Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869

blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/

Li Fengpei December 5, 2017

5 December 2017 / IoT Botnet
Author: 360 netlab

```
[Update History]
- At 2017-12-05 18:56:40 UTC, 2 hours after our blog goes live, we observed the C2
sending kill scan command to the bots, and that explains why the scan activities on
the two ports started to drop on a global scale.

- The C2 address 95.211.123.69:7654 is the typo for 95.211.123.69:7645
```

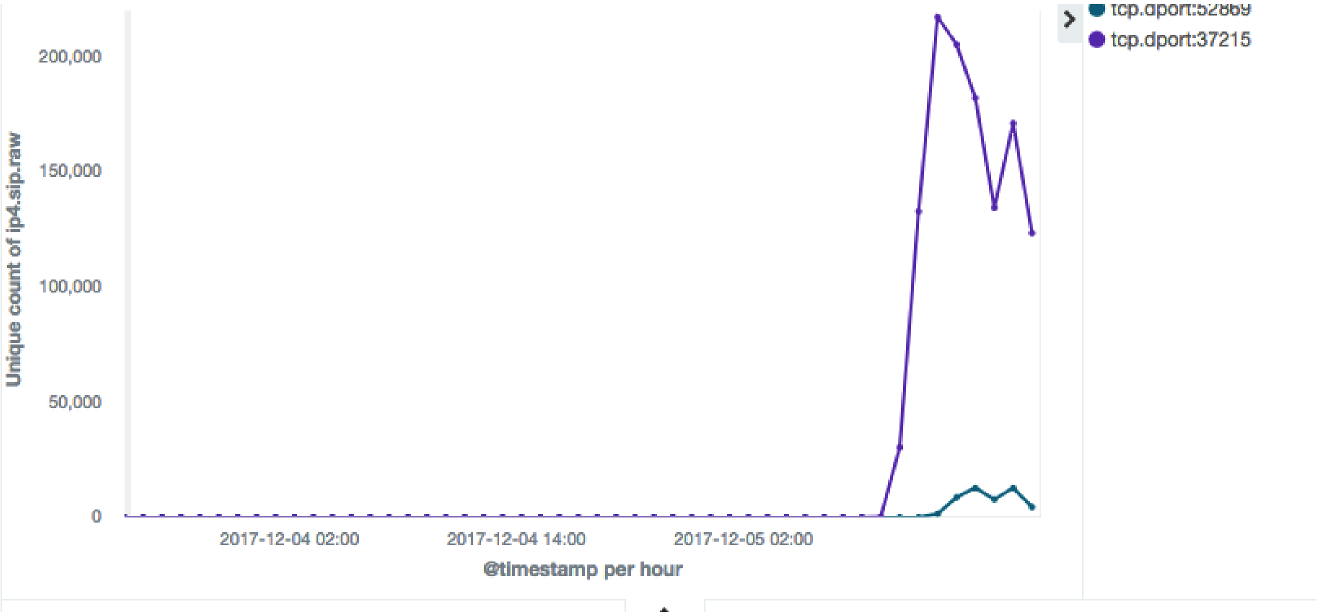
In our last blog, we mentioned there were almost 100k unique scanner IPs from Argentina scanning port 2323 and port 23, and we concluded it was a new mirai variant. For the last few days, the scanning behavior has gotten more intense, and more countries started to show up on our ScanMon platform as scan source. We have been able to dig more into this situation and see some bigger picture, and realized that the 2323|23 scan is only a piece of a big puzzler, while we are still doing more in-depth research into this matter, we bumped into a new situation today which we think needs some immediate attention from the security community, so here is a very brief and rough write-up.

About 12 hours ago (2017-12-05 11:57 AM GMT+8), we noticed a new version of Satori (a mirai variant which we named Satori), starting to propagate very quickly on port 37215 and 52869. This new variant has two significant differences from known mirai variants:

- The bot itself now does NOT rely on loader|scanner mechanism to perform remote planting, instead, bot itself performs the scan activity. This worm like behavior is quite significant.
- Two new exploits, which work on port 37215 and 52869 have been added, see below for more details. Due to the worm like behavior, we all should be on the lookout for the port 37215 and 52869 scan traffic. (For those who don’t have the visibility, feel free to check out our free Scanmon system for port 37215 and 52869, or ISC port pages for 37215 and 52869.

This malware is the newest version of Satori. We have been tracking Satori for months, and have strong evidence this new wave of attack can be linked to previous attack on port 23 and 2323 scanning traffic upticks.

The scanning IP (aka, the bot) numbers are now climbing straight up. For example, during last recent 12 hours we have seen 263,250 different IPs scanning port 37215, and 19,403 IPs scanning port 52869.



The Malware Sample and the C2s

We have collected following samples from our honeypot.

df9c48e8bc7e7371b4744a2ef8b83ddf	hxxp://95.211.123.69/b
a7922bce9bb0cf58f305d17ccbc78d98	hxxp://95.211.123.69/fahwrzadws/okiru.mipsel
37b7c9831334de97c762dff7a1ba7b3f	hxxp://95.211.123.69/fahwrzadws/okiru.arm7
e1411cc1726afe6fb8d09099c5fb2fa6	hxxp://95.211.123.69/fahwrzadws/okiru.x86
cd4de0ae80a6f11bca8bec7b590e5832	hxxp://95.211.123.69/fahwrzadws/okiru.x86
7de55e697cd7e136dbb82b0713a01710	hxxp://95.211.123.69/fahwrzadws/okiru.mips
797458f9cee3d50e8f651eabc6ba6031	hxxp://95.211.123.69/fahwrzadws/okiru.m68k
353d36ad621e350f6fce7a48e598662b	hxxp://95.211.123.69/fahwrzadws/okiru.arm
8db073743319c8fca5d4596a7a8f9931	hxxp://95.211.123.69/fahwrzadws/okiru.sparc
0a8efeb4cb15c5b599e0d4fb9faba37d	hxxp://95.211.123.69/fahwrzadws/okiru.powerpc
08d48000a47af6f173eba6bb16265670	hxxp://95.211.123.69/fahwrzadws/okiru.x86_64
e9038f7f9c957a4e1c6fc8489994add4	hxxp://95.211.123.69/fahwrzadws/okiru.superh

Satori borrows code from mirai with some major changes.

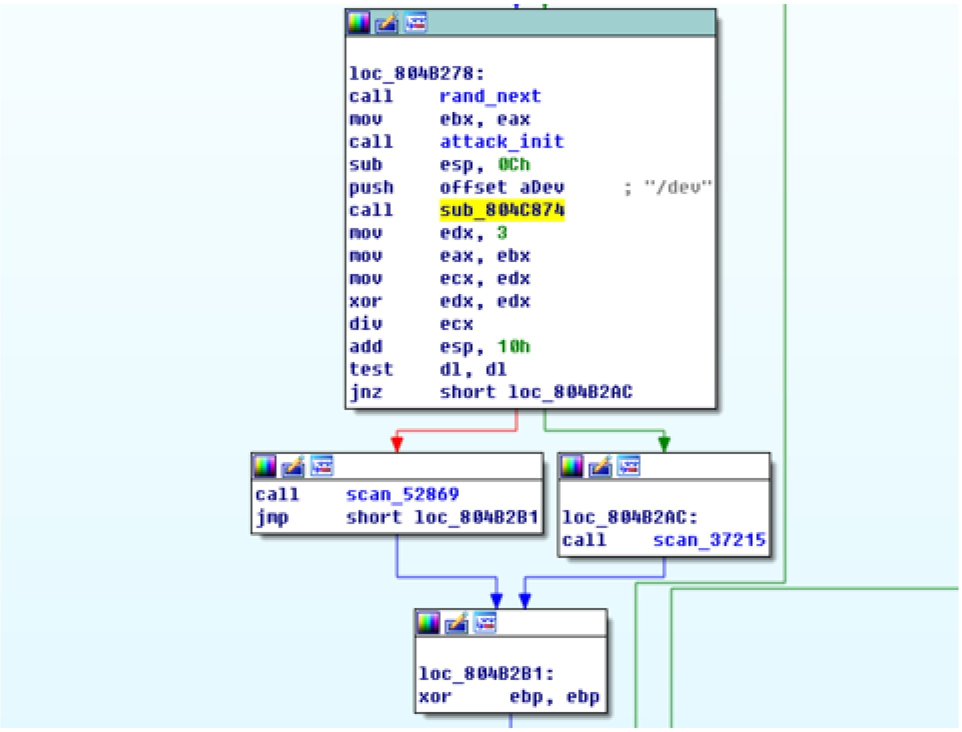
there are 3 C2s in the sample e1411cc1726afe6fb8d09099c5fb2fa6 we got,

- 95.211.123.69:7645
- network.bigbotpein.com:23
- control.almashosting.ru

Note: the only working c2 is **95.211.123.69:7645**, the other network.bigbotpein.com:23 and control.almashosting.ru is not actually being used here, they might be there just to trick security researcher to connect to the wrong C2s. (Note again, we also have old samples, as well as some fresh new samples coming in, in which control.almashosting.ru is really been used.)

The Scanning Activity

As can be seen from the following picture, the bot will scan port 37215 and 52869 randomly, determined by the remainder of a random integer mod 3.



```
loc_804B278:
call    rand_next
mov     ebx, eax
call    attack_init
sub     esp, 0Ch
push    offset aDev     ; "/dev"
call    sub_804C874
mov     edx, 3
mov     eax, ebx
mov     ecx, edx
xor     edx, edx
div     ecx
add     esp, 10h
test    dl, dl
jnz     short loc_804B2AC
```

```
call    scan_52869
jmp     short loc_804B2B1
```

```
loc_804B2AC:
call    scan_37215
```

```
loc_804B2B1:
xor     ebp, ebp
```

The Exploits

During the scanning, Satori will utilize two different exploits, one on port 37215, while the other on 52869.

- The one on port 37215 is not fully disclosed yet, our team has been tracking this in the last few days and got quite some insight, but we will not discuss it here right now.(stay tuned for our update later).
- The one on port 52869 is derived from CVE-2014-8361.

Not only are Satori penetrating with these exploits, but they also drive infected devices to download themselves from the same original download URL. This makes a loop, and causes Satori spreading in a `worm` manner.

The Connection to Previous Port 23 and 2323 Scanning Upticks

In our previous blog, we have mentioned an upticks on port 23 and 2323 scanning traffic in Argentina.

Actually, in the next few days, more countries such as Egypt, Tunisia, Columbia have been picked up by our monitoring system, as we mentioned in the beginning of this blogpost, our investigation reveals the port scan is only part of the whole picture.

Right now we just want to point out that the 2323|23 attacks and today Satori's attack shares some common factors, for example, the samples' name and static features, some of the C2 protocols and sharing of the same exploits. These make we believe they two are connected.

We will share more details on our blog later on.

IoC

Samples in This Wave

Satori is evolving as of our writing, we have capture some more samples with difference c2..etc, so here is only some of the IoCs.

```
df9c48e8bc7e7371b4744a2ef8b83ddf        hxxp://95.211.123.69/b
a7922bce9bb0cf58f305d17ccbc78d98        hxxp://95.211.123.69/fahwrzadws/okiru.mipsel
37b7c9831334de97c762dff7a1ba7b3f        hxxp://95.211.123.69/fahwrzadws/okiru.arm7
e1411cc1726afe6fb8d09099c5fb2fa6        hxxp://95.211.123.69/fahwrzadws/okiru.x86
cd4de0ae80a6f11bca8bec7b590e5832        hxxp://95.211.123.69/fahwrzadws/okiru.x86
7de55e697cd7e136dbb82b0713a01710        hxxp://95.211.123.69/fahwrzadws/okiru.mips
797458f9cee3d50e8f651eabc6ba6031        hxxp://95.211.123.69/fahwrzadws/okiru.m68k
353d36ad621e350f6fce7a48e598662b        hxxp://95.211.123.69/fahwrzadws/okiru.arm
8db073743319c8fca5d4596a7a8f9931        hxxp://95.211.123.69/fahwrzadws/okiru.sparc
0a8efeb4cb15c5b599e0d4fb9faba37d        hxxp://95.211.123.69/fahwrzadws/okiru.powerpc
08d48000a47af6f173eba6bb16265670        hxxp://95.211.123.69/fahwrzadws/okiru.x86_64
e9038f7f9c957a4e1c6fc8489994add4        hxxp://95.211.123.69/fahwrzadws/okiru.superh
```

Some Earlier Samples

```
c63820d8aff3b18b3ee0eaee4e9d26b0        hxxp://172.93.97.219/okiru.mipsel
fd2bd0bf25fc306cc391bdcde1fcaeda        hxxp://172.93.97.219/okiru.arm
ba98c78a65ebf17615fee9a7ef34b405        hxxp://172.93.97.219/okiru.arm7
8a561bda915c89668e611b0ba72b0429        hxxp://172.93.97.219/okiru.m68k
f8130e86dc0fcdbcfa0d3b2425d3fcbf        hxxp://172.93.97.219/okiru.x86
7a38ee6ee15bd89d50161b3061b763ea        hxxp://172.93.97.219/okiru.mips
3f401fc6b8a5847376e4d070505bd9fe        hxxp://172.93.97.219/cryptonite.mips
a69692a2506f2127b23a8c35abe11427        hxxp://165.227.220.202/bins/mips
hxxp://198.7.59.177/fahwrzadws/okiru.mips
hxxp://198.7.59.177/cryptonite.mips
```