DDG botnet, round X, is there an ending?

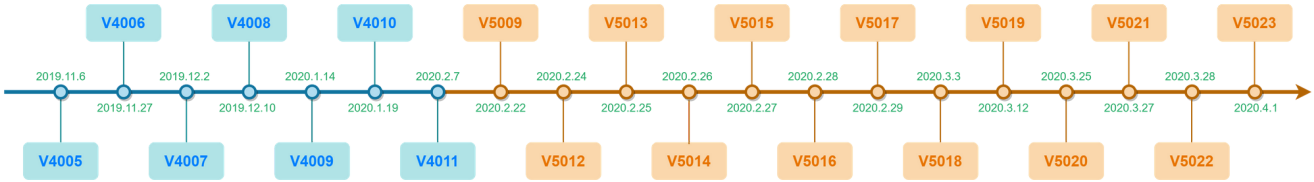
blog.netlab.360.com/ddg-botnet-round-x-is-there-an-ending/

JiaYu April 8, 2020

8 April 2020 / Botnet

DDG is a mining botnet that we first blogged about in Jan 2018, we reported back then that it had made a profit somewhere between 5.8million and 9.8million RMB(about 820,000 to 1.4Million US dollar), we have many follow up **blogs** about this botnet after that, but it shows no sign of slowing down.

Since November 2019, we started to see a frenzy of version updates of DDG, all together, we counted 20 updates, the following is a timeline:



This is something unprecedent, more interestingly, we see DDG totally dropped the mechanism for infecting servers on public network, instead, it put all its focus on the servers on intranet.

DDG now discard the use of XMR wallet so we lost the visibility on the money it makes now, but given the above two factors, it is probably safe to bet this botnet is making very good profits, the author probably is pretty happy with the already compromised devices he got, and he wants to stay low, and is in no rush to expand his bot army.

In the early days, DDG used IP and DNS for C2 communications, in 2018 we successfully registered two C2 domains in advanced before the author could do so and **sinkholed** the traffic, and we were able to get an accurate count of the compromised servers, 4,391 at that time..

One year later, in Jan 2019, DDG ditched the DNS C2 and introduced **Memberlist** based P2P network into its communication protocol. We **blogged** about it and was able to tap into the P2P network to track the infected devices again, and we logged a total of 5,695 devices

In Feb 2020, DDG made a major change regarding to its communication protocol again, a self-developed P2P protocol to build a hybrid P2P network has been adopted. The botnet still needs static C2(IP or dns), but with this new development, the author basically has a fail back safe that even if the c2 is taken down, the infected devices are still going to keep going and perform the mining tasks.

With this new update, we correspondingly developed a new p2p tracking module that joins the botnet's P2P network to track it, the number we are getting this time is much lower though, about 900 nodes every day, this has things to do with the new hybrid P2P implementation as it won't spit out all nodes now. And keep in mind that the botnet focuses on intranet now, so there are probably many devices behind a single ip.

To get a better number of the infection in China, we collaborate with a trusted partner in China, and was able to get the daily unique clients count just in China that connect to the active C2 on its C2 port, the daily number is about 17,xxx. the compromised devices are mostly servers, so frequent IP change is not expected, and there will be noise in this number for sure, but the number might provide some perspectives of the botnet's size just in China.

We are now **sharing** the tracking demo with some related data and data parsing tools at Github, so more security researchers can take a good look at it and hopefully slow down the seemingly unstoppable DDG botnet.

Currently, DDG only goes after weak SSH password for one single user name **root**, and the password dictionary comes with DDG has **17,907** entries in it, so make sure you have strong password for your **root** (and all other accounts)!

We are now simultaneously publishing a VERY lengthy technical write up, including IoCs with this blog **here** for readers who want to read all the newest details. Take a breath and check it out!