An Update for a Very Active DDos Botnet: Moobot

blog.netlab.360.com/ddos-botnet-moobot-en/

Hui Wang July 9, 2020

9 July 2020 / 0-day

Overview

Moobot is a Mirai based botnet. We first discovered its activity in July 2019. Here is our log about it[0]. And ever since then, its sample updates, DDoS attacks and other activities have never stopped.Recently we saw it participated in some very high profile DDoS attacks, we got asked quite a few times in the security community regarding to what botnet is behind the attacks, so here is some more details.

Sample dissemination

Moobot samples are mainly spread through weak telnet passwords and some nday and 0day [1][2]vulnerabilities. The vulnerabilities we observed using Moobot are as follows:

Vulnerability	Affected Aevice
HiSilicon DVR/NVR Backdoor	Firmware for Xiaongmai-based DVRs, NVRs and IP cameras
CVE-2020-8515	DrayTek Vigor router
JAWS Webserver unauthenticated shell command execution	MVPower DVR
LILIN DVR	LILIN DVRs
GPON Router RCE	Netlink GPON Router 1.0.11
TVT OEM API RCE	TVT Digital Technology Co. Ltd & OEM {DVR/NVR/IPC} API RCE
ThinkPHP 5.0.23/5.1.31 RCE	
Android Debug Bridge Remote Payload Execution	
AVTECH Devices Multiple Vulnerabilities	AVTECH IP Camera / NVR / DVR Devices
CVE-2017-17215	Huawei Router HG532
Netcore Router Udp 53413 Backdoor	Netcore Router

Vulnerability	Affected Aevice
CVE-2014-8361	Devices using the Realtek SDK
CVE_2020_5722	Grandstream UCM6202
CVE-2017-8225	The Wireless IP Camera (P2P) WIFICAM
DVRIP backdoor	

Sample analysis

In the previous article, we introduced many variants of Moobot. We believe that its author is more inclined to develop and use new methods than to simply change C2. The authors of Moobot had made many attempts at the sample binary level & network traffic level. Generally, samples used multiple combinations of the following methods to make job difficult for security researchers.

- Use DNS TXT to carry C2/ manually construct DNS TXT request
- Packing with the new UPX magic number
- Hidden sensitive resources using encryption method of code table replacement
- Use SOCKS PROXY, TOR PROXY

Since Jan 2020, another variant we called Moobot_xor became active. Moobot_xor doesn't adopt mothods metioned above,but just only modified the register message?). Maybe the author of Moobot has found that only one such simple modification and the constant replacement of C2 is needed to achieve very good benefits during the operation for up to 1 year, there is no need to invest in new technology research.

Sample information

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

Moobot_xor is very close to Mirai, so we are not going to cover things folks already knew. We will only introduce Moobot_xor’s encryption method and the communication protocol, understanding the encryption method will help extract the bot's configuration information, knowing the communication protocol should facility tracking C2 to obtain the attack instructions, we hope that these contents can help the community to better fight the Moobot family.

Encryption method

Moobot_xor uses Mirai's classic Xor encryption and decryption method, the key is `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;
```

Communication protocol

Moobot_xor has made some minor modifications on the basis of the Mirai communication protocol. Let's look at a few of them here.

Registration packet

```
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"
```

Heartbeat packet

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

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

Attack command

```
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
```

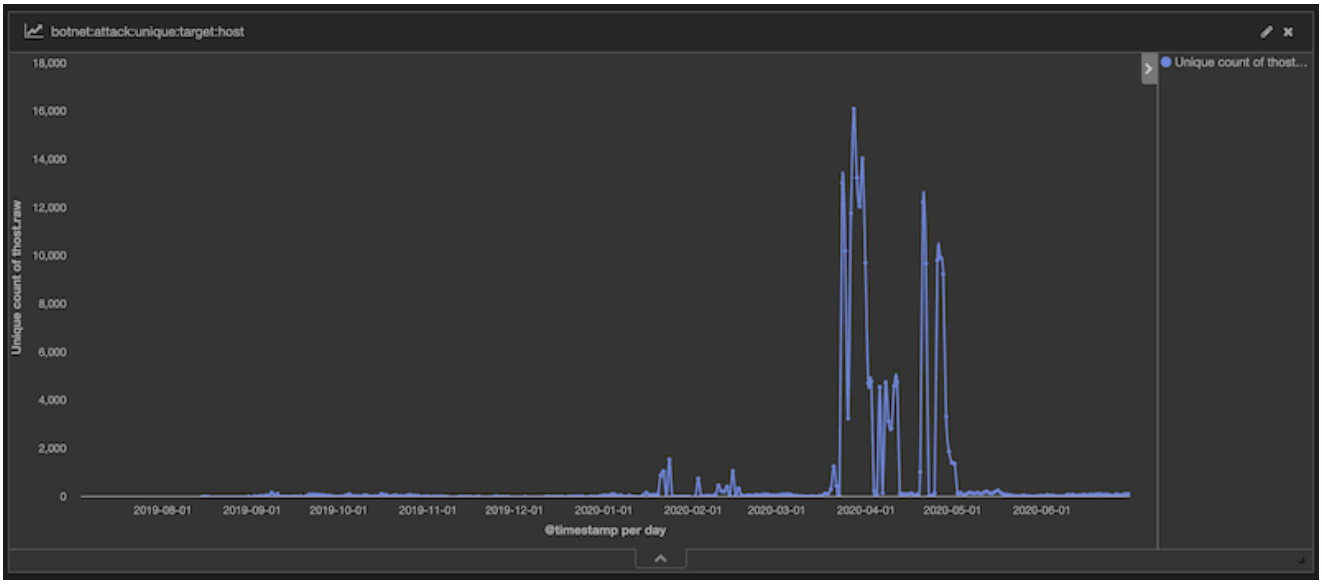
```
msg parsing
----------------------------------------------------------------
similar to Mirai

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 activity

Since we started tracking Moobot, its attack activity has never stopped. There are only a handful of C2s, but attack targets are all over the world, with about 100 targets per day.

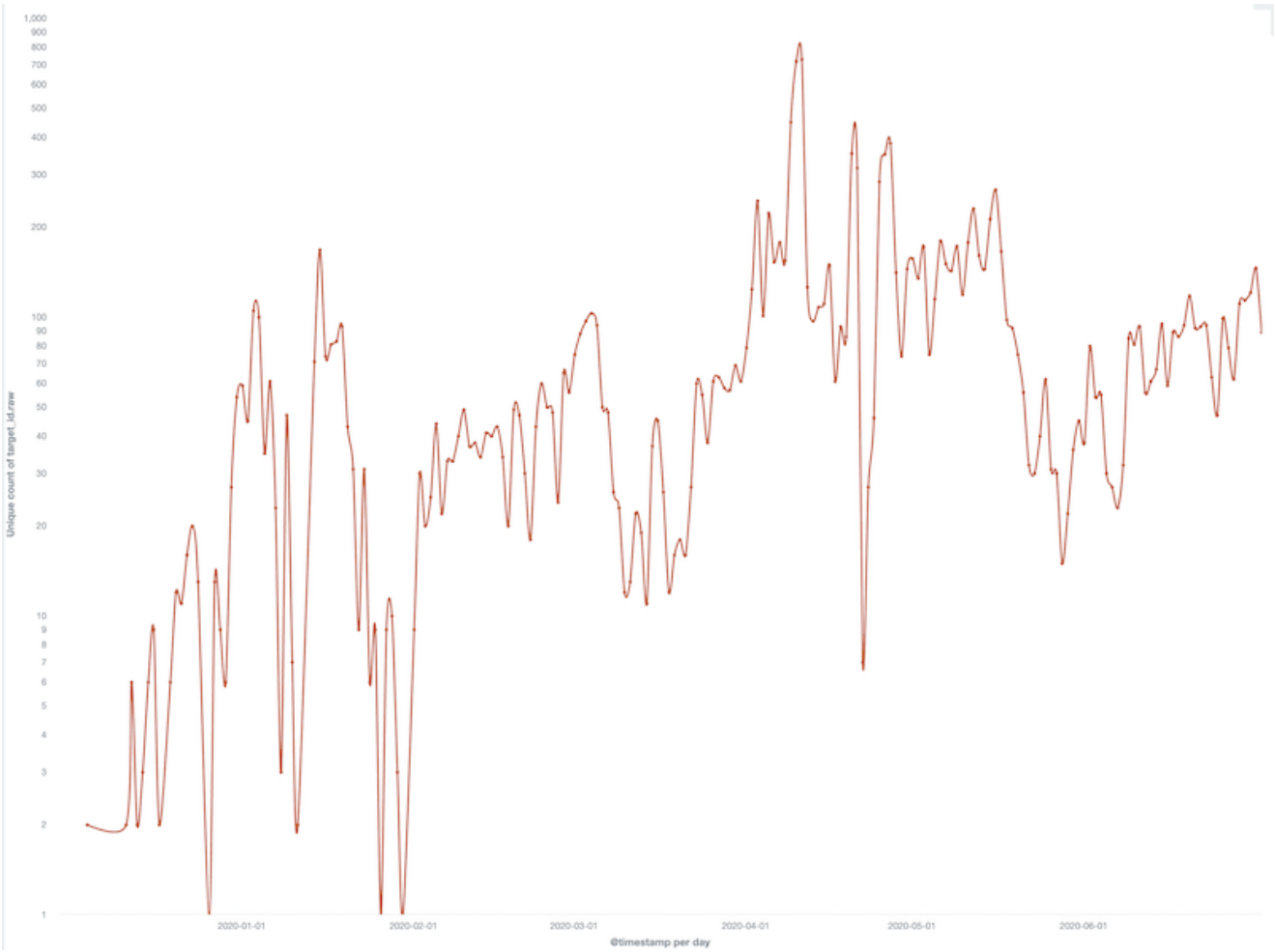
Moobot's target

The trend of Moobot's daily attack targets is shown in the figure below: :



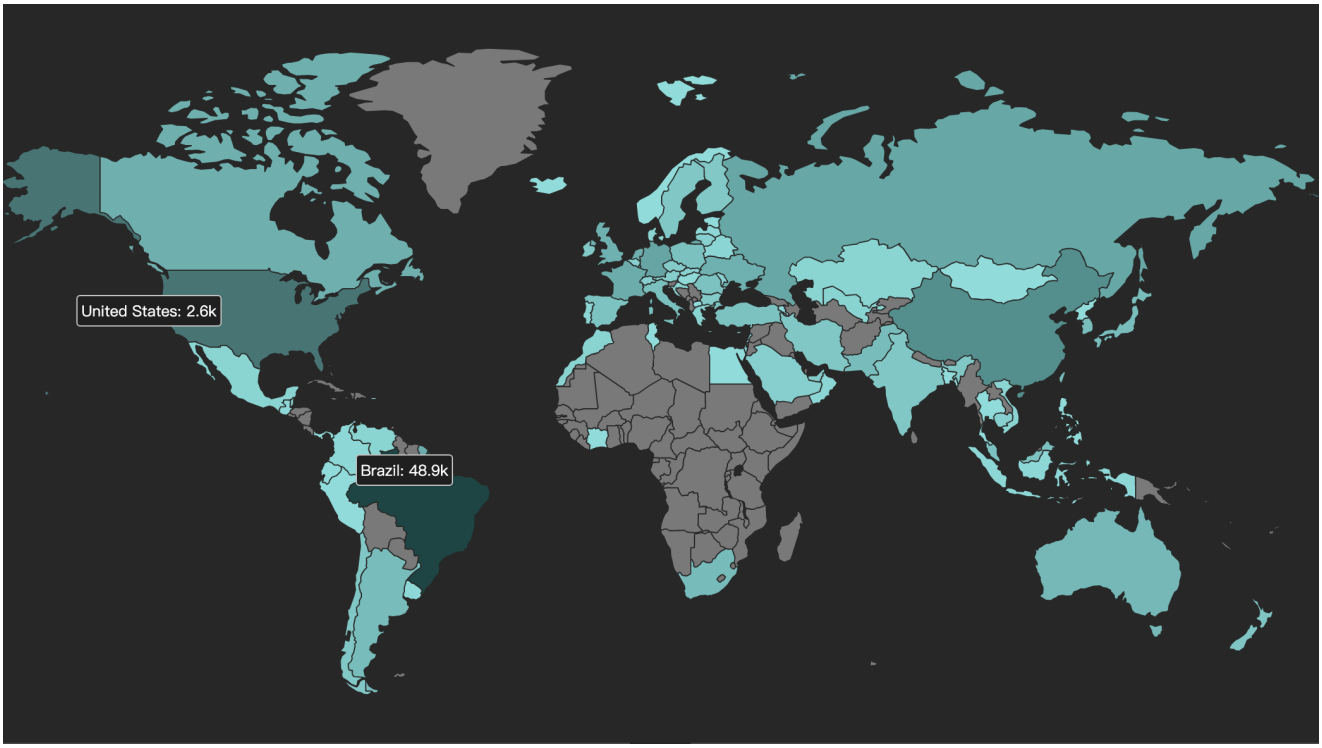
It can be seen from the above figure that Moobot's DDoS attack activity has obvious anomalies from the end of March 2020 to the beginning of May 2020, and the daily attack target of Moobot has increased from a few hundred to nearly 20,000. When we took a close look, we found that Moobot's attack target surged because Moobot attacked about 48k of Brazilian IP during this period. We don’t know what was reason behind that. After taking

Brazil our from the attack targets. Moobot's daily live attack targets are as follows, about 100 attack targets per day:



Moobot attack target geographic location distribution

Moobot's attack targets are all over the world.The geographical distribution of its attack targets is as follows:



Moobot attacks the affected domain name

We were able to confirm that Moobot has been behind some very high profile DDos attacks.We cannot disclose more detail here, but we had a tag cloud in our prior blog here[3].

Contact us

Readers are always welcomed to reach us on Twitter, WeChat 360Netlab or email to netlab at 360 dot cn.

IOC

C2

190.115.18.238 AS262254|DANCOM_LTD
Russian_Federation|Moscow|Unknown
31.13.195.56   AS34224|Neterra_Ltd.
Bulgaria|Sofia|Unknown
37.49.226.216   AS208666|Estro_Web_Services_Private_Limited
Netherlands|Overijssel|Enschede
45.95.168.90   AS42864|Giganet_Internet_Szolgaltato_Kft   Hungary|Szabolcs-
Szatmar-Bereg_County|Nyiregyhaza
abcdefg.elrooted.com
audi.n1gger.com
botnetisharam.com
cykablyat.raiseyourdongers.pw
dbkjbueuvmf5hh7z.onion
frsaxhta.elrooted.com
gcc.cyberium.cc
n1gger.com
nd3rwzslqhxibkl7.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