# Threat Alert: DDG 3013 is Out

blog.netlab.360.com/threat-alert-ddg-3013-is-out/

JiaYu

August 1, 2018

1 August 2018
DDG is a mining botnet mainly focusing on SSH, Redis databases and OrientDB database servers. We captured the first DDG botnet on October 25, 2017, and subsequently released several reports. A recent report was released in 2018-06, which reflected the newest version of DDG 3012 at that time.

This morning, we noticed that DDG version 3013 came out.

### IoC

C2

```
149.56.106.215:8000    Canada/CA Pierrefonds   "AS16276 OVH SAS"
```

Download URL

```
hxxp://149.56.106.215:8000/i.sh               #fca88105ed6f1fc72d25cfb30a0080b8
hxxp://149.56.106.215:8000/static/3011/ddgs.i686    #999fc24f53034b4c73866a0699be15fa
hxxp://149.56.106.215:8000/static/3011/ddgs.x86_64  #55b1d7b0fa1c479c02660896e05db910
hxxp://149.56.106.215:8000/static/3012/ddgs.i686    #e31c1d7a8025e7c3266a07e37c55a4ba
hxxp://149.56.106.215:8000/static/3012/ddgs.x86_64  #26b3aef91bacfa082deff9812acf7875
hxxp://149.56.106.215:8000/static/3013/ddgs.i686    #7fb5665a632fe3f91c65df960ef56d9f
hxxp://149.56.106.215:8000/static/3013/ddgs.x86_64  #c090e30a008b6bc0ea323ba5928c4a62
hxxp://149.56.106.215:8000/static/qW3xT             #c50d3e20b3519f096630e31277fefceb
hxxp://149.56.106.215:8000/static/qW3xT.1           #532a35a8d0fe4944c24575c0336eff8a
hxxp://149.56.106.215:8000/static/qW3xT.2           #0a63e48163056b04bf1d48420b7c8150
```

New mining pool agent

```
104.197.211.117:443 United States/US "AS15169 Google LLC"
```

### Infect Method

Using mis-configured Redis in the same way as previous versions of DDGs.

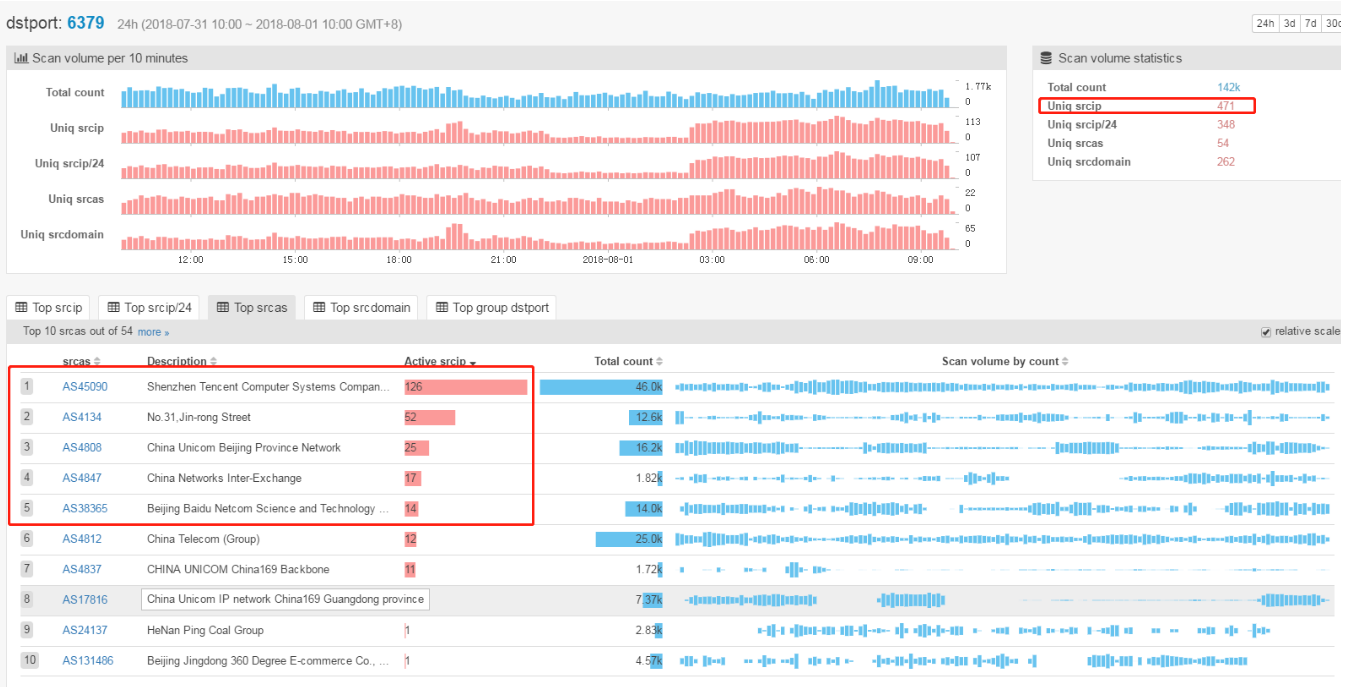
### Monetization method

Mining

- Mining Pool:Agent: 104.197.211.117
- Wallet Address: 42d4D8pASAWghyTmUS8a9yZyErA4WB18TJ6Xd2rZt9HBio2aPmAAVpHcPM8yoDEYD9Fy7eRvPJhR7SKFyTaFbSYCNZ2t3ik

### Activities

In the past 24 hours, our ScanMon reported 471 scan sources, mainly from China mainland.



dstport: 6379 24h (2018-07-31 10:00 ~ 2018-08-01 10:00 GMT+8)

Scan volume statistics

| | |
|---|---|
| Total count | 142k |
| Uniq srcip | 471 |
| Uniq srcip/24 | 348 |
| Uniq srcas | 54 |
| Uniq srcdomain | 262 |

Top 10 srcas out of 54 more »

| | srcas | Description | Active srcip | Total count |
|---|---|---|---|---|
| 1 | AS45090 | Shenzhen Tencent Computer Systems Compan... | 126 | 46.0k |
| 2 | AS4134 | No.31,Jin-rong Street | 52 | 12.6k |
| 3 | AS4808 | China Unicom Beijing Province Network | 25 | 16.2k |
| 4 | AS4847 | China Networks Inter-Exchange | 17 | 1.82k |
| 5 | AS38365 | Beijing Baidu Netcom Science and Technology ... | 14 | 14.0k |
| 6 | AS4812 | China Telecom (Group) | 12 | 25.0k |
| 7 | AS4837 | CHINA UNICOM China169 Backbone | 11 | 1.72k |
| 8 | AS17816 | China Unicom IP network China169 Guangdong province | | 7.37k |
| 9 | AS24137 | HeNan Ping Coal Group | 1 | 2.83k |
| 10 | AS131486 | Beijing Jingdong 360 Degree E-commerce Co., ... | 1 | 4.57k |

## Contact Us

Readers can feel free to contact us on our **twitter** or WeChat **360Netlab**