

DNSMon

DNSMon: 用DNS数据进行威胁发现(3)



suqitian, Alex.Turing

Feb 8, 2021 • 10 min read

--- *Linux, Windows, Android, 一个都不能少*

背景

本文是介绍DNSMon在生产威胁情报(域名IoC)系列文章的第三篇。

DNS协议作为互联网的一项基础核心协议，是互联网得以正常运行的基石之一。在祖国960万平方公里的土地上，那一张纵横交错的数据网络里，每一秒都有数万亿计的DNS数据包在高速穿梭着，它们或来自于机房的服务器，或来自于办公室的电脑，或来自于我们身边的手机，或来自于场景繁多的IoT，总之DNS无处不在。

生长于斯的DNSMon，依托DNS协议的基础性，天然具备宽广的视野，对那些发生在不同行业或不同平台的安全事件，都能有所涉猎。在DNSMon科普系列的前两篇博文中，[第一篇](#)提及的Skidmap是感染Linux平台的云主机；而[第二篇](#)提及的一组域名是网吧的Windows平台被感染后发出的；本文则是一个涉及Android平台的案例。

如果仔细阅读文章并理解其中内容，可以看到DNSMon在面对3个差异巨大的平台时，所使用的知识点或者说规则并没有根本性的变化，几乎做到了无差别预警。

对未知威胁的拦截

最近，我们注意到DMSMon从2021-01-10开始，陆续对一组结构相似的域名报黑并自动拦截。

```
BLOCK:      utionstro.top (from 2021-01-10 to [REDACTED])
--  
BLOCK:      lesseased.top (from 2021-01-12 to [REDACTED])
--  
BLOCK:      ssuminat.top (from 2021-01-14 to [REDACTED])
--  
BLOCK:      holidano.top (from 2021-01-16 to [REDACTED])
--  
BLOCK:      thinkdisen.top (from 2021-01-17 to [REDACTED])
```

登录系统查看采集到的关联信息，我们看到这是一组跟Android平台相关的恶意域名。正好系列文章没有介绍过跟Android平台相关的博文，而前两篇赶巧一篇跟Linux相关，一篇跟Windows有关，为科普DNSMon而写篇Android的，集齐3大平台不失为一件趣事。

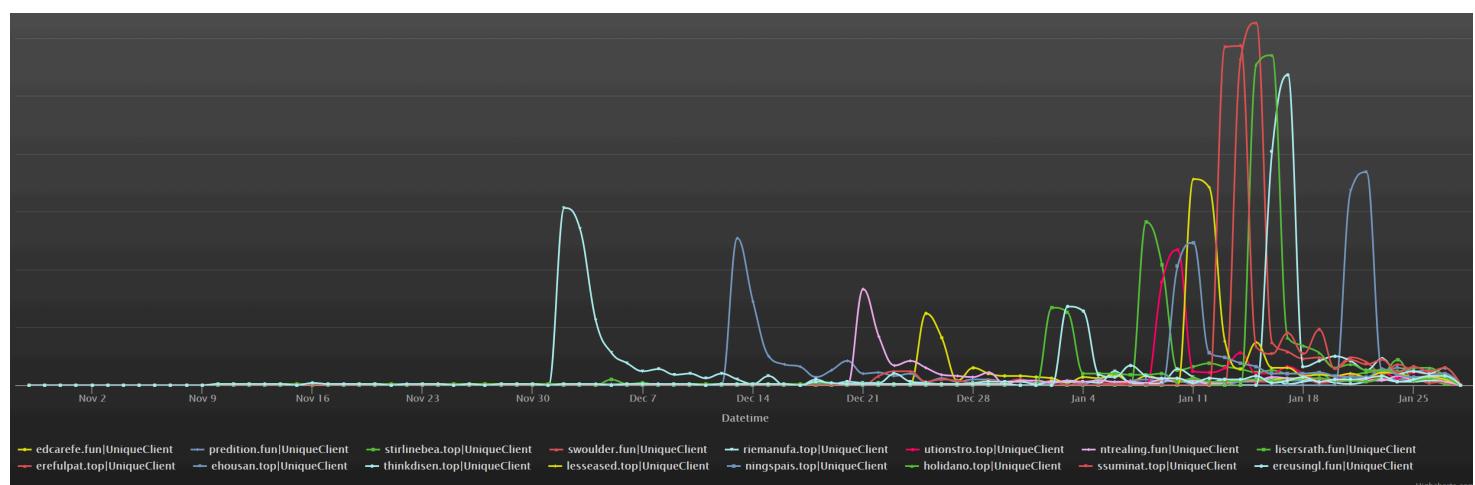
扩展同类域名

利用自动拦截域名的rdata和其它数据，发现DNSMon其实不止预警了上图列举的5个域名，在这个类别里一共有16个域名。

```
ereusingl[.]fun
lisersrath[.]fun
predition[.]fun
ningspais[.]top
ssuminat[.]top
erefulp[.]top
stirlinebea[.]top
utionstro[.]top
lesseased[.]top
thinkdisen[.]top
edcarefe[.]fun
holidano[.]top
ehousan[.]top
swoulder[.]fun
```

riemanufa[.]top
ntrealing[.]fun

从活跃时间上看，这16个域名是依次投入使用的，且在2021年1月份有一个比较密集的投放期。



在写本文的过程中，又陆续看到系统捕获到其它新的同类域名被投入使用，比如 antdaugh[.]top, ngsllalatfin[.]top等等，但为了行文的连贯，本文会略过这些新启用的域名。

判黑缘由

在第一篇文章里，我们提及：

DNSMon的核心在于将海量的DNS数据与360所拥有安全相关数据（包括whois, web, 沙箱, 蜜罐, 证书等等）交叉对比，并从中分析得出威胁情报IOC。

下面我们从系统获取的whois和沙箱这两个数据出发，举例分析数据特征并注解判黑缘由。当然，除了这些数据，DNSMon的判黑流程还依赖其它的特征数据，在此就不一一列举了。

1. whois

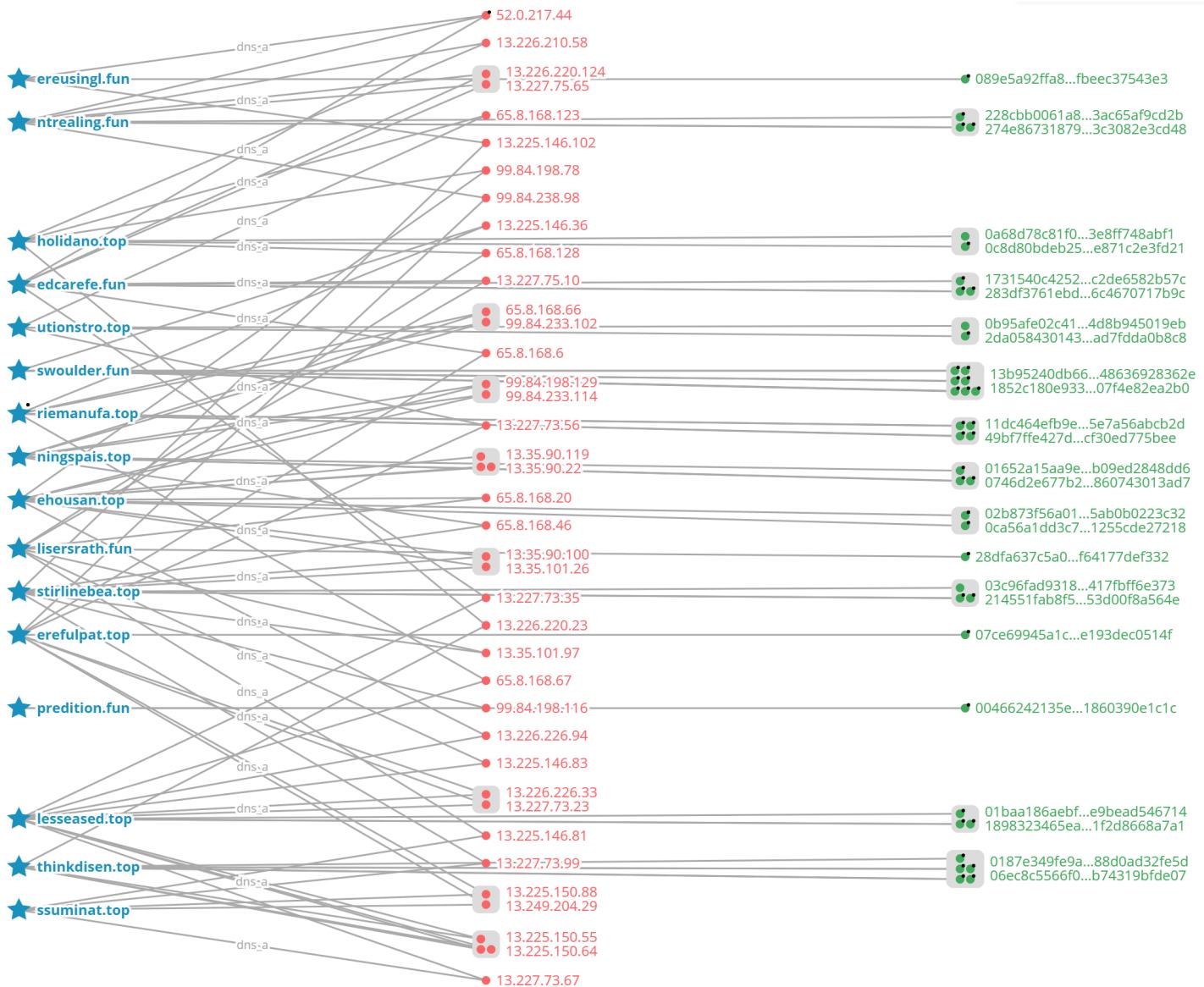
16个域名共分成两批注册，一批注册时间为2020-11-06，另一批为2020-12-23；注册的有效期时长：一年，且开启了隐私保护。

ereusingl.fun	createddate	2020-11-06 10:10:12
ereusingl.fun	updateddate	2020-11-06 10:20:27
ereusingl.fun	expiresdate	2021-11-06 23:59:59
ereusingl.fun	status	addPeriod clientTransferProhibited se
lisersrath.fun	createddate	2020-11-06 10:10:12
lisersrath.fun	updateddate	2020-11-06 10:20:20
lisersrath.fun	expiresdate	2021-11-06 23:59:59
lisersrath.fun	status	addPeriod clientTransferProhibited se
predition.fun	createddate	2020-11-06 10:09:51
predition.fun	updateddate	2020-11-06 10:15:26
predition.fun	expiresdate	2021-11-06 23:59:59
predition.fun	status	addPeriod clientTransferProhibited se
...		
ningspais.top	createddate	2020-12-23 15:57:59
ningspais.top	updateddate	2021-01-06 10:37:20
ningspais.top	expiresdate	2021-12-23 15:57:59
ningspais.top	status	clientTransferProhibited
ssuminat.top	createddate	2020-12-23 15:58:00
ssuminat.top	updateddate	2021-01-06 10:37:23
ssuminat.top	expiresdate	2021-12-23 15:58:00
ssuminat.top	status	clientTransferProhibited
erefulpat.top	createddate	2020-12-23 15:58:01
erefulpat.top	updateddate	2021-01-06 10:37:24
erefulpat.top	expiresdate	2021-12-23 15:58:01
erefulpat.top	status	clientTransferProhibited
...		

批量注册+新域名+注册有效期短+隐私保护，判黑可能性加分。

2. 沙箱

DNSMon对沙箱的数据，主要是关注样本的网络行为并提取样本到域名的访问关系，然后借助样本的评分反过来评估域名的得分。从关联图可以看到，访问域名的样本在系统里都有恶意标签（样本右上角标注了“黑色圆点”）。



根据标签传播算法，16个域名判黑的可能性加分。

借助DNSMon的一系列关联数据，最终可以判定这是一组恶意域名，且性质为downloader。为了清晰样本传播目的，我们对样本进行了的简单地逆向分析。

逆向分析

本文选取一个名为 `Your File Is Ready To Download.apk` 的样本作为分析对象，它的基本信息如下所示

`MD5: 230ca35f90c55bf9c46ddfb798ob632d`

`File type: Android`

Magic: Zip archive data, at least v2.0 to extract

File size: 543671 bytes

样本的 `Assets` 有一个dat文件，里面有Base64编码的配置信息。

它的内容是：

```
eyJjaWQiOiIxZGZiZTAzNS1kNzViLTQzYzgtYmMwMy1kYTg5YWU5NzU1ZjYiLCJ1cmxzIjpBImh0dHBz0i8vb
```

Base64解码后，得到以下json格式的配置信息，可以看到"urls"字段里存有我们要定性的域名。

```
{
  "cid": "1dfbe035-d75b-43c8-bc03-da89ae9755f6",
  "urls": [
    "https[:]//lisersrath.fun"
  ],
  "fn": "Your File Is Ready To Download",
  "info": "blank_",
  "routes": {
    "x86": "/x86",
    "arm64-v8a": "/arm64",
    "x86_64": "/x64",
    "armeabi-v7a": "/arm"
  },
  "uid": "888098709355331972",
  "sid1": "888098709355331972",
  "tid": "792297",
  "sid2": ""
}
```

通过以下代码片段向urls中的域名请求下载数据，

这个过程会产生如下的URL：

```
lisersrath[.]fun/x86?v=0.0&l=6.9&p=Y29tLmludGVuc2l2ZS5zb3VuZA==  
lisersrath[.]fun/x64?v=0.0&l=6.9&p=Y29tLmludGVuc2l2ZS5zb3VuZA==  
lisersrath[.]fun/arm?v=0.0&l=6.9&p=Y29tLmludGVuc2l2ZS5zb3VuZA==
```

那下载的到底是什么呢？以 `x86` 参数为例，下载得到一个json文件（`f7e8f0aec32ceb27d5e202d4b2b50812`），它的 `apk` 字段指向一个新的APK文件（`12098a59b35bcabb16bfeab887eb7f9f`）。

经分析，新的APK文件隶属于 `FakeAdsBlocker` 家族，是一个隐蔽的广告程序，本文编写时，它在VT的查杀率不高，4/64。

此外，我们还发现了另外一类URL：

```
lisersrath[.]fun:80/?cid=c423cdff-6c1b-4052-859f-11223c65f1ad&tid=827722&sid1=3182549
```

以访问上面的域名为例，会下载一个名为 `synapse_x_key` 的 APK（`a384b97af0f9432a71b27fa0cccd9667`），它和上文分析的样本是同源的，

本身是下载&加载器，主要功能是下载执行FakeAdsBlocker。

至此简单地逆向分析告一段落，这一批域名的传播目的也十分明了了，它们用于传播FakeAdsBlocker Downloader以及FakeAdsBlocker。

新特征

在人工查看URL的过程中，我们注意到了一个之前没有见过的现象，就是一串完全相同的URL，不同时间随机下载样本，每次样本文件的MD5值都不一样。

比如：

```
https[:]//lisersrath.fun/?cid=f0e87e37-1bc6-4073-af71-efcc4a3eca22&tid=792297&sid1=72
```

随机下载3次，文件名都是“Your File Is Ready To Download.apk”，但MD5值分别为：

```
ab2f4fde57fdcb56bce5ffa48c4d9069  
21c99e0a12a7ce9dc0d91df9e29af4ad  
1e55fde5540147fbfac1c8060c449c58
```

再次随机挑选了另一个域名试验，还是一样的现象。

```
https[:]//holidano.top/?cid=a53fd199-f207-49dc-b5d7-aea0de14eee3&tid=899546&sid1=4009
```

文件名“MobileVPN.apk”，MD5各不相同：

```
a3ad2ba6caf05275545d65cb2e8990d4  
f4316d300116fa9de72f6f0ed3d29c28  
56396eae0bbaf82701399d717ff3708
```

受此启发，我们提取了一条新特征，以新特征在数据库里搜索，找出历史上具备同一特征的数据，比如下图的URL：

随后，人工对所有符合条件的历史数据进行统计分析，以确定新特征对判黑动作的贡献值大小，最后决定是否合并到DNSMon系统里。可以说，特征的积累，对DNSMon这种海量数据分析挖掘系统来说是极其重要的，正是2014年至今的6年多时间里，系统沉淀了很多的规则，才有可能从每天千亿级别的DNS流量里提取出威胁情报(域名IOC)，并向最终用户提供安全防御。

结论

得益于DNS的基础性，DNSMon具备宽广的视野，能无差别的看见Linux，Windows和Android平台上发生的安全事件。而之所以具备这种能力，主要的原因是系统积累了大量的跟安全相关的特征规则。

读者请注意，不要轻易自行模仿文中的判黑过程。工业化的IoC生产不仅包括基本的判定过程，还有复杂的过滤、防止误报、反馈修正、失效保护和自动化过程。书写本文的目的是为了便于读者了解DNSMon工作的一般原理，但工业化过程中各种魔鬼细节的复杂程度，已经远非行文所能描述。

版权声明

本文为360Netlab原创，依据 [CC BY-SA 4.0](#) 许可证进行授权，转载请附上出处链接及本声明。

IoC

```
ereusingl[.]fun  
lisersrath[.]fun  
predition[.]fun  
ningspais[.]top  
ssuminat[.]top  
erefulp[.]top  
stirlinebea[.]top  
utionstro[.]top  
lesseased[.]top  
thinkdisen[.]top  
edcarefe[.]fun  
holidano[.]top  
ehousan[.]top  
swoulder[.]fun  
riemanufa[.]top  
ntrealing[.]fun
```

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

DNSMon



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

[See all 28 posts →](#)

DNSMon

DNSMon: using DNS data to produce threat intelligence (3)

Background This article is the third in our series of articles introducing DNSMon in the production of threat intelligence (Domain Name IoC). As a basic core protocol of the Internet, DNS protocol is one of the cornerstones for the normal operation of the Internet. DNSMon, which was born and raised



Feb 9,

7 min



2021

read

DDoS

New Threat: Matryosh Botnet Is Spreading

Background On January 25, 2021, 360 netlab BotMon system labeled a suspicious ELF file as Mirai, but the network traffic did not match Mirai's characteristics. This anomaly caught our attention, and after analysis, we determined that it was a new botnet that reused the Mirai framework, propagated through



Feb 2,

8 min



2021

read