DDoS Cyber-Attacks Network: Who's Attacking Whom

Sumeet Kumar, Kathleen M. Carley
Carnegie Mellon University
5000 Forbes Ave, Pittsburgh, PA 15213, USA
Email: {sumeetku@cmu.edu, kathleen.carley@cs.cmu.edu}

***Abstract*—Cyber-attacks aimed at breaking into networks and bringing websites down appear to have become an every-day phenomenon, but there is less clarity on where the attacks come from and who are the top targets. We used DDoS attacks data shared by Arbor Networks, from June 2013 to Mar 2016, to understand the cyber-attacks network. We take a high-level view of attacks mostly considering aggregate country-to-country attacks, using which we summarize the major players and trends in DDoS cyber-attacks.**

I. INTRODUCTION

There is a general belief that cyber attacks are increasing, and cost billions of dollars. While multiple studies suggest that cyber-attacks are pervasive and vary in type, little is known about the overall global picture. We use DDoS attacks data to visualize global attacks and discover patterns in cyber-attacks e.g. Which countries are the top targets? Which countries attack the most? Are attacks increasing or decreasing?

II. METHODOLOGY

We built our dataset using Arbor Networks ddos-attacks data shared on the website www.digitalattackmap.com, which shares top 2% of global attacks identified by Arbor Networks global treat monitoring system. The dataset starts from May 2013 and new data gets added daily. For this analysis, we used data till March 2016. Using the dataset, we build a time-series network, where the network comprises of country-to-country attacks. This enables us to visualize the attacks-received network and attacks-sent network, as well as do a trend analysis. Note that the source country information is available only for around one-third of the total attacks.

III. RESULTS AND CONCLUSIONS

Based on attacks analysis using data from June 2013 to March 2016, we summarize the top results below and, in tables 1 and 2.

1. The USA was the top target of DDoS attacks. The USA received 23832 attacks, followed by China (10670 attacks), Peru (3530 attacks), France (3270 attacks) and Canada (3043 attacks).

2. The majority of attacks originated from China (27.4%). China was responsible for a total of 20,443 attacks followed by the USA (20356), Netherlands (5436), Germany (2695), Korea (2122) and Brazil (1926).

3. The average number of DDoS Attacks per day on the USA saw a decrease from 2014 (108.5) to 2015 (54.6). In contrast, attacks on some European countries like France have increased 2014 (17.5), 2015 (22.8) to 2016 (43.08).

4. Attacks originating from the USA, China, Netherlands, and Germany have decreased over years (2013 to 2016). However, attacks from some other attacking countries like South Korea, Brazil, UK, and Russia have remained stable.

5. Attacks statistics for the top ten attackers and the top ten targets are presented in tables 1 and 2.

Table 1: DDoS Attacks: Summary of the Top Targeted countries based on ddos-attacks data from June 2013 to March 2016

Top 10 Targets	Top 5 Attackers of the Target country	Mean Inter-arrival time (minutes)	Bandwidth of Attacks (Gbps) (mean, std dev, min, max)	Number of Attacks received per day (mean, std dev, min, max)
US	CN, US, TR, NL, DE	26	19 , 24 , 0 , 320	74 , 64 , 0 , 399
CN	CN, NL, US, DE, SE	93	12 , 15 , 0 , 255	18, 22 , 0 , 237
PE	US, AR, PE, CO, LU	243	19 , 32 , 0 , 321	6 , 17 , 0 , 157
FR	CN, US, FR, DE, RU	125	19 , 21 , 0 , 295	20 , 19 , 0 , 144
CA	CN, US, CA, RU, KR	272	18 , 19 , 0 , 308	10 , 14 , 0 , 123
PL	US, PL, DE, NL, CN	436	16 , 18 , 0 , 253	4 , 11 , 0 , 104
GB	US, GB, CN, NL, RU	205	21 , 25 , 0 , 313	9 , 11 , 0 , 100
BR	BR, US, NL, CN, DE	329	6 , 10 , 0 , 219	6 , 7 , 0 , 72
DE	CN, US, DE, TH, JP	380	14 , 18 , 0 , 267	5 , 12 , 0 , 218
KR	KR, US, CN, BR, JP	641	10 , 11 , 0 , 113	3 , 6 , 0 , 86

Table 2: DDoS Attacks: Summary of the Top Attacking Countries based on ddos-attacks data from June 2013 to March 2016

Top 10 Attacking Country Code	Top 5 country attacked by the attacking country	Mean Inter-departure time (min)	Bandwidth of Attacks (Gbps) (mean, std dev, min, max)	Number of Attacks sent per day (mean, std dev, min, max)
CN	US, CN, CA, FR, DE	84	10 , 13 , 0 , 303	21 , 24 , 0 , 217
US	US, PL, CN, PE, GB	84	16 , 26 , 0 , 320	22 , 19 , 0 , 146
NL	CN, US, TH, GB, AU	286	7 , 14 , 0 , 240	5 , 12 , 0 , 161
DE	US, CN, FR, PL, RO	635	11 , 18 , 0 , 301	2 , 5 , 0 , 89
KR	KR, US, CN, FR, CA	889	6 , 10 , 0 , 96	2 , 4 , 0 , 81
BR	BR, US, FR, CN, CA	844	10 , 12 , 0 , 219	2 , 3 , 0 , 50
GB	GB, US, FR, CN, PL	1297	16 , 23 , 0 , 242	1 , 2 , 0 , 31
RU	US, FR, CN, GB, CA	1389	14 , 19 , 0 , 260	1 , 2 , 0 , 29
FR	FR, US, CN, GB, PE	1357	11 , 19 , 0 , 254	1 , 2 , 0 , 32
TR	US, CN, TR, FR, HK	902	5 , 14 , 0 , 302	1 , 10 , 0 , 185

IV. ACKNOWLEDGMENTS

This work was supported by the NSA under Award No. H9823014C0140 and CASOS at CMU. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the National Security Agency or the U.S. government.