Old Botnets never Die, and DDG REFUSE to Fade Away

blog.netlab.360.com/old-botnets-never-die-and-ddg-refuse-to-fade-away/

JiaYu July 12, 2018

12 July 2018
DDG is a mining botnet that specializes in exploiting SSH, Redis database and OrientDB database servers. We first caught it on October 25, 2017, at that time, DDG used version number 2020 and 2021, and we noticed that the botnet has two internally reserved domain names that had not been registered. So we went ahead and registered the two domain names so we were able to measure the infections, (4,391 infected IPs) The original blog is here.

Some botnet goes away after we release the analysis report, such as http81 (persirai), but the DDG stays.

Three months after the release of our first DDG report, in May 2018, DDG got some major updates. Version 3010 and 3011 appeared, we also witnessed the authors effort to polish the 3011 so he can get the mining part work.

On June 12, we captured that DDG.Mining.Botnet released yet another new version 3012 with yet another c2 address. For all the technical details, please check our detailed DDG blog here.

List of DDG Updates

The following figures describe some high level overview and comparison between different DDG versions.

Version	notice	report	update	202.181.169.98	218.248.40.228	165.225.157.157	69.64.32.12
2011	2017-10-25	2018-02-01		Yes	Yes		
2020	2017-10-25	2018-02-01			Yes		
2021	2017-10-25	2018-02-01			Yes		
3010	2018-05-07	2018-05-21				Yes	
3011	2018-05-07	2018-05-21	2018-06-01			Yes	Yes
3012	2018-06-12	2018-06-13				Yes	Yes

Version	crontab script keep alive	main process & SSH implant & Redis implant	Struts 2 implant	OrientDB implant	xmr wnTKYg	xmr imWBR1	xmr 2t3ik
2011	Yes	Yes	Yes	Yes	Yes		
2020	Yes	Yes	Yes	Yes	Yes	Yes	
2021	Yes	Yes	Yes	Yes	Yes	Yes	
3010	Yes	Yes				Yes	Yes
3011	Yes	Yes				Yes	Yes
3012	Yes	Yes					Yes

Module	File	Variant	Purpose
crontab script	i.sh	i.sh	keep live
main process & SSH implant & Redis implant	ddg	ddg.x86_64 ddg.i686	SSH Brute Force, Redis Misconfiguration
Struts 2 implant	ss22522	ss22522 ss22522.2 s2052 (?)	Struts2 Server, S2-052
OrientDB implant	ss2480	ss2480 ss2480.1 ss2480.2	OrientDB Server, CVE-2017-11467, Port 2480
xmr	wnTKYg	wnTKYg wnTKYg.noaes	monero.crypto-pool.fr 4AxgKJtp8TTN9Ab9JLnvg7BxZ7Hnw4hxigg35LrDVXbKdUxmcsXPEKU3SEUQ xeSFV3bo2zCD7AiCzP2kQ6VHouK3KwnTKYg
xmr	imWBR1	imWBR1	monero.crypto-pool.fr 45XyPEnJ6c2STDwe8GXYqZTccoHmscoNSDiTisvzzekwDSXyahCUmh19Mh2e wv1XDk3xPj3mN2CoDRjd3vLi1hrz6imWBR1
xmr	2t3ik	2t3ik 2t3ik.s 2t3ik.p 2t3ik.m qW3xT qW3xT.1	multi mining pool, 42d4D8pASAWghyTmUS8a9yZyErA4WB18TJ6Xd2rZt9HBio2aPmAAVpHcPM 8yoDEYD9Fy7eRvPJhR7SKFyTaFbSYCNZ2t3ik

From the figure we can see:

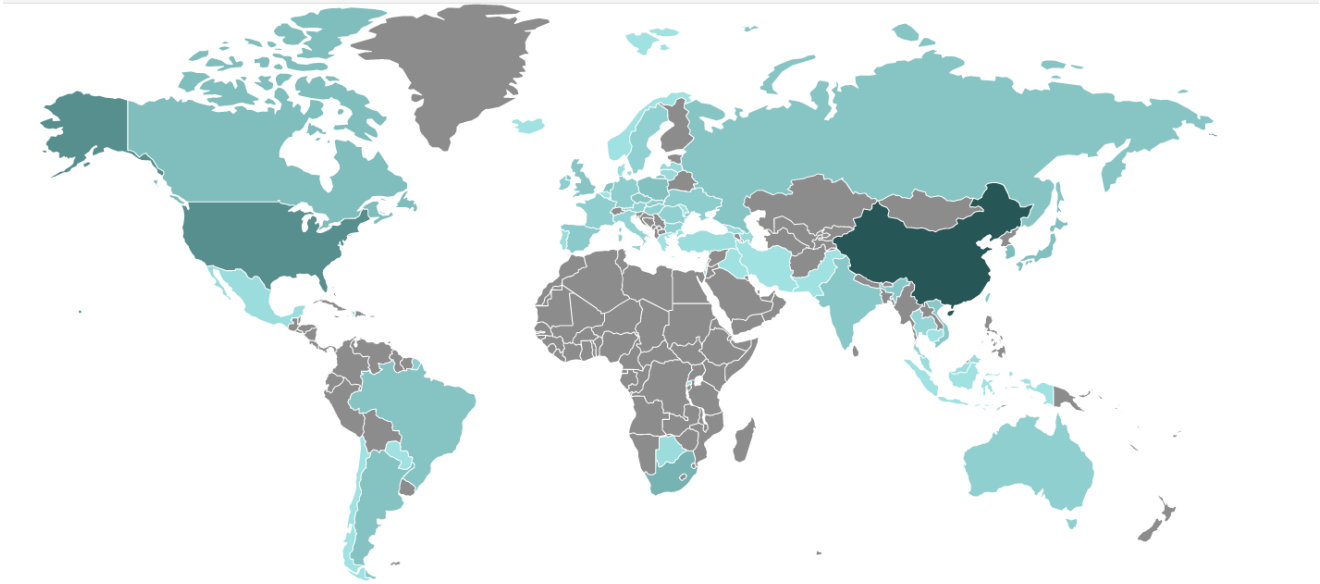
- **Version Update**: Starting from October 2017, DDG has released three major version of 201x, 202x, and 301x, and six minor-versions.
- **C2 IP address**: Four major C2 IPs have bee used.
- **Module structure**: Three major modules, propagate, keep-live, and mining
- **Infection method**: Brute force attacks on the SSH server and unauthorized access by the Redis server (2017-10 to date). In versions 201x and 202x, the Struts2 and OrientDB database servers were also targeted for infection.
- **Wallet Address**: Three wallet addresses. And the file name of the mining program normally the same as the last 5 to 6 strings of the wallet address.
- **Redundancy**: The author always keeps two versions of the botnet running at the same time to provide fault tolerance. After the 301x version, the author also started to use multiple mine pools for redundancy. Such as mining pool hk02.supportxmr.com, pool.supportxmr.com, xmr-asia1.nanopool.org, xmr-us-west1.nanopool.org, and mining pool proxy 47.52.57.128,165.225.157.157

In addition:

- **Profit**: According to our incomplete statistics, DDG's wallet addresses have received at least 7,425 Monroe coins just from Monero.crypto-pool.fr.

- **HUB**: DDG uses a group of hacked servers to provide download service to infected hosts. Each DDG version update refreshes this HUB_IP list. See the IoC section at the end of this article for infected IPs.

For Sinkhole, we sinkholed two unregistered domain names for DDG version 2020. Although the DDG 2021 version were quickly released and removed these two domain names, we were still able to get an accurate number of the infections. At that time, we recorded a total of 4,391 victim IP addresses. The main victims were China (73%) and the United States (11%):



IoC

DDG C2 List

```
218.248.40.228    India/IN    National Capital Territory of Delhi/New Delhi
202.181.169.98    Hong Kong/HK    Central and Western District/Central
165.225.157.157    United States/US    Nevada/Las Vegas
69.64.32.12    United States/US    Missouri/St Louis
```

IP_HUB list