IoT_reaper: A Rappid Spreading New IoT Botnet

blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

Genshen Ye October 20, 2017

20 October 2017 / IoT Botnet
On 2017-09-13 at 01:02:13, we caught a new malicious sample targeting IoT devices. Starting from that time, this new IoT botnet family continued to update and began to harvest vulnerable iot devices in a rapid pace.

The bot borrowed some code from the famous mirai botnet, but it does not do any password crack all. Instead, it purely focuses on exploiting IoT device vulnerabilities. So, we name it **IoT_reaper**.

IoT_reaper is fairly large now and is actively expanding. For example, there are multiple C2s we are tracking, the most recently data (October 19) from just one C2 shows the number of unique active bot IP address is more than 10k per day. While at the same time, there are millions of potential vulnerable device IPs being queued into the c2 system waiting to be processed by an automatic loader that injects malicious code to the devices to expand the size of the botnet.

Currently, this botnet is still in its early stages of expansion. But the author is actively modifying the code, which deserves our vigilance.

Here we are sharing some quick summary so the security community may stop its before it causes bigger damage.

From Mirai, Beyond Mirai

The botnet partially borrows some mirai source code, but is significantly different from mirai in several key behaviors, including:

- No longer crack any weak password, only exploit IoT devices vulnerabilities;
- A LUA execution environment integrated, so more complex attacks can be supported and carried out;
- Scan behavior is not very aggressive, so it can stay under the radar.

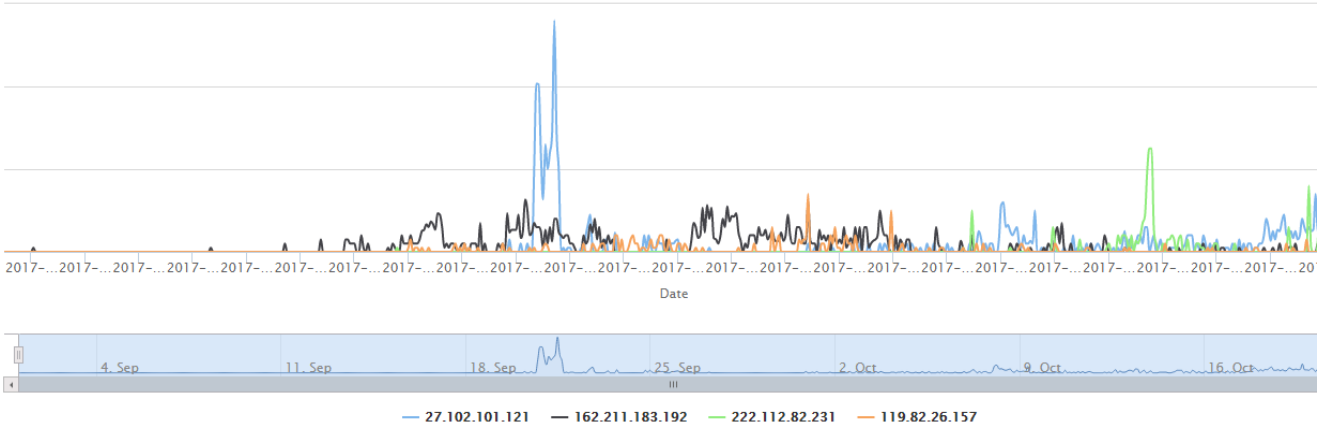
Sample Delivery, C2 Distribution and Traffic Pattern

Take hxxp://162.211.183.192/sa as an example, **IoT_reaper**'s sample delivery and C2 distribution are as follows. There is a `downloader`, quite different from Mirai:

- **downloader**: 162.211.183.192, samples can be downloaded from this server and it usually uses "d" as subdomain, like d.hl852.com

- **controller**: 27.102.101.121, which can control bots, send commands and usually uses "e" as subdomain, like e.hl852.com
- **reporter**: 222.112.82.231, which is used to receive potentially vulnerable device info collected by bots, it usually uses "f" as subdomain, like f.hl852.com.
- **loader**: 119.82.26.157, implants bot program through vulnerabilities into devices collected by reporter

The following figures shows traffic pattern of the above 4 IPs：



9 IoT Vulnerability Exploits Integrated in the Malware

Unlike Mirai that uses weak password cracking, **IoT_reaper** infects IoT devices by exploiting multiple IoT device vulnerabilities.

We noticed 9 IoT vulnerability exploits have been integrated into current samples as follows:

- **Dlink** https://blogs.securiteam.com/index.php/archives/3364
- **Goahead** https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html
- **JAWS** https://www.pentestpartners.com/blog/pwning-cctv-cameras/
- **Netgear** https://blogs.securiteam.com/index.php/archives/3409
- **Vacron** NVR https://blogs.securiteam.com/index.php/archives/3445
- **Netgear** http://seclists.org/bugtraq/2013/Jun/8
- **Linksys** http://www.s3cur1ty.de/m1adv2013-004
- **dlink** http://www.s3cur1ty.de/m1adv2013-003
- **AVTECH** https://github.com/Trietptm-on-Security/AVTECH

vulnerabilities	desc	source or Credit	release date	first seen in samples
1	D-Link 850L Multiple Vulnerabilities	Zdenda, Peter Geissler, Pierre Kim	2017-08-08	early than 2017-10-10
2	multiple vulnerabilities on multiple device	Pierre Kim	2017-03-08	early than 2017-10-10
3	vulnerabilities on JAWS			early than 2017-10-10
4	Netgear ReadyNAS Surveillance Unauthenticated Remote Command Execution	Kacper Szurek	2017-09-27	early than 2017-10-10
5	Vacron NVR Remote Command Execution	independent researcher	2017-10-08	early than 2017-10-10
6	Unauthenticated command execution on Netgear DGN devices	roberto () greyhats it	2013-05-31	2017-10-12
7	Multiple Vulnerabilities in Linksys E1500/E2500	m1k3	2013-02-05	2017-10-12
8	Multiple Vulnerabilities in D'Link DIR-600 and DIR-300 (rev B)	m1k3	2013-02-04	2017-10-12
9	multiple vulnerabilities on AVTech devices	Trietptm-on-Security	2016-10-11	2017-10-16

Note just in the last 10 days, the attacker has continuously added more new exploits into samples, one of which is adopted only 2 days after the disclosure of the vulnerability was made.

- Vacron NVR remote exploit was exposed on 2017-10-08 and was added into bot sample before 2017-10-10;
- 3 and 1 exploits are added separately in two updates on 2017-10-12 and 2017-10-16;

The LUA Execution Environment Integrated in the Malware

Md5: CA92A3B74A65CE06035FCC280740DAF6
Based on the integrated LUA execution environment, author will be able to write very complex and efficient attack scripts now

Approximately 100 DNS Open Resolvers Were Integrated in This Malware

The botnet has embedded more than 100 DNS open resolvers in its lua sample, so dns amplification attack can be easily carried out. And a cross-checking with our DRDoS data feed indicates that about one-third of these open DNS servers have been used as reflector in real dns amplification attacks. We have yet to see this type of config in any other mirai variants.

No DDoS Attack Command observed Till Now

In terms of attacking command, although we saw support of DDoS attack in the source file of Lua execution environment, we have not seen actual DDoS attack so far. The only instructions we saw are to download samples. This means the attacker is still focusing on spreading the botnets.

Infection Measurement

By using some tricks, we are able to draw some fairly accurate measurement on the scale of the infection, here are a sample of the numbers.

- Number of vulnerable devices in one c2 queue waiting to be infected : over 2m;
- Infected bots controlled by one c2 in last 7 days: over 20k ;
- Number of daily active bots controlled by one c2 : around 10k for yesterday(October 19) ;
- Number of simultaneous on-line bots controlled by one c2 : around 4k

IoC URLs

hxxp://cbk99.com:8080/run.lua
hxxp://bbk80.com/api/api.php
hxxp://103.1.221.40/63ae01/39xjsda.php
hxxp://162.211.183.192/down/server.armel
hxxp://162.211.183.192/sa
hxxp://162.211.183.192/sa5
hxxp://162.211.183.192/server.armel
hxxp://162.211.183.192/sm
hxxp://162.211.183.192/xget
hxxp://198.44.241.220:8080/run.lua
hxxp://23.234.51.91/control-ARM-LSB
hxxp://23.234.51.91/control-MIPS32-MSB
hxxp://23.234.51.91/ht_am5le
hxxp://23.234.51.91/ht_mpbe
hxxp://27.102.101.121/down/1506753086
hxxp://27.102.101.121/down/1506851514

IoC Hashes

3182a132ee9ed2280ce02144e974220a
3d680273377b67e6491051abe17759db
41ef6a5c5b2fde1b367685c7b8b3c154
4406bace3030446371df53ebbdc17785
4e2f58ba9a8a2bf47bdc24ee74956c73
596b3167fe0d13e3a0cfea6a53209be4
6587173d571d2a587c144525195daec9

6f91694106bb6d5aaa7a7eac841141d9
704098c8a8a6641a04d25af7406088e1
726d0626f66d5cacfeff36ed954dad70
76be3db77c7eb56825fe60009de2a8f2
95b448bdf6b6c97a33e1d1dbe41678eb
9ad8473148e994981454b3b04370d1ec
9f8e8b62b5adaf9c4b5bdbce6b2b95d1
a3401685d8d9c7977180a5c6df2f646a
abe79b8e66c623c771acf9e21c162f44
b2d4a77244cd4f704b65037baf82d897
ca92a3b74a65ce06035fcc280740daf6
e9a03dbde09c6b0a83eefc9c295711d7
f9ec2427377cbc6afb4a7ff011e0de77
fb7c00afe00eeefb5d8a24d524f99370