Art of Steal: Satori Variant is Robbing ETH BitCoin by Replacing Wallet Address

blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/

RootKiter January 17, 2018

17 January 2018 / Botnet
The security community was moving very fast to take actions and sinkhole the Satori botnet C2 after our December 5 blog. The spread of this new botnet has been temporarily halted, but the threat still remains.

Starting from 2018-01-08 10:42:06 GMT+8, we noticed that one Satori's successor variant (we name it Satori.Coin.Robber) started to reestablish the entire botnet on ports 37215 and 52869.

What really stands out is something we had never seen before, this new variant actually hacks into various mining hosts on the internet (mostly windows devices) via their management port 3333 that runs Claymore Miner software, and replaces the wallet address on the hosts with its own wallet address.

From the most recently pay record till 2018-01-16 17:00 GMT+8, we can see:

- Satori.Coin.Robber is actively mining, with lastest update 5 minutes ago.
- Satori.Coin.Robber owns an average calculation power of 1606 MH/s for the last 2 days; the account has accumulated 0.1733 ETH coins over the past 24 hours
- Satori.Coin.Robber has already got the first ETH coin paid at 14:00 on January 11, 2017, with another 0.76 coin in the balance

Also worth mentioning is that the author of Satori.Coin.Robber claims his current code is not malicious and leaves an email address(see the section below for more details):

```
Satori dev here, dont be alarmed about this bot it does not currently have any
malicious packeting purposes move along. I can be contacted at curtain@riseup.net
```

A Series of Security Issues on Claymore Miner Remote Management

Claymore Miner is a popular coin-mining software used by quite a lot of mining devices these days.

According to its document, the Claymore Miner Windows version provides a remote monitoring and/or management interface on port 3333 (the EthMan.exe file in the "remote management" directory). And by default earlier versions allow not only remote reading for mining status, but also operations like restart, upload files and some other control operations.

Apparently, the above feature is a security issue. As a fix, after version 8.1, the Claymore Miner will not use port 3333 but -3333 (a negative one) as the startup parameter by default, which means read-only monitoring actions are supported, but other controlling actions are all denied.

But this is not the end. In November 2017, CVE-2017-16929 went public, which allows remote read and/or write to arbitrary files for Claymore Miner. The corresponding exploit code has also been disclosed.

The scanning payload (the exploit code) we are going to discuss here is different from all above though. It works primarily on the Claymore Mining equipment that allows management actions on 3333 ports with no password authentication enabled (which is the default config). In order to prevent potential abuse, we will not discuss too much details in this article.

Satori.Coin.Robber Variant is Exploiting above Issue to Robber ETH Coins

From 2018-01-08 to 2018-01-12, have captured the following malware samples:

```
737af63598ea5f13e74fd2769e0e0405        http://77.73.67.156/mips.satori
141c574ca7dba34513785652077ab4e5        http://77.73.67.156/mips.satori
4e1ea23bfe4198dad0f544693e599f03        http://77.73.67.156/mips.satori
126f9da9582a431745fa222c0ce65e8c        http://77.73.67.156/mips.satori
74d78e8d671f6edb60fe61d5bd6b7529        http://77.73.67.156/mips.satori
59a53a199febe331a7ca78ece6d8f3a4        http://77.73.67.156/b
```

These samples are subsequent variants of Satori, which scan not only the previous 37215 and 52869 ports, but also the 3333 ports. The payload on on three ports are:

- **Port 37215**: Known, exploiting vulnerabilities CVE-2017-17215, Huawei recently released the relevant statement
- **Port 52869**: Known, exploiting vulnerabilities CVE-2014-8361, related to some Realtek SDK, the exploit code PoC is published since 2016
- **Port 3333**: Newly emerged, exploiting ETH mining remote management interface mentioned above.

The scanning payload on port 3333 is shown in the above image. Satori.Coin.Robber issues three packets respectively:

- **Package 1**: miner_getstat1, get mining state
- **Package 2**: miner_file, update reboot.bat file, replace the mine pool and wallet address;
- **Package 3**: miner_reboot, reboot the host with new wallet

During this process, the mining pool and the wallet will be replaced:

- New pool: eth-us2.dwarfpool.com:8008
- New wallet: 0xB15A5332eB7cD2DD7a4Ec7f96749E769A371572d

Similarities and Differences between Satori.Coin.Robber and the Original Satori

Comparison between Satori.Coin.Robber and Satori:

- 737af63598ea5f13e74fd2769e0e0405 Satori.Coin.Robber
- 5915e165b2fdf1e4666a567b8a2d358b satori.x86_64, the original Satori in October 2017 with VT report here

Similarities:

- **Code**: Both use UXP packing, with the **same magic number 0x4A444E53**. The unpacked code share similar code structures
- **Configurations**: The configurations are both encrypted. The encryption algorithm and a large number of configuration strings are the same. For example, /bin/busybox SATORI, bigbotPein, 81c4603681c46036, j57*&jE, etc.
- **Scanning payload**: Both scan ports 37215 and 52869 and share the same payload

Differences:

- **Scanning payload**: Satori.Coin.Robber added a new payload against Claymore Miner on port 3333
- **Scanning process**: Satori.Coin.Robber adopts an asynchronous network connection (NIO) method to initiate a connection, which improves scan efficiency
- **C2 Protocol**: Satori.Coin.Robber enables a new set of C2 communication protocols that communicate with 54.171.131.39 using the DNS protocol. We will go through the details later.

Below are some detailed screenshots:

Both samples share the same UPX packing magic numbers:

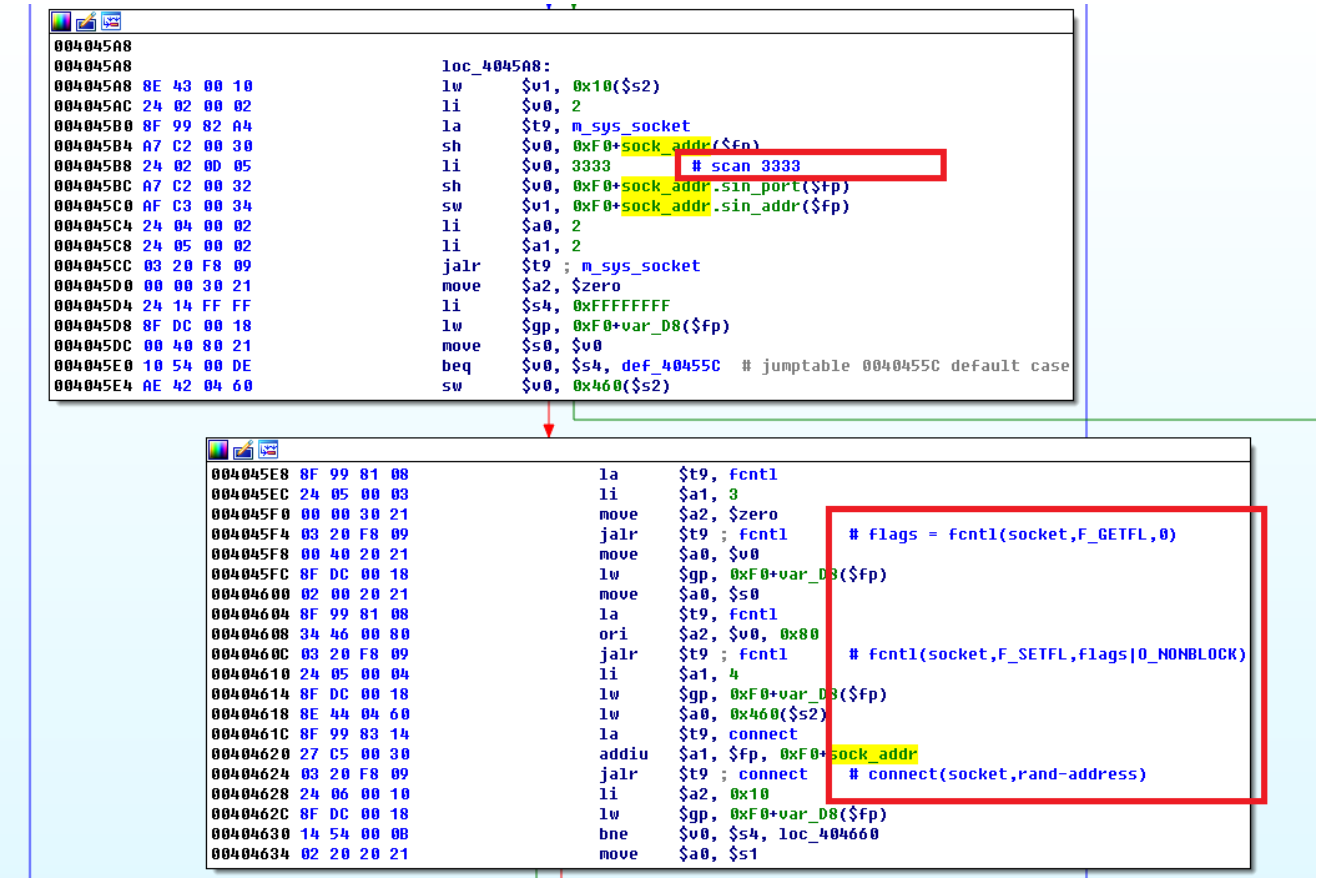
```
00006B00  B9 70 C2 CE 8F E0 29 4A D0 F3 4A 1A E6 75 D6 91  ¹pÂÎ.à)JÐóJ.æuÖ.
00006B10  E2 44 D0 62 C0 5D 36 D5 31 2B 96 F1 18 D8 A1 05  âDÐbÀ]6Õ1+.ñ.Ø¡.
00006B20  32 9C 21 40 00 00 00 00 53 4E 44 4A 00 00 00 00  2.!@....SNDJ....
00006B30  53 4E 44 4A 0D 16 0E 0A 99 DD 3E F6 F9 88 0E 82  SNDJ.....Ý>öù...
00006B40  C0 02 00 00 A4 00 00 00 A0 E0 00 00 49 07 00 54  À...¤....à..I..T
00006B50  F4 00 00 00                                     ô...
```

5915E165B2FDF1E4666A567B8A2D358B

```
00004E80  61 2D 2C D7 4A 91 C5 94 1D A4 D9 C1 7B A0 99 86  a-,×J.Å..¤ÙÁ{...
00004E90  B3 79 39 68 9B 4E E9 7D 8D FF F9 0A D2 D6 C4 83  ³y9h.Né}.ÿù.ÒÖÄ.
00004EA0  3E DD 20 CD DC 18 93 B1 7B D6 00 00 00 00 53 4E  >Ý ÍÜ..±{Ö....SN
00004EB0  44 4A 00 00 00 00 00 00 53 4E 44 4A 0D 89 0E 0A  DJ......SNDJ....
00004EC0  00 00 02 60 00 00 00 CE CA 0D 82 13 C6 A9 5D 23  ...`...ÎÊ...Æ©]#
00004ED0  00 00 C0 38 00 00 00 4F 00 00 00 80              ..À8...O....
```

737AF63598EA5F13E74FD2769E0E0405

Satori.Coin.Robber uses asynchronous network connection for scanning:



Satori.Coin.Robber's New C2 Communications Protocol

C2 of Satori.Coin.Robber:

- A hard coded IP address 54.171.131.39, located in Dublin, Ireland.

- The communication protocol is based on DNS protocol, which can be tested by query like "dig@54.171.131.39 $DNS-QNAME any+short", and different $DNS-QNAME corresponds to different function.

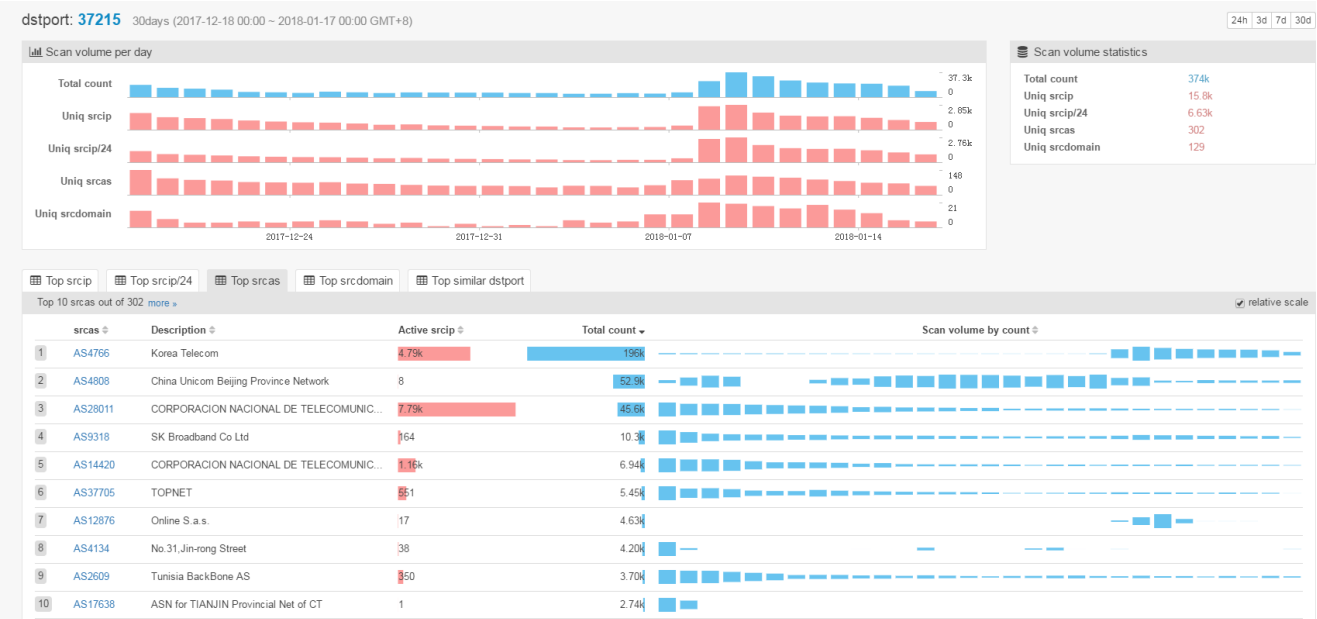
All C2 protocol lists as follows, note the fourth one is not written anywhere in the Satori.Coin.Robber code, we just tied and found it has dns response:

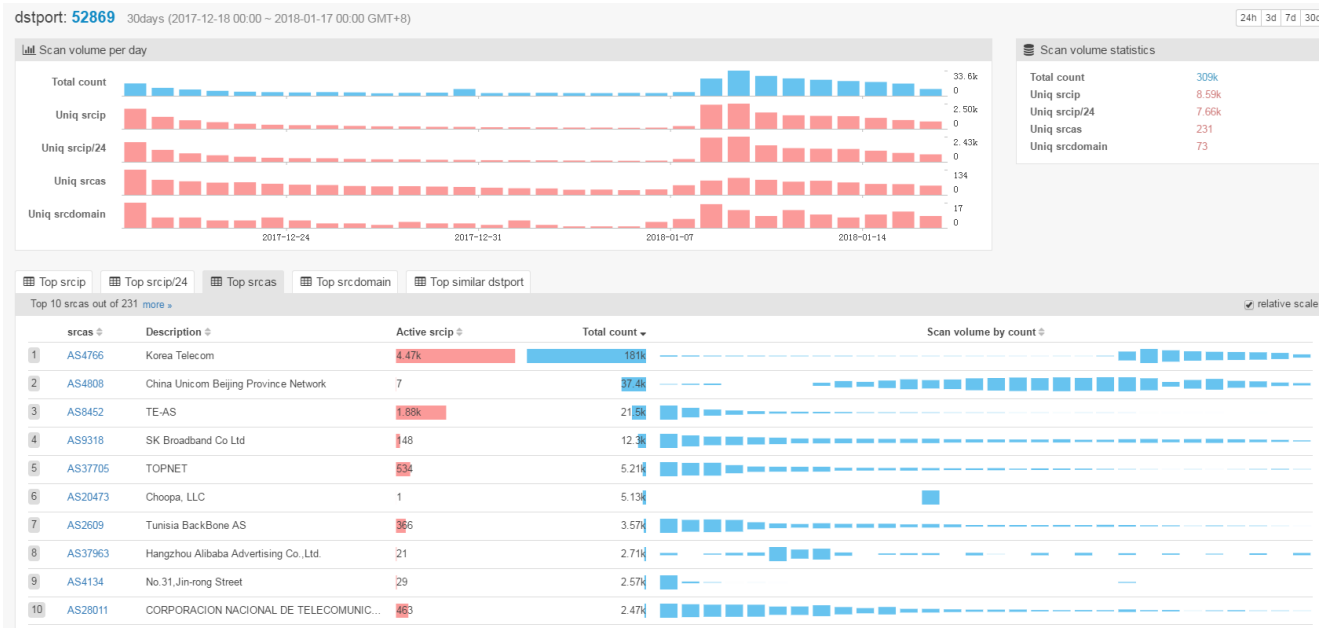
C2	dns-qname	source	dns-response
54.171.131.39	w.sunnyjuly.gq	sample	0xB15A5332eB7cD2DD7a4Ec7f96749E769A371572d
54.171.131.39	p.sunnyjuly.gq	sample	eth-us2.dwarfpool.com:8008
54.171.131.39	s.sunnyjuly.gq	sample	Satori dev here, dont be alarmed about this bot it does not currently have any malicious packeting purposes move along. I can be contacted at curtain@riseup.net.
54.171.131.39	f.sunnyjuly.gq	fuzzing	213.74.54.240

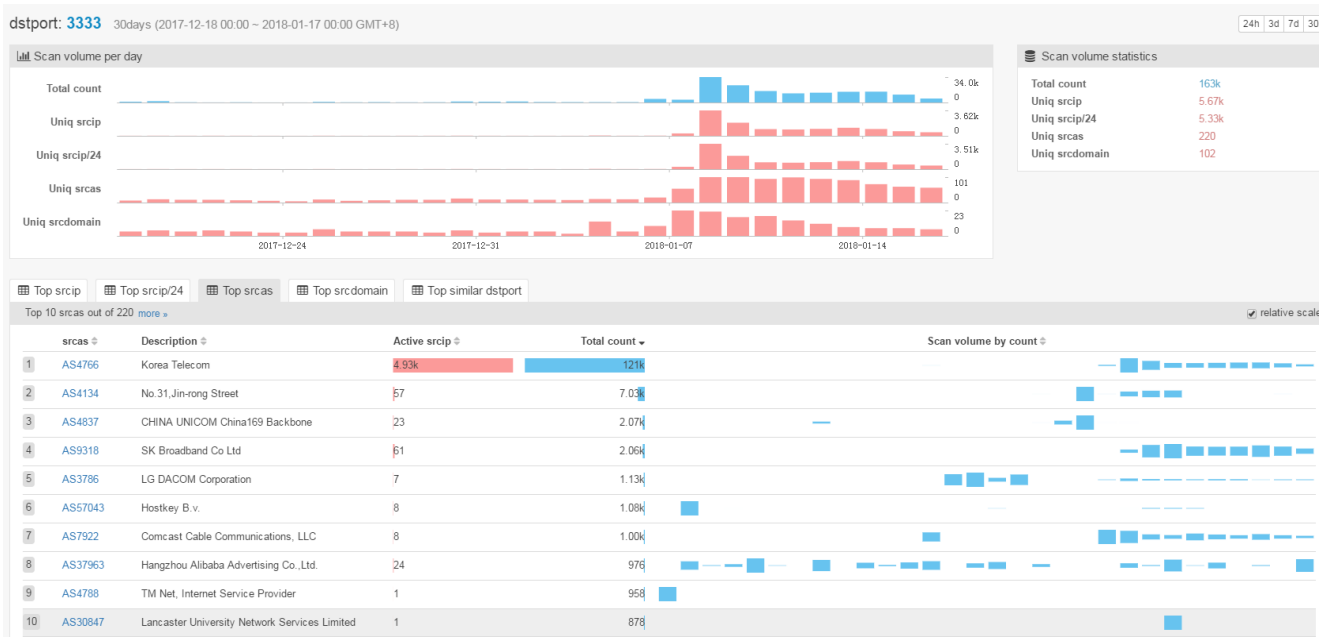
The first two responses are the same mining pool and wallet addresses used by the bot after tampering with other Claymore Miner mining equipment. However, at this stage, it seems that these server returned values is yet to be used.

Infection Trend

We evaluate Satori.Coin.Robber's infection scale and trend by comparing the scanning volumes on three ports: 37215, 52869 and 3333.







The three figures above show that the scanning volumes of these three ports all increase sharply during this period, which is consistent with the behavior of Satori.Coin.Robber samples.

- all emerged around 2018-01-08
- scanning spikes were all around 2018-01-08 to 2018-01-09
- the volumes of scanning decrease in recent few days
- AS4766 Korea Telecom contributes most of the scanning source
- totally about 4.9K uniq scanning source IPs