

DNSMon

DNSMon: 用DNS数据进行威胁发现(2)



suqitian, Alex.Turing

Dec 31, 2020 • 14 min read

----**DNSMon抓李鬼记**

背景

本文是介绍DNSMon在生产威胁情报(域名IoC)系列文章的第二篇。

为了对抗安全人员的分析，钓鱼域名是恶意样本经常采用的一种技术手段。从字符组成和结构上看，钓鱼域名确实具有混淆视听的功效，但对于DNSMon这种具备多维度关联分析的系统来说，模仿知名公司域名的效果则适得其反，因为这样的域名一旦告警，反而更容易引起分析人员的注意。

本案例从一组疑似钓鱼域名出发，逐步介绍DNSMon是如何利用whois, ICP备案，域名解析内容和图关联等信息，让一组干瘪的域名逐渐一点点丰富起来直至最后恶意定性的。

意料之外的是，随着线索的展开，我们发现这是一起失陷设备数量巨大的安全事件，从我们的数据测算，感染规模远超100w设备。为此，我们进行了较为细致的逆向分析和回溯，但限于篇幅，样本分析细节及其家族演变，将在后续再另起一篇介绍。

通常威胁分析普遍的惯例是先知道样本恶意再逆向，有时根据DNS数据估算感染规模。这次DNSMon系列文章里揭示的，更多是先根据DNS数据发现异常并定性，再进一步探寻还原事件真相。即从先逆向再统计，变成了先统计再逆向。这个顺序的变动，是DNSMon的一小步，却是整个威胁分析分支的一大步。

DNSMon对未知威胁的预警

2020-11-17, DNSMon系统提示一组域名baidugif[.]com, qqjpeg[.]com, 163pics[.]com, 163image[.]com存在安全威胁, 打开一看, 域名的特殊构造立刻勾起了我们进一步细致查看的兴趣。

baidu + gif, qq + jpeg, 163 + pics, 163 + image, 看起来像是大厂提供图片服务的域名, 难道近期有什么新政策或者新业务, 导致几个大公司纷纷加开新的图片服务? 不过既然系统提示有安全威胁, 是李鬼的可能性更大。

就先从系统汇总的域名基础信息开始, 看看有哪些异常的内容。

第一步, 从系统提取whois注册信息。一般来讲, 合规运营的公司注册信息会规范且完整。

163pics.com	createddate	2020-11-12 12:26:17
163pics.com	updateddate	2020-11-12 12:26:17
163pics.com	expiresdate	2022-11-12 12:26:17
163pics.com	status	clientDeleteProhibited clientRenewProhibited
163image.com	createddate	2020-11-12 12:26:17
163image.com	updateddate	2020-11-12 12:26:17
163image.com	expiresdate	2022-11-12 12:26:17
163image.com	status	clientDeleteProhibited clientRenewProhibited
qqjpeg.com	createddate	2020-11-12 12:26:17
qqjpeg.com	updateddate	2020-11-12 12:26:17
qqjpeg.com	expiresdate	2022-11-12 12:26:17
qqjpeg.com	status	clientDeleteProhibited clientRenewProhibited
baidugif.com	createddate	2020-11-12 12:26:17
baidugif.com	updateddate	2020-11-12 12:26:17
baidugif.com	expiresdate	2022-11-12 12:26:17
baidugif.com	status	clientDeleteProhibited clientRenewProhibited

查询的结果显示, 4个域名的注册信息很一致, 注册时间甚至精确到同一秒完成, 而且都打开了隐私保护。鉴于百度, 腾讯和网易不会走上“分久必合, 合久必分”的历史路线, 因此不可能存在统一进行域名注册的操作。

李鬼的可能性+1。

第二步，从系统提取ICP备案信息。下面这段话是从域名备案管理系统的政策文件
《工业和信息化部关于规范互联网信息服务使用域名的通知》摘抄的：

...进一步规范互联网信息服务域名使用，现就有关事项通知如下：

一、互联网信息服务提供者从事互联网信息服务使用的域名应为其依法依规注册所有。

...

也就是说，在国内合规运营的公司一般都要进行域名备案以正常开展业务，而这4个域名的查询结果是“未备案或备案取消”。

李鬼的可能性+2。

第三步，从系统提取域名的DNS解析信息。

2020-11-13 18:18:56	baidugif.com	A	47.100.164.28	37963 Hangzhou_Alibaba
2020-11-13 18:19:04	qqjpeg.com	A	47.116.142.94	37963 Hangzhou_Alibaba
2020-11-13 18:18:50	163pics.com	A	39.98.228.46	37963 Hangzhou_Alibaba
2020-11-13 17:00:22	163image.com	A	39.98.228.46	37963 Hangzhou_Alibaba

4个域名的活跃时间一致，解析结果看起来还算正常，没有指向同一个IP，但ASN都同属37963阿里云，显然是同一组织或个人所为。

此外，当我们观察这个四个域名的流量曲线，注意到这4个域名活动行为几乎一致。

李鬼的可能性+3。

到这里，这一组域名已经可以标记为99%级别可靠的恶意域名了，但是要将其标注为99.99%可靠的域名的话，我们还需要更多的交叉数据比对。

关联

从DNSMon提取的基础信息显示，这组域名就是李鬼无疑了。但系统的安全威胁告警，并不是仅仅依赖这些基础信息做决策得出的，而是借助了更多的数据展开关联分析得出的结论。

关联分析根源于最朴素的想法：“近朱者赤近墨者黑”，和坏蛋打交道大概率不是好人，马老板的朋友圈多数是能人异士。

以4个域名做为种子，从我们的数据得到了下面的关联图：



对于关联图，一方面，是利用其中的样本信息对4个域名进行定性，就是回答域名具体用途是什么，钓鱼？Downloader还是C&C？

分析之后，可以看出系统预警的原因是因为：关联出来的样本，能在VT查询到结果的，比如e64ac44596e1c66036ca3e58c28c24a6，已经被众多杀毒引擎标注有问题；未能在VT查到结果的，比如b4070c64ae268e9edf383b6096a68fc3，图系统也

有偏黑的属性标签。而和4个种子域名关联最紧密的 b4070c64ae268e9edf383b6096a68fc3 是一个DLL文件，都以TCP: 2653和4个域名进行了通信，看起来域名的用途大概率是C&C。

另一方面，关联图可以弥补遗漏的信息。

其中，最有意思的是关联出的一个域名“xia.doubeidong[.]com”，在其上承载着一个 URL “http[:]//xia.doubiedong.com:45678/”，后台服务是国内黑客的最爱HFS。根据页面信息显示，在服务器提供服务的16个小时里，已经有超过**700**万次的下载。

Name .extension	Size	Timestamp	Hits
45678.txt	469B	2020/11/17 10:03:20	7450557

弥补信息的另一个有趣点在URL。

```
http[:]//wx1.sinaimg.cn/large/0082blolly1gkh5uqz322g300g00g7jv.gif MD5: c3a7d82f3943  
http[:]//tiebapic.baidu.com/tieba/pic/item/e1fe9925bc315c6070d21eae9ab1cb134954772f..
```

打开这两个URL，页面显示的是一个很小很模糊的顺时针转动箭头，但是另存为文件后，文件大小却接近571KB，明显是在玩假图片的路数。

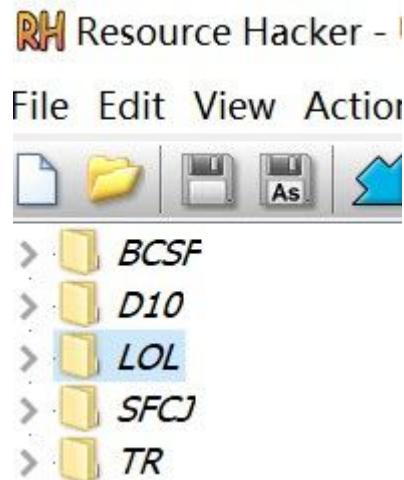
至此，利用DNSMon系统，我们从数据层面对这4个域名有了“恶意”的定性。但要解释样本和域名之间的关系，还是要进行简要地逆向分析。

逆向定性

经分析，baidugif[.]com, qqjpeg[.]com, 163pics[.]com, 163image[.]com的用途确实是C&C，而xia.doubiedong[.]com则和挖矿有关。

样本1分析：b4070c64ae268e9edf383b6096a68fc3

样本b4070c64ae268e9edf383b6096a68fc3，是一个加载器，主要功能是加载运行内嵌在PE资源里的5个恶意的文件。



其中名为 **LOL** 的资源与本案例相关的，因此本文只聚焦LOL文件。

Dump出LOL的MD5为a20a9e26865291aa651242abcf8a958c，它包含了5个域名，比我们从数据观测的角度多一个。

```
qqjpegs.com  
163pics.com  
163image.com  
baidugif.com  
baidupics.com
```

LOL运行时会向C&C发送加密的长度10字节的上线信息，以下明文为例

```
6c 36 04 00 00 ff 02 ff 02 ff
```

加密算法RC4, KEY 10字节,

```
0C 22 38 4E 5A 0C 22 38 4E 5A
```

加密后得到BOT向C&C发送的密文

```
6f 50 4f 3a 7b 94 b2 8e ec e6
```

当C&C收到BOT的请求后，向BOT回发的加密的信息

```
ba 0a 43 19 eb 61 9b 1a d3 0c 74 5e d5 c1 ae 59 a0 cf 52 d7 15 35 9b c1 61 07 20 16 9
```

解密算法RC4, KEY 10字节

```
0C 22 38 4E 5A 0C 22 38 4E 5B
```

解密后得到以下URL，可以看出，它们和前文所述"玩假图片的路数的URL"的模式是一样的。

```
https[:]//imglf3.nosdn.127.net/img/T0]id3A3NGx6NGYwR1RURm53bXUvVnBSMnp4Kyt6NW1rUi9lN2  
https[:]//imglf6.nosdn.127.net/img/T0]id3A3NGx6NGYwR1RURm53bXUvWXYvd1U3QUt6SXUrNctvK2  
http[:]//tiebapic.baidu.com/tieba/pic/item/cffc1e178a82b901bc520176648da9773812effd.  
http[:]//tiebapic.baidu.com/tieba/pic/item/cffc1e178a82b901bc520176648da9773812effd.
```

http[:]/wx3.sinainmg.cn/large/008elXdrly1glzkcp1nndg300g00gqht.gif
http[:]/wx2.sinainmg.cn/large/008elXdrly1glzkclznjtg300g00gqht.gif

那图片到底是什么呢？以上面URL对应的图片

(MD5:6f978ff7382f89d613647283850d4a38) 为例，经发析，发现它是一个使用RC4加密，zlib压缩的文件，解密解压后得到下面的最终的业务PE文件

(MD5:dd8a3e4e5c84ffb9ec8b845ac687d647)，验证了我们最初的判断，“假图片”。

至此b4070c64ae268e9edf383b6096a68fc3与4个李鬼域名，以及“玩假图片的路数”URL都关联起来了。

样本2分析：d8380bf0739384d82aaadc4d36f3abee

样本d8380bf0739384d82aaadc4d36f3abee访问URL下载到的45678.txt文件是一串被加密过的数据：

A5CA21A8E6A3DCC0E2B1AE786464602A3F3F7E7F64753E697F6574717F3E737F7D3F6967633F7160793F6

这串数据解密后得到有道云笔记的一个URL：

http[:]/note.youdao.com/yws/api/personal/file/WEBcb63181389a6c37631e5b8c769969d6c?me

上述URL下载得到的是一个EXE文件，名为n1.exe或n2.exe：

731c9d6e7c77e4f507de16ba8146779b n1_exe_youdao
b1fd035f4aab2cd1e56e25e94dd99f3 n2_exe_youdao

该文件本质是一个RAR自解压文件：

其中的 audiodg.exe 或 lsmm.exe 文件，是易语言编写的一个 EXE 文件。它在运行过程中会对自身内嵌的PE进行部分数据的替换与组合，并释放出以下两个文件：

1. servicesXX.exe(XX为2个随机字符)
2. delziji123.txt(存放自身的文件路径，后续会根据这个路径将自身删除)
servicesXX.exe 文件中包含另一条有道云笔记的URL:

```
http[://]//note.youdao.com/yws/api/personal/file/WEB7d6e44695d1d0f3e1c0cd07fb4d60643?me
```

访问该URL下载到hx1.exe文件，该文件即为矿机程序。

感染分布

从实际的感染分布来看，中国大陆地区的31个省市均有感染。

溯源分析

在查看数据的过程中，我们也一直在想，究竟样本是经过什么途径到达了感染的目标？经过溯源，我们还原了感染的路径，如下图。

是一个叫NBMSClient的工具一系列的父子进程创建，最终加载了一个名为uwspvps.dll的动态链接库，访问了引起我们注意的4个域名。

通过搜索引擎搜索“NBMSClient”，结果显示是一个网吧相关的运维工具。可以猜测，随着样本被维护通道的不断下发推广，域名和其他诸多线索逐渐汇集到了DNSMon，从而触发了此次预警。

结论：

- 得益于DNS的基础性，DNSMon具备及时发现不同行业安全威胁的能力，尤其在现有安全软件无检出，或者是用户没有使用安全安全软件的场景下，这种新维度可以和现有安全产品组成有效的交叉火力。
- 网吧运维工具由于安装范围广，应该具备较为专业的安全能力为维护通道保驾护航，防止下发通道被恶意利用。
- 为躲避各类安全产品的检测，恶意样本的传播借助了大公司的基础服务，比如本次事件用到了wx1.sinaimg[.]cn，tiebapic.baidu[.]com和note.youdao[.]com提供的图片下载服务。

loc

域名：
baidugif.com
qqjpegs.com
163pics.com
163image.com
xia.doubiedong.com
baidupics.com



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 —

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

DGA

Necro在频繁升级，新版本开始使用PyInstaller和DGA

概述 Necro是一个经典的Python编写的botnet家族，最早发现于2015年，早期针对Windows系统，常被报为Python.IRCBot，作者自己则称之为N3Cr0m0rPh(Necromorph)。自2021年1月1号起，360Netlab的BotMon系统持续检测到该家族的新变种，先后有3个版本的样本被检测到，它们均针对Linux系统，并且最...

0-day

Another LILIN DVR 0-day being used to spread Mirai

Author: Yanlong Ma, Genshen Ye Background Information In March, we reported[1] that multiple botnets, including Chalubo, Fbot, Moobot were using a same 0 day vulnerability to attack LILIN DVR devices, the vendor soon fixed the vulnerability. On August 26, 2020, our Anglerfish honeypot detected that another new LILIN DVR/

See all 28 posts →



• Jan 21, 2021 • 16 min read



• Dec 3, 2020 • 5 min read