

0-day

那些年我们一起追过的僵尸网络之Moobot

Moobot是一个基于mirai开发的僵尸网络,样本通过Telnet弱口令和利用nday,0day漏洞传播

**Hui Wang, Alex.Turing**

Jul 9, 2020 · 6 min read

概述

Moobot是一个基于Mirai开发的僵尸网络，我们最早发现其活动在2019年7月，这里有一篇我们关于Moobot的文章，感兴趣的读者可以去阅读[\[o\]](#)。2019年8月起我们开始对其进行跟踪，在这将近一年的时间其样本更新、DDoS攻击等活动从未间断过。其最近参加了一次我们不方便透露的重大DDoS攻击活动，又一次成功引起了我们的注意。所以决定来扒一扒它的前世今生。

样本传播

Moobot样本主要通过Telnet弱口令和利用nday,0day[\[1\]](#)[\[2\]](#)漏洞传播，我们观察到的Moobot利用的漏洞如下：

VULNERABILITY	AFFECTED AEVICE
HiSilicon DVR/NVR Backdoor	Firmware for Xiaongmai-based DVR
CVE-2020-8515	DrayTek Vigor router
JAWS Webserver unauthenticated shell command execution	MVPower DVR
LILIN DVR	LILIN DVRs

VULNERABILITY	AFFECTED DEVICE
GPON Router RCE	Netlink GPON Router 1.0.11
TWT OEM API RCE	TWT Digital Technology Co. Ltd & OI
ThinkPHP 5.0.23/5.1.31 RCE	
Android Debug Bridge Remote Payload Execution	
AVTECH Devices Multiple Vulnerabilities	AVTECH IP Camera / NVR / DVR Dev
CVE-2017-17215	Huawei Router HG532
Netcore Router Udp 53413 Backdoor	Netcore Router
CVE-2014-8361	Devices using the Realtek SDK
CVE 2020 5722	Grandstream UCM6202
CVE-2017-8225	The Wireless IP Camera (P2P) WIFI
DVRIP backdoor	

样本分析

在之前的文章中介绍了Moobot的诸多变种，我们认为其作者相较于简单的改改C2，更倾向开发使用新的技术。Moobot的作者在样本二进制层面&网络流量层面做了许多尝试，一般样本都会采用下述方法中的多种组合，来和安全研究人员进行对抗。

- 使用DNS TXT存储C2/手动构建DNS TXT请求
- 使用新的UPX幻数进行加壳
- 使用码表替换的加密方法的隐藏敏感资源
- 使用SOCKS PROXY, TOR PROXY

但是在2020年1月起活跃至今的名为Moobot_xor的变种中，情况出现了变化。Moobot_xor是Moobot大家族中少见的只是修改了上线协议的变种，或许是因为Moobot的作者在长达1年的运营中，发现只需要做这样简单的修改，再加上不停的更换C2，就能达到非常好的收益，没必要再投入新技术的研究了。

样本信息

```
MD5:98c8326b28163fdaeeb0b056f940ed72
ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Packer:None
Lib:uclibc
Verdict: Moobot_xor
```

Mirai已经是安全社区非常熟悉的老朋友了,而Moobot_xor与Mirai很接近,因此下文只从加密方法以及通信协议俩个方面介绍Moobot_xor,别的方面就不再细述。了解加密方法可以提取bot的配制信息,了解通信协议可以跟踪C2以获取最新的攻击指令,希望这些内容能帮助社区更好的打击Moobot家族。

加密方法

Moobot_xor采用Mirai经典的Xor加解密方法, key为 0DEADBEEFh ,

```
v1 = &dword_80517E0[2 * a1];
result = dword_80516FC;
if ( *((WORD *)v1 + 2) )
{
    v3 = dword_80516FC;
    v4 = 0;
    v5 = (unsigned int)dword_80516FC >> 8;
    v8 = HIBYTE(dword_80516FC);
    v6 = (unsigned int)dword_80516FC >> 16;
    do
    {
        *_BYTE(*v1 + v4) ^= v3;
        *_BYTE(*v1 + v4) ^= v5;
        *_BYTE(*v1 + v4) ^= v6;
        v7 = v4++;
        *_BYTE(*v1 + v7) ^= v8;
        result = v1[1] & 0xFFFF;
    }
    while ( result > v4 );
}
return result;
```

通信协议

Mobot_xor在Mirai通信协议的基础上做了微小的修改，下文将从上线，心跳，功击指令等方面介绍其具体的变化。

- 上线包

```
00000000 33 66 99 06 67 6c 61 69 76 65 3f..glai ve
```

```
msg parsing
```

```
-----  
33 66 99 -----> hardcoded magic  
06 -----> group string length  
67 6c 61 69 76 65 -----> group string, here it is "glaive"
```

- 心跳包

```
0000000C 00 00 ..  
00000002 00 00 ..
```

```
msg parsing
```

```
-----  
00 00 -----> hardcoded msg from bot  
00 00 -----> hardcoded msg from c2
```

- 攻击指令包

```
00000000: 00 00 00 3C 01 01 77 A7 B5 CB 20 02 00 02 32 30 ...<...w... ...20  
00000010: 07 02 38 30 ..80
```

```
msg parsing
```

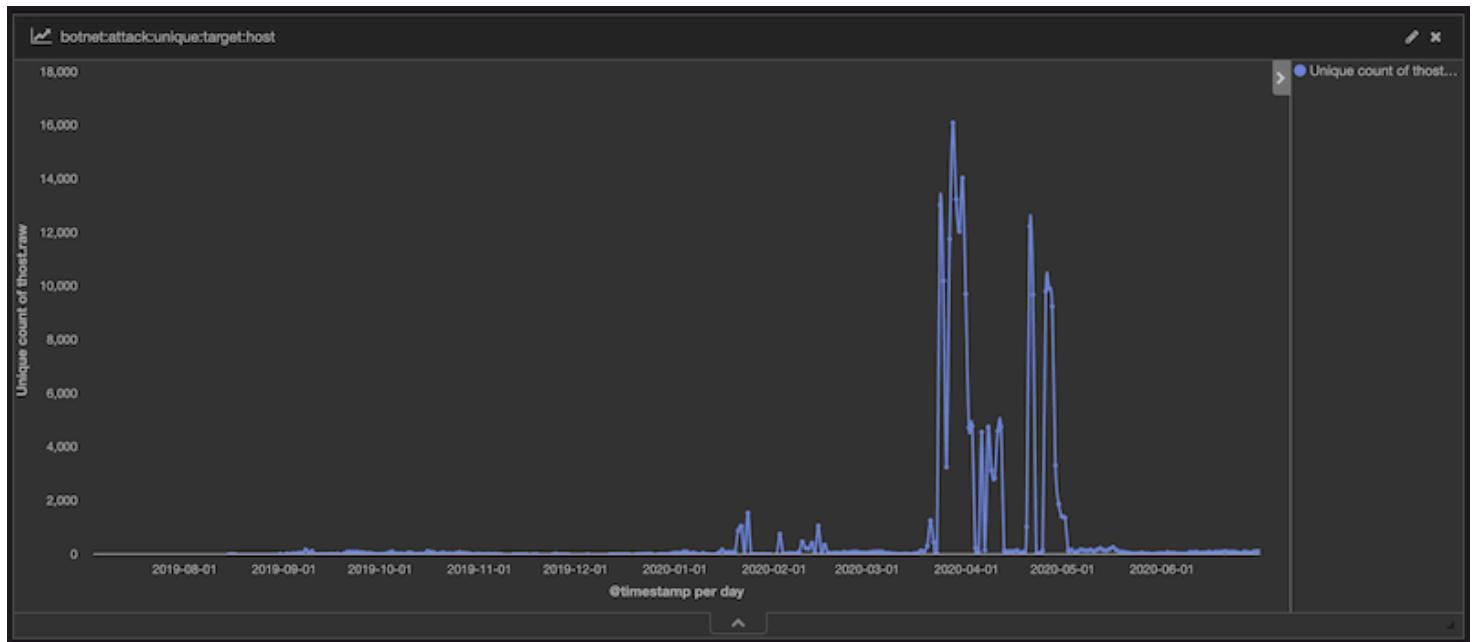
```
-----  
similar to mirai  
  
01 -----> number of targets  
  
77 a7 B5 CB 20 -----> target/mask, 119.167.181.203/32  
  
02 -----> number of flags  
  
00 -----> flag type  
02 -----> flag length  
32 30 -----> flag data  
  
07 -----> flag type  
02 -----> flag length  
38 30 -----> flag data
```

Moobot DDoS活动

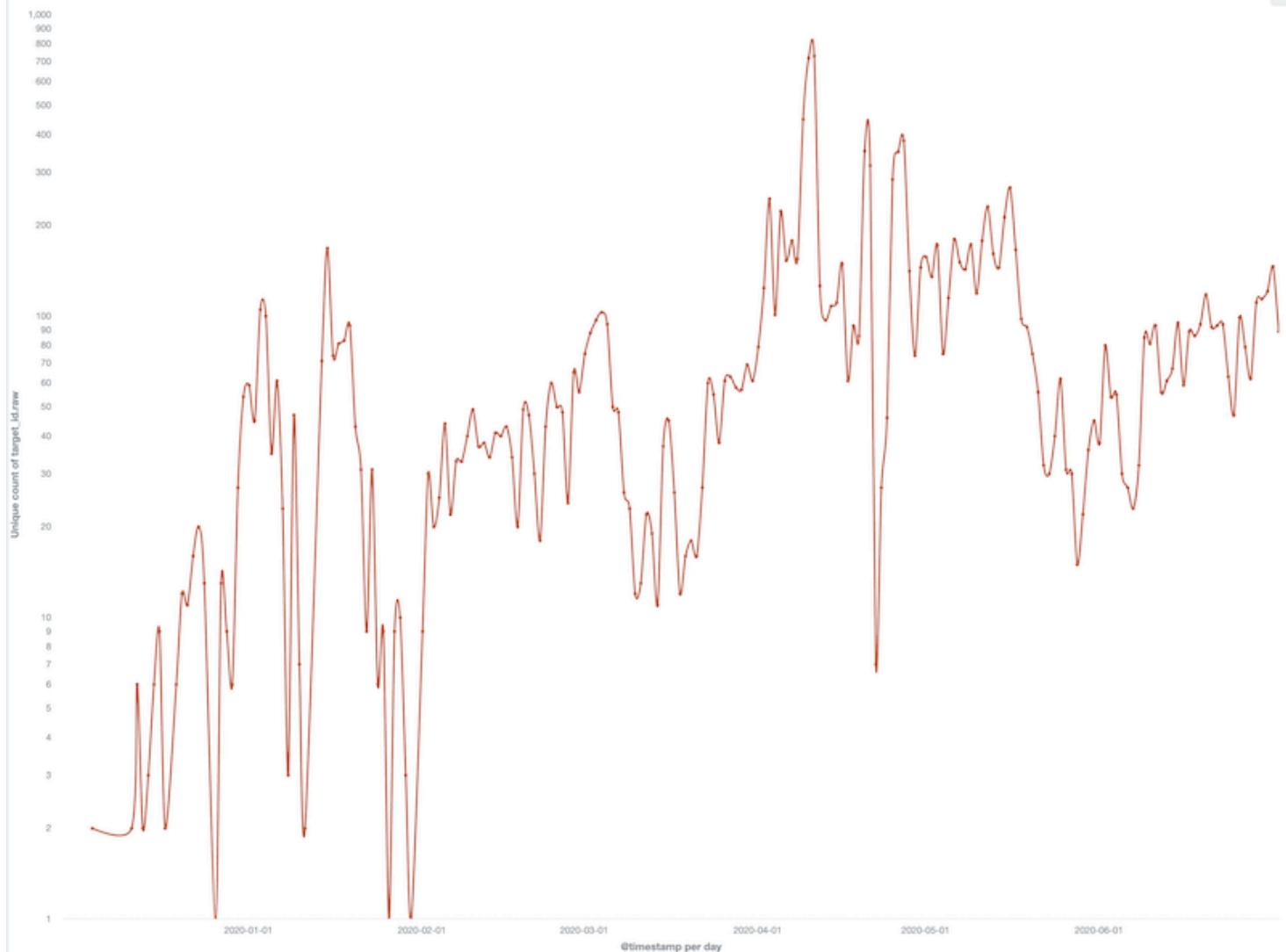
自从我们开始跟踪Moobot，其攻击活动从未停止过。根据我们的观察，其日活C2始终保持个位数，但是C2存活时间较长。攻击目标遍布全球，每日攻击目标100个左右。

Moobot的攻击目标

Moobot的每日攻击目标趋势如下图所示：

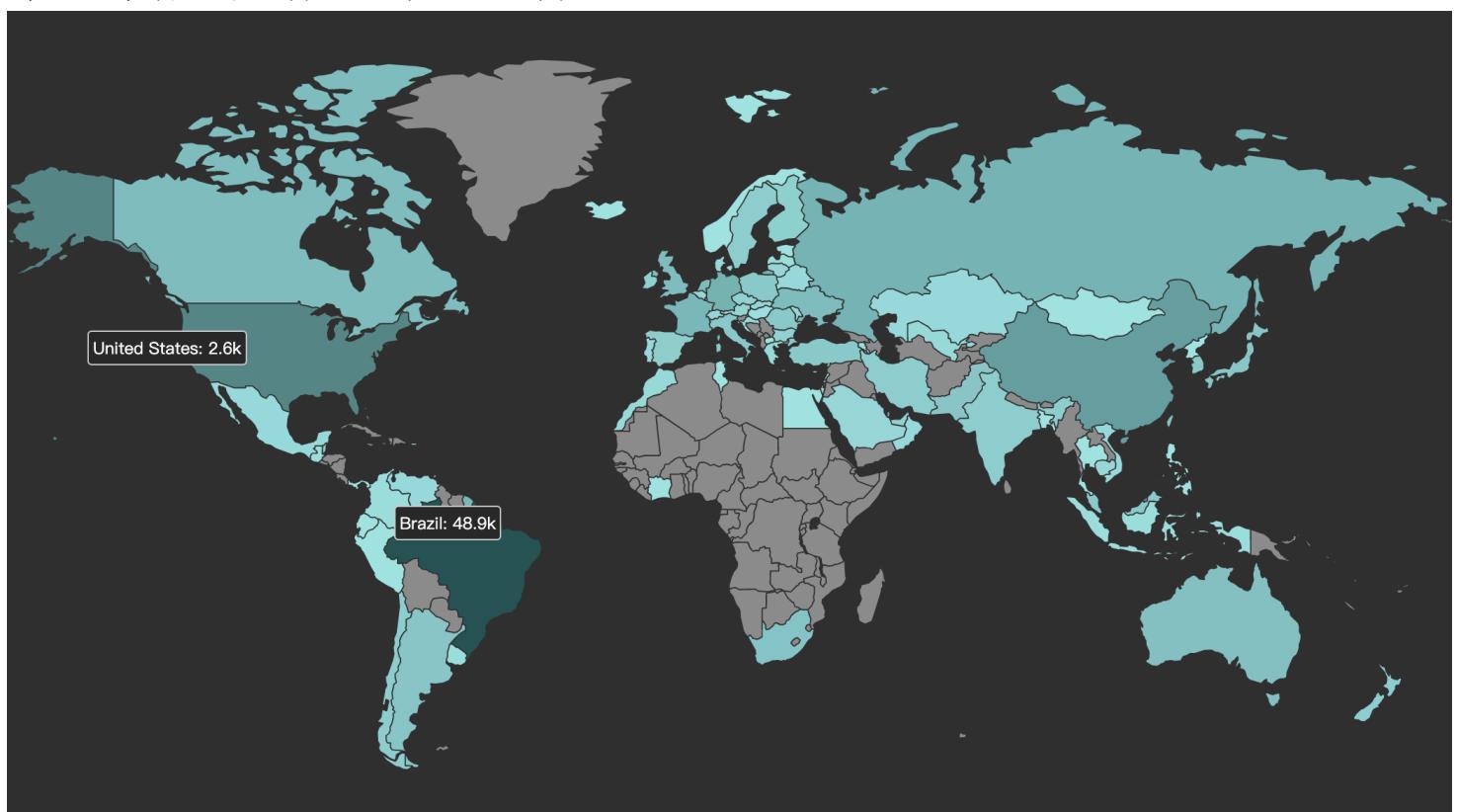


从上图可以看出Moobot的DDoS攻击活动在2020年3月末至2020年5月初出现明显的异常点，Moobot的日攻击目标从平常的几百暴增到将近2万。经过分析我们发现Moobot攻击目标暴增是因为在这段期间Moobot攻击了大约48k左右的巴西的IP。我们不清楚Moobot盯着巴西往死里打打奇怪攻击行为的目的是什么。去除地理位置在巴西的攻击目标。Moobot的日活攻击目标如下，每天100左右的攻击目标：



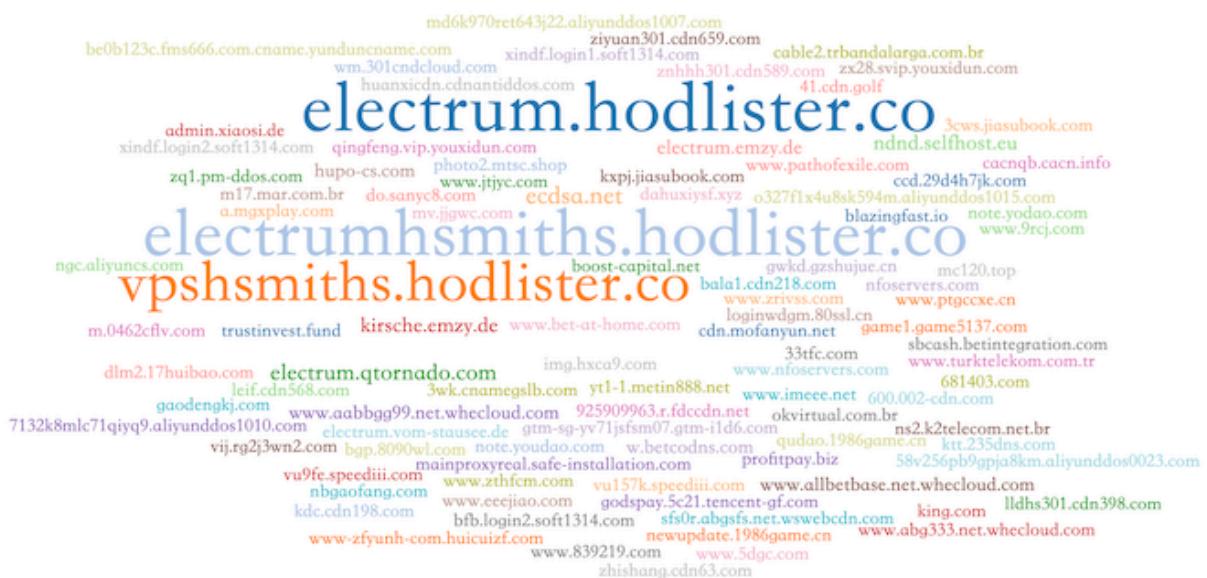
Moobot攻击目标地理位置分布

Moobot的攻击目标遍布全球，被攻击的目标主要分布在中国，美国，德国，俄罗斯等地。其攻击目标地理位置分布如下：



Moobot攻击受影响的域名

通过我们的PDNS数据反查被Moobot攻击的IP，发现至少3k以上的域名被影响，之前我们也观察到Moobot[攻击了很多流行站点/重要服务](#)。包括DNS ROOT, Twitter, Facebook, Pornhub, [Wikimedia](#), [Twitch](#), [World of Warcraft Server](#), Google, Baidu, Alibaba, Krebs on Security等。当时据一名为[UKDrillas](#)的黑客或客户组织称攻击这些流行站点的目的是为了测试该Botnet的攻击效果。部分Moobot攻击目标对应的域名如下图所示：



IOC

C2

190.115.18.238	AS262254 DANCOM_LTD	Russian_Federation Mo
31.13.195.56	AS34224 Neterra_Ltd.	Bulgaria Sofia Unknow
37.49.226.216	AS208666 Estro_Web_Services_Private_Limited	Netherlands Overijsse
45.95.168.90	AS42864 Giganet_Internet_Szolgaltato_Kft	Hungary Szabolcs-Sza
abcdefg.elrooted.com		
audi.n1gger.com		
botnetisharam.com		
cykablyat.raiseyourdongers.pw		
dbkjgueuvmf5hh7z.onion		
frsaxhta.elrooted.com		
gcc.cyberium.cc		

n1gger.com
nd3rwzs1qhxibkl7.onion
nlocalhost.wordtheminer.com
park.cyberium.cc
park.elrooted.com
proxy.2u0apcm6ylhdy7s.com
rr442myy7yz4.osrq.xyz
sisuugde7gzpef2d.onion
typicalniggerdayatthecoolaidparty.n1gger.com
wor.wordtheminer.com
zrqq.xyz
tbpsboy.com

0 Comments

1 Login ▾

G

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 —

0-day

0-day

An Update for a Very Active DDoS Botnet: Moobot

Import 2022-11-30 11:16

The Gafgyt variant vbot seen in its 31 campaigns



EwDoor僵尸网络，正在攻击美国AT&T用户

EwDoor Botnet Is Attacking AT&T Customers

一个藏在我们身边的巨型僵尸网络 Pink

[See all 22 posts →](#)

Moobot is a mirai based botnet. Spread through weak telnet passwords and some nday and 0day vulnerabilities.



Jul 9,
2020 · 5 min
read

Overview Gafgyt botnets have a long history of infecting Linux devices to launch DDoS attacks. While dozens of variants have been detected, new variants are constantly emerging with changes in terms of register message, exploits, and attacking methods. On the other hand, their new botnets are usually short lived, with



Jul 6, 2020 · 7 min read