Cloud Server Port Access Analysis

Daniel Barry
CoffeeSpace Research

2017

Abstract - We analyse the logs of a Russian based virtual private server, revealing >98% are SSH packets and >80% of packets are from China.

Introduction

The purpose of this experiment is to log the traffic activity on ports of interest and from which Countries these originate, despite never having linked to or advertised the server online. This in turn can be used to speculate the use of default passwords on publicly internet connected devices, such as IoT (internet of things) devices, as well as the hacking capability of each Country.

Method

The Linux utility `tcpdump` [1] was used to log the activity on ports `21`, `22`, `80` and `443` to give information in the following format:

```
[Time] IP [Source IP].[Source Port] > \
  [Dest IP].[Dest Port]: tcp [TCP Seq]
```

The data was piped to file, with the resulting IP addresses being parsed into `whois` [2] to gain location data. Data was collected between 2nd November and 24th December in 2016. The server was a Debian virtual machine hosted on the Profit Server cloud, based in Russia [3].

Results

The results can be accessed via either [4] or [5], two mirror University hosted sites. Approximately 98% of the traffic is for SSH (port 22) and 1% for HTTP (port 80). We recorded a total of 3,776,468 packets over 52 days, roughly 50 per minute on average.

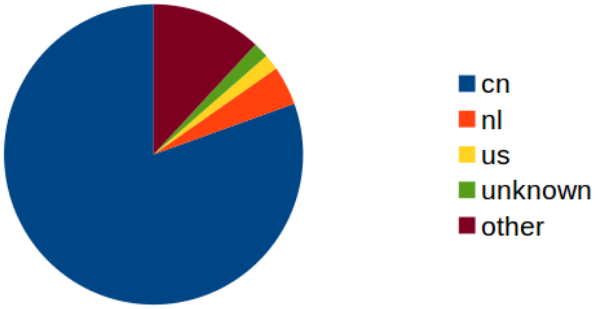

Figure 1: Traffic by Country for top 4 sources.

The data is broken down as follows: China (80.48%), Netherlands (4.22%), United States (1.68%), Unknown (unable to retrieve `whois` data) (1.68%) and Other (11.94%).

Conclusion

Interestingly, despite the servers being based in Russia, most of the attacks originate from Chinese IP addresses. It is not known whether the origin of the attack is from China or just used as part of a virtual private network. It's quite likely that the majority of these attacks are testing commonly used password lists in multiple languages, both found in password breaches and popular default passwords.

We see the following potential issues from these attacks:

- IoT or embedded devices that ship with non-unique default SSH passwords, such as Raspberry Pi's [6], often used to help form powerful distributed botnets [7].
- IoT or embedded devices that are designed to be internet connected and online 24/7 could make use of a service that automatically tests their connectivity from public servers. Basic firewall issues could be resolved automatically, or at least warn the client.
- Most computers, laptops and other internet connected Linux devices don't enforce a minimum level of password security for user accounts. SSH is often running by default.

The following actions are recommended:

- Test passwords against most used password lists in breaches.
- Ensure password strength using a method such as entropy [8].

References

[1] The TCPdump group. *TcpDump & LibPCap*, The TCPdump group. Link: http://www.tcpdump.org/

[2] d'Itri, M. *Package: whois*, Debian. Link: https://packages.debian.org/sid/whois

[3] Profit Server. *Virtual Servers VPS*, Profit Server. Link: https://profitserver.ru/en/

[4] Barry, D. *Open Test Data*, University of Hertfordshire. Link: https://homepages.herts.ac.uk/~db13acy/

[5] Barry, D. *Open Test Data*, University of Canterbury. Link: https://studweb.cosc.canterbury.ac.nz/~dba71/

[6] Clay, L., Nuttall, B. *Linux Users*, Raspberry Pi Foundation. Link: https://www.raspberrypi.org/documentation/linux/usage/users.md

[7] Krebs, B. *Source Code for IoT Botnet 'Mirai' Released*, Krebs on Security. Link: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

[8] Wikipedia. *Password strength*, Wikipedia Foundation. Link: https://en.wikipedia.org/wiki/Password_strength