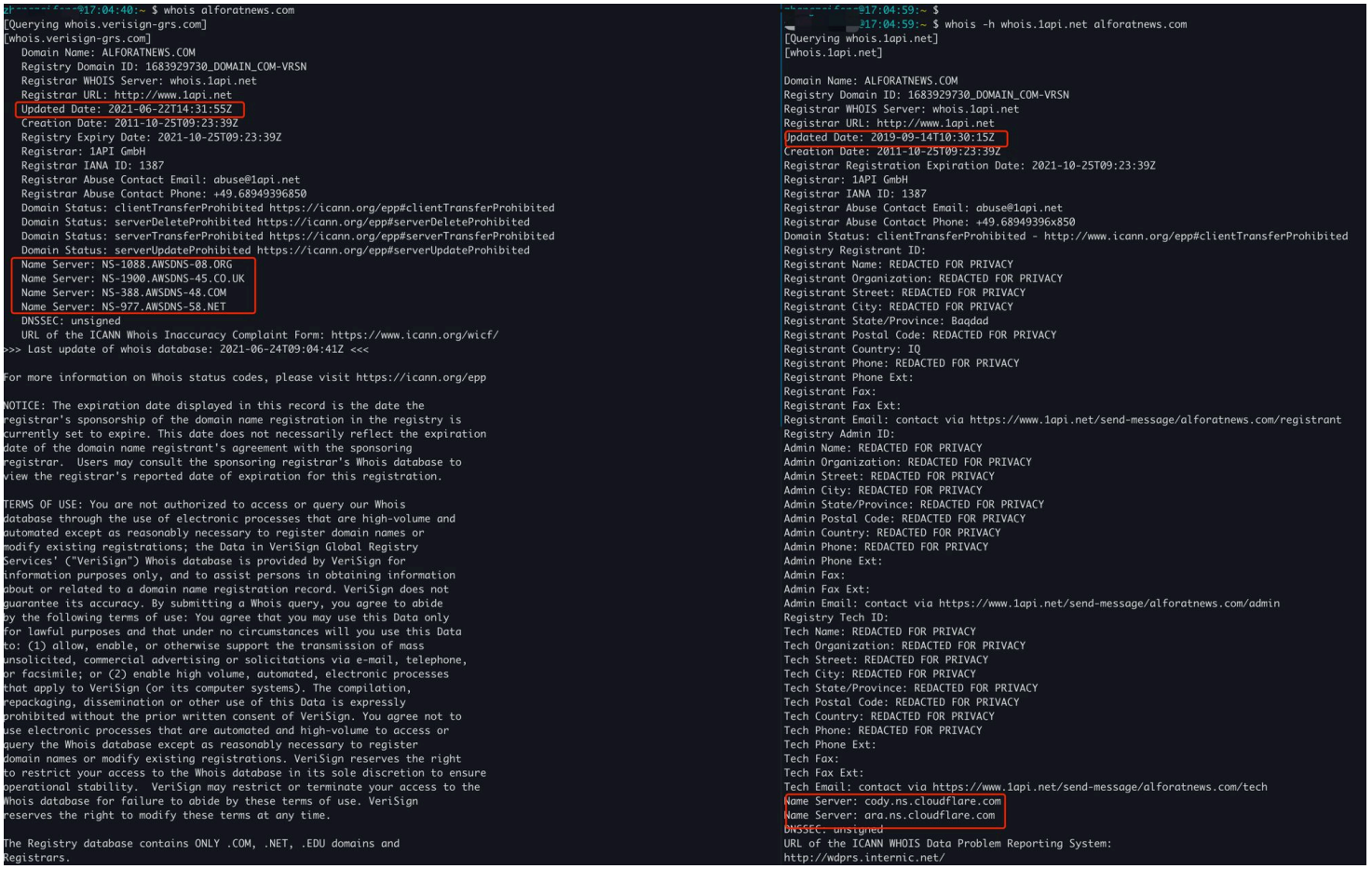
- 注册局的NS服务器全部为amazon的服务器，注册商的则有两个amazon的服务器，还有一个之前老的alalmtv.com自己的NS服务器。注册商和注册局的数据不一致。
- 注册商的更新时间要比注册局的更新时间早大约两个小时。

以上两点推断：注册局和注册商同步了部分信息（比如NS服务器有部分重合），同步之后，注册局对可能注册信息进行了再次修改，导致其修改时间比注册商晚了两个小时。

2. 第二点不一样的是域名状态，相比老的记录，新的记录中，域名状态多了几个server开头状态，而server开头的状态均由注册局设置。关于这些代码的含义，可以参考ICANN关于EPP状态码的解释。

如果再对比另外一个被拦截的域名 `alforatnews.com`，该域名的注册商是注册于1api.net，和 `alalamtv.net` 并不是同一家注册商。可以更清晰的看到注册局和注册商（左边为注册局，右边为注册商）对该域名的whois信息完全不同。注册商的

whois信息完全再拦截前后完全没有任何变化，而注册局的更新时间，域名状态和NS服务器则发生了明显的变化，显然是注册局绕过注册商对注册信息进行了修改。如下图：



经过分析，发现其他被拦截的域名也有类似的注册局和注册商信息完全不同步的情况。

挖掘更多被拦截的域名

结合DNS数据和whois数据，判定是通过对域名的权威DNS服务器的接管达到了对域名的冻结。
针对这两个域名可以这么做，那么其他的域名劫持方式也是类似的。

此时利用PassiveDNS数据库，可以很方便的把被劫持的域名抽取出来，目前利用网络基础数据可以挖掘的36个被拦截的域名中的32个他们均在2021.06.22被冻结，另发现2个域名分别在**2021.03.25**和**2021.04.17**冻结，具体见下文。分别涉及 `tv, net, com, org` 四个顶级域。其中 `tv, net, com` 归Verisign管理， `org` 则归PIR管理。

关于域名所有权，注册局/注册商，冻结/接管域名的问题

冻结/拦截域名的流程，从入口来说是域名注册局/域名注册商，那么究竟在什么样的情况下可以对域名实施接管（domain take-down）？

在ICANN现有体系下，注册商和注册局，自己是没有权力自行主动发起域名接管流程的。
一般情况下，如果域名被滥用，如版权纠纷，钓鱼网站，僵尸网络，恶意软件；那么很明确，需要有用户/安全厂商发起投诉，注册局/注册商紧接着才可以实施域名接管。
还有一种情况是注册商和注册局接收到法院的命令的时候，也必须执行。美国对伊朗域名接管的事件，都是通过法院下达命令。这次涉及到的几个域名注册局，都是美国公司，所以不得不执行法院的规定。有如下相关内容可以供参考:

- 在2011年10月份的时候，theregister.com网站刊登了美国的移民和海关执法局（Immigration and Customs Enforcement，ICE)的资深探员针对 `.com` 域名管辖权的意见，他认为，.com下面所有域名都应该受到美国法律的管辖。(**Senior ICE agents are on record saying that they believe all .com addresses fall under US jurisdiction.**)。
- 在2020年11月份美国司法部公共事务办公室的在“冻结伊朗革命卫队使用的域名”的公告中提到国家安全助理司法部长约翰·C·德默斯对外部势力利用美国公司进行进行宣传的说法：“我们将继续使用，我们所有的工具来阻止伊朗政府滥用美国公司和社交媒体来暗中传播宣传、试图秘密影响美国公众，并挑拨离间。（We will continue to use all of our tools to stop the Iranian Government from **misusing U.S. companies and social media** to spread propaganda covertly, to attempt to influence the American public secretly, and to sow discord）。

被拦截的域名列表

```
afaq.tv
ahlulbayt.tv
alalamtv.net
al-anwar.tv
```

```
aleshraq.tv
alforatnews.com
alimantv.com
alkawthartv.com
almaalomah.org
almaalomah.com  (2021.04.17 冻结)
almaaref.tv
almasaraloula.tv
almasirah.net
almasirah.tv
alnaeem.tv
asiasat.tv
assirat.tv
haditv.com
hidayat.tv
hodhod.tv
interaztv.com
irtvu.com
kafmedia.net
karbala-tv.net
kataibhezbollah.org
kudustv.com
lualuatv.com
nabaa.tv
nooraf.tv
paltoday.tv
presstv.com
r-m-n.net (2021.03.25 冻结)
u-news.net
wintvindia.com
```

版权

nday

Mirai_ptea Botnet利用KGUARD DVR未公开漏洞报告

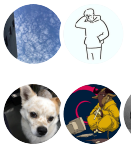
2021-06-22我们检测到一个我们命名为mirai_ptea的mirai变种样本通过未知漏洞传播。经过分析，该漏洞为KGUARD DVR未公开的漏洞。从我们的分析看该漏洞存在于2016年的固件版本中。我们能找到的2017年之后的固件厂家均已经修复该漏洞

Backdoor

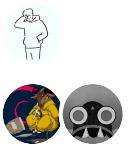
窃密者Facefish分析报告

背景介绍 2021年2月，我们捕获了一个通过CWP的Nday漏洞传播的未知ELF样本，简单分析后发现这是一个新botnet家族的样本。它针对Linux x64系统，配置灵活，并且使用了一个基于Diffie–Hellman和Blowfish的私有加密协议。但因为通过合作机构（在中国区有较好网络通信观察视野）验证后发现对应的C2通信命中为0，所以未再深入分析。 2021年4...

See all 27 posts →



Jul 1, 2021 • 12 min read



May 28, 2021 • 17 min read