

Anchor_dns malware goes cross platform

medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30

Waylon Grange

July 13, 2020



Waylon Grange

Jul 13, 2020

.

3 min read

The actors behind Trickbot, a high profile banking trojan, have recently developed a Linux port of their new DNS command and control tool known as Anchor_DNS.

Often delivered as part of a zip, this malware is a lightweight Linux backdoor. Upon execution it installs itself as a cron job, determines the public ip for the host and then begins to beacon via DNS queries to its C2 server.

Because the DNS channel provides an indirect route for the malware to communicate the attackers aren't provided with the ip address of the victim. To mitigate this the malware utilizes public ip lookup services to determine where the target is located. Upon first run the malware will randomly select one of the following urls to find its external ip.



It then enters its main communication loop where it generates the DNS query and parses the result. The method for generating the DNS query uses a similar format as the windows version described in [this article](#) by NTT but with a few changes.



`anchor_dns` is instead replaced with `anchor_linux` and the `uname` command is utilized to determine the hostname and linux version. The `client_id` is a 32 byte value hardcoded into the binary. `LVER` is the Linux version which is also used as part of the hostname. If my linux version is `5.6.0` the `LVER` would be `L560`. Finally, the public ip discovered above along with the payload is appended to the end. This is all combined as shown above which is then XOR'd with `0xb9`, hex encoded, and then prepended to the root C2 domain. In this case, `billpi.com`

The server responds with a number of A records which contain the encoded response in a similar format to that outlined by NTT.



The malware's main functionality is to be a simple dropper. It has basic download and execute capabilities and when doing so on the linux host it will drop the payload to

```
/tmp/<random_15_chars> and execute via sh .
```

More interesting however is it that it also contains support for windows execution via smb shares and IPC. The sample also has a Windows version of the malware embedded inside that it can install on remote windows shares and then execute as a service. It utilizes the open source libsmb2 project to do this.



Given that the trickbot family has a history of harvesting putty credentials (see <https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire/>) we see how this can be used to further propagate with in the victims network.

The further development of the anchor family of malware suggests the trickbot family intends to continue utilizing its new DNS based command and control comms. Given the generally lower rate of linux malware detection it is of the utmost importance organization closely monitor their network traffic *and* DNS resolutions.

Hashes:

55754d178d611f17efe2f17c456cb42469fd40ef999e1058f2bfe44a503d877cC721189a2b89cd279e9a033c!

Domains:

*.biillpi.com

IPs:

23.95.97.59

Yara:

```
rule anchor_linux_dns{meta: author = "Stage 2 Security" description = "Trickbot
anchor_linux"strings: $hdr = {7f 45 4c 46} $x1 = {80 74 0? ?? b9} $x2 = "anchor_1" $x3 =
"getaddrinfo" $x4= "IPC$" $x5 = {48 ?? 2f 74 6d 70 2f 00 00 00} $x6 = "test my ip" $x7 =
{73 6d 62 32 5f [4-7] 5f 61 73 79 6e 63 20} $x8 = "Kernel32.dll" $x9 = "libcurl" $x10 =
"/1001/"condition: $hdr at 0 and 7 of ($x*)}
```