University of CINCINNATI

IT7021: ENTERPRISE SECURITY AND FORENSICS

EXAMINING ADVERSARY COMMAND AND CONTROL SERVERS USING THREAT INTELLIGENCE

SUBMITTED BY:

MOHAN RAJESH PENKEY
GANESH BABU ATHOTA

SUBMITTED TO:
DR. CHENGCHENG LI PhD

SEMESTER: FALL YEAR:2023

Abstract:

Social networking sites such as Twitter can also be used to acquire information about threats. Nevertheless, the knowledge must be provided in perspective to be beneficial. For obtaining threat information from internet-based reports, data which can be analyzed, evaluated, validated, and situated is necessary. A hacker or online criminal uses a control-and-control server to send commands to malicious software-infected machines and to collect stolen information through the network being targeted. Botnet monitoring is critical to preventing future harm. We address this issue through tracking control and command (C2) communication traffic statistics, which discloses the botnet's architecture while it causes significant harm. That may be observed, C2 communication maintains an established routine. Conventional C&C server detection tactics include private IP addresses, Net infrastructures, and independent apps/services. From a different angle, social networking sites such as Twitter could be used as an instrument of knowledge.

Introduction:

A command-and-control server commands all machines infected with its malicious element, transforming them into automated bots thus transforming the whole network through a botnet. If equipment becomes infected with ransomware and is not well-protected, it can become a bot: Threat actors frequently send malicious files or URLs via email communications. Whenever malware is downloaded or clicked on, it gets installed on the computer right away, transforming it into a bot. Risks have been taken advantage of. Exploiting an opening is one frequent approach for taking authority over an organization. If security professionals concentrate on reducing connection with control-and-control nodes, an infection with malware can be effectively stopped. It is impossible to avoid spyware from infiltrating a company since users would surely open a file attached to an email or hyperlink, leading to contamination. Cybersecurity and spyware identification systems that utilize signatures are just part-effective. Security efforts should focus on preventing infection from communicating to the control-and-control network to snap the web of destruction.

Attackers may gain control and access to a piece of equipment by using extensions, upgrades, and software that has not been updated. As the World Wide Web has developed and connectivity evolved, so have P2P applications, web searching engine (WSE) solutions, and other innovative apps. Alternate app types, including social media sites on the internet (OSN) and internet communication, have arisen, and gained in popularity, especially as handheld equipment/smartphones become more frequently used. All those apps/services expand the scope of C&C server growth, resulting in a plethora of C&C server-finding tactics for bots. As mobile technology for computers has grown, handheld devices (such as smartphones and laptops) have provided sophisticated features at lower costs. Because their computational capacities are increasing and they remain connected to the World Wide Web via Wi-Fi or cell phone networks, cell phones have become frequent targets for attackers attempting to build up cellular botnets that are (X. Guo, 2016 p1723-1727).

Malicious hackers created new avenues in which to flourish by exploiting the web's enormous supply of spare power for computation and bandwidth on the network. Considering many investigations, different kinds of Botnet topologies, C2 guidelines, and connectivity-based strategies were developed to oppose Botnet discoveries. And, over the past ten years, these technologies have evolved to the point that they can now identify new undiscovered Botnets (G. Vormayr, 2017). The method begins by detecting all the common phrases in the information being analyzed. A rating mechanism is then used to assign high scores to the traffic-class distinguishing phrases. They are likely genuine C&C initials. This is because botnet C&C links, or botnet orders, show internet-level similarities, whereas non-C&C traffic appears to be more diverse. Our solution has been evaluated using data from an evolving malware detection platform. We also showed that our method is far more precise than Signature. Its C&C signatures were also compared to Bot Hunter and Snort detecting precision. The entire system investigated around 2.6 billion linkages produced by over 1.4 million data. A rating mechanism is then used to assign high scores to the traffic-class distinguishing phrases. The findings show that our method applies in the real world and allows for important C&C signals (Ali Zand, 2014). Botnet identification is now the primary objective of current studies. Numerous investigators have been working diligently to develop effective ways for identifying Botnets. Others wish to investigate Botnet behavior via network communication monitoring. They accomplish this by interconnecting many data sets in order to anticipate whether the network is acceptable to operate. However, they frequently run into issues because of a lack of significant data, making forecasting information problematic. Furthermore, it is not fair to protect and acquire information from several Botnets, as this will degrade the efficiency of deep learning techniques (Alothman, 2017).

DDoS assaults, the illegal acquisition of important data, unwanted content, and other forms of cybercrime represent just a few instances. Peer-to-peer botnets (P2P) are another sort of distributed spyware that runs outside the user's knowledge. Scientists are increasingly combining methods for data mining, such as neural communication, with methods from strategies learning to discover Botnets. (S. Chen, 2018)

Twitter threat analysis:

The raw information can be retrieved via a variety of different techniques. Several freely available intel instruments in addition to openly accessible Twitter streamed applications programming interfaces (API) for harvesting material (e.g., TWINT). A different strategy would be to delve further into current records, like those utilized in a Five Thirty-Eight analysis of troll tweets. Twitter and researchers have suggested various spamming filters to protect consumers. The detection of Twitter spam methods is divided into two categories: automatic gets closer, such as deep learning, and quasi-automated gets more intimate, which requires human interaction. There are numerous techniques for analysis.

- Tactical Threat Analysis
- Technical Threat Analysis
- Operation Threat Analysis

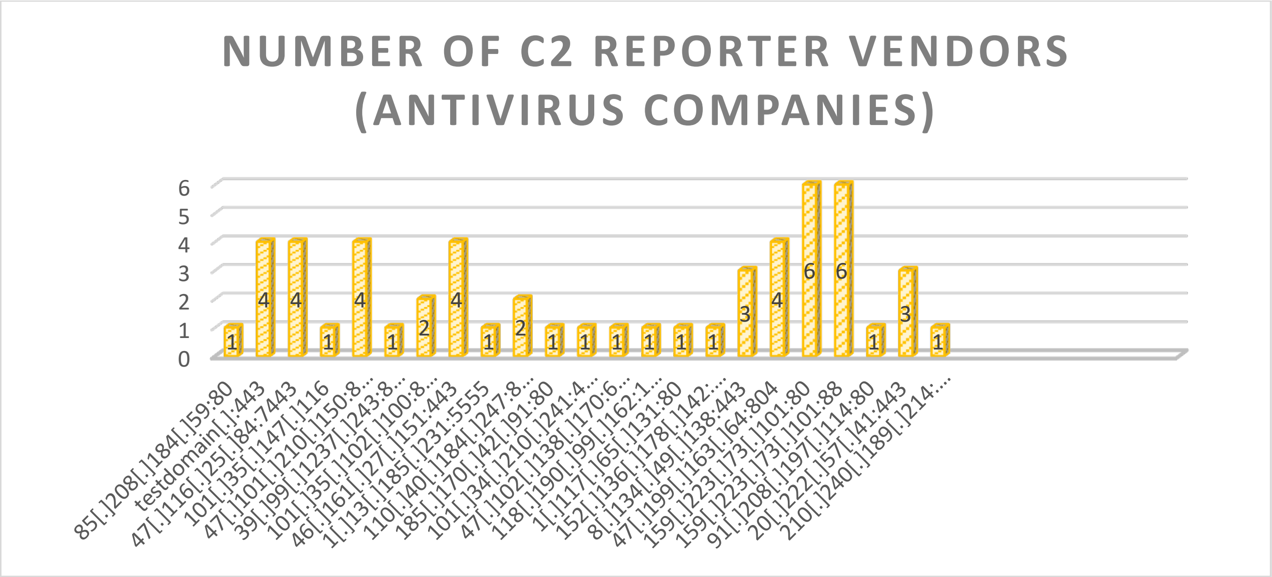
Data Analysis (Dataset):

Information was gathered from intelligence agencies using the Twitter account @drb_ra. As a component of the information gathering, we obtained 72 controlling and command Server information from the Twitter account

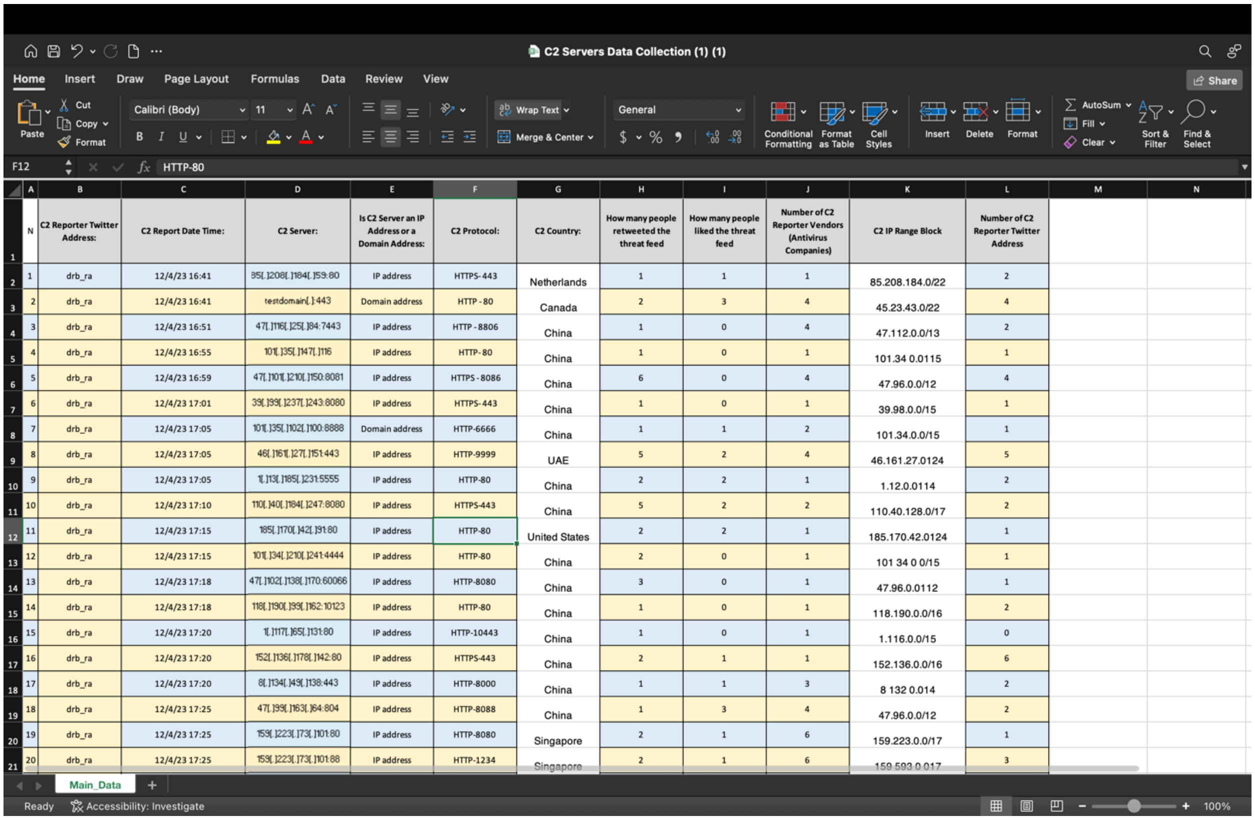
Absolutely nothing is specifically stated. Just three of the total 72 IP addresses have been utilized a couple of times with the others being utilized just once.

In this section, we examine the acquired data and generate insights to present our responses to the study questions. Every inquiry is answered in depth below:

1) **Are there any specific IP ranges used to create malicious C2 servers**



There appears to be widespread use of IP addresses for C2 servers. C2 servers headquartered in China were particularly used.

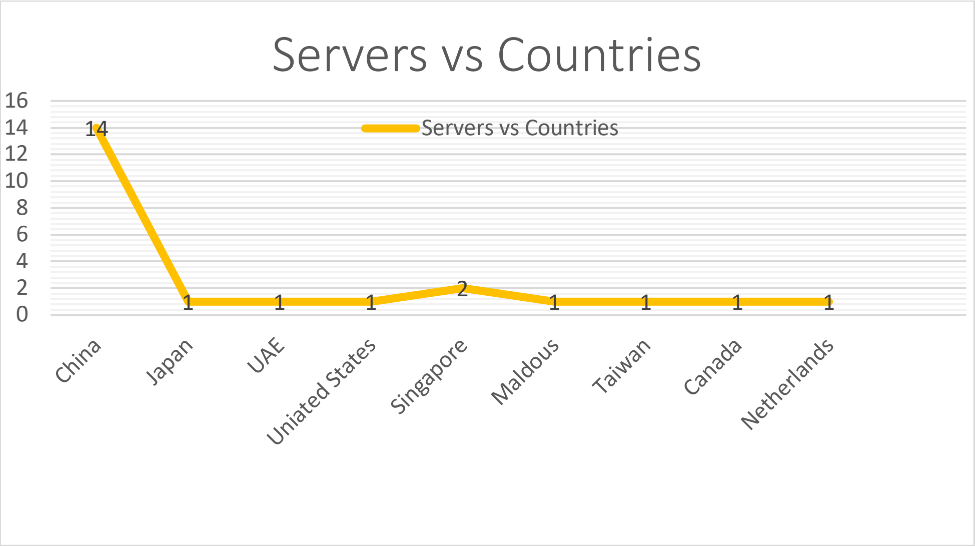


C2 Servers Data Collection (1) (1)

F12 HTTP-80

N	C2 Reporter Twitter Address:	C2 Report Date Time:	C2 Server:	Is C2 Server an IP Address or a Domain Address:	C2 Protocol:	C2 Country:	How many people retweeted the threat feed	How many people liked the threat feed	Number of C2 Reporter Vendors (Antivirus Companies)	C2 IP Range Block	Number of C2 Reporter Twitter Address
1	drb_ra	12/4/23 16:41	85[.]208[.]184[.]59:80	IP address	HTTPS- 443	Netherlands	1	1	1	85.208.184.0/22	2
2	drb_ra	12/4/23 16:41	testdomain[.]:443	Domain address	HTTP - 80	Canada	2	3	4	45.23.43.0/22	4
3	drb_ra	12/4/23 16:51	47[.]116[.]25[.]84:7443	IP address	HTTP - 8806	China	1	0	4	47.112.0.0/13	2
4	drb_ra	12/4/23 16:55	101[.]35[.]147[.]116	IP address	HTTP- 80	China	1	0	1	101.34 0.0115	1
5	drb_ra	12/4/23 16:59	47[.]101[.]210[.]150:8081	IP address	HTTPS - 8086	China	6	0	4	47.96.0.0/12	4
6	drb_ra	12/4/23 17:01	39[.]99[.]237[.]243:8080	IP address	HTTPS- 443	China	1	0	1	39.98.0.0/15	1
7	drb_ra	12/4/23 17:05	101[.]35[.]102[.]100:8888	Domain address	HTTP-6666	China	1	1	2	101.34.0.0/15	1
8	drb_ra	12/4/23 17:05	46[.]161[.]27[.]151:443	IP address	HTTP-9999	UAE	5	2	4	46.161.27.0124	5
9	drb_ra	12/4/23 17:05	1[.]13[.]185[.]231:5555	IP address	HTTP-80	China	2	2	1	1.12.0.0114	2
10	drb_ra	12/4/23 17:10	110[.]40[.]184[.]247:8080	IP address	HTTPS-443	China	5	2	2	110.40.128.0/17	2
11	drb_ra	12/4/23 17:15	185[.]170[.]42[.]91:80	IP address	HTTP-80	United States	2	2	1	185.170.42.0124	1
12	drb_ra	12/4/23 17:15	101[.]34[.]210[.]241:4444	IP address	HTTP-80	China	2	0	1	101 34 0 0/15	1
13	drb_ra	12/4/23 17:18	47[.]102[.]138[.]170:60066	IP address	HTTP-8080	China	3	0	1	47.96.0.0112	1
14	drb_ra	12/4/23 17:18	118[.]190[.]99[.]162:10123	IP address	HTTP-80	China	1	0	1	118.190.0.0/16	2
15	drb_ra	12/4/23 17:20	1[.]117[.]65[.]131:80	IP address	HTTP-10443	China	1	0	1	1.116.0.0/15	0
16	drb_ra	12/4/23 17:20	152[.]136[.]178[.]142:80	IP address	HTTPS-443	China	2	1	1	152.136.0.0/16	6
17	drb_ra	12/4/23 17:20	8[.]134[.]49[.]138:443	IP address	HTTP-8000	China	1	1	3	8 132 0.014	2
18	drb_ra	12/4/23 17:25	47[.]99[.]163[.]64:804	IP address	HTTP-8088	China	1	3	4	47.96.0.0/12	2
19	drb_ra	12/4/23 17:25	159[.]223[.]73[.]101:80	IP address	HTTP-8080	Singapore	2	1	6	159.223.0.0/17	1
20	drb_ra	12/4/23 17:25	159[.]223[.]73[.]101:88	IP address	HTTP-1234	Singapore	2	1	6	159.593 0.017	3

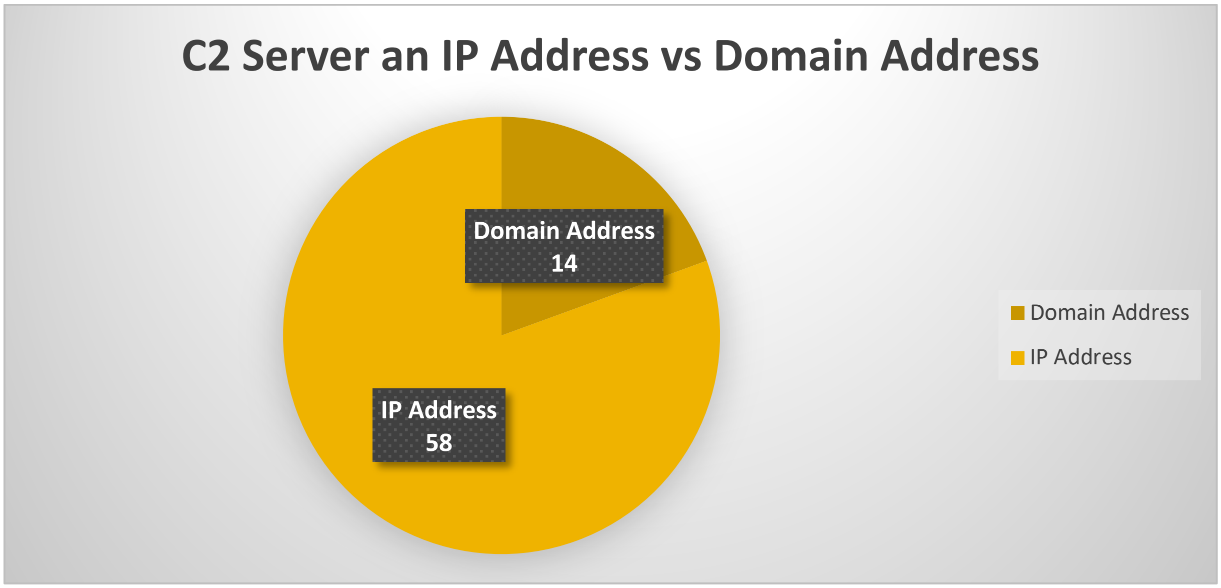
2) Which are the most typical IP zones/countries for creating C2 servers?



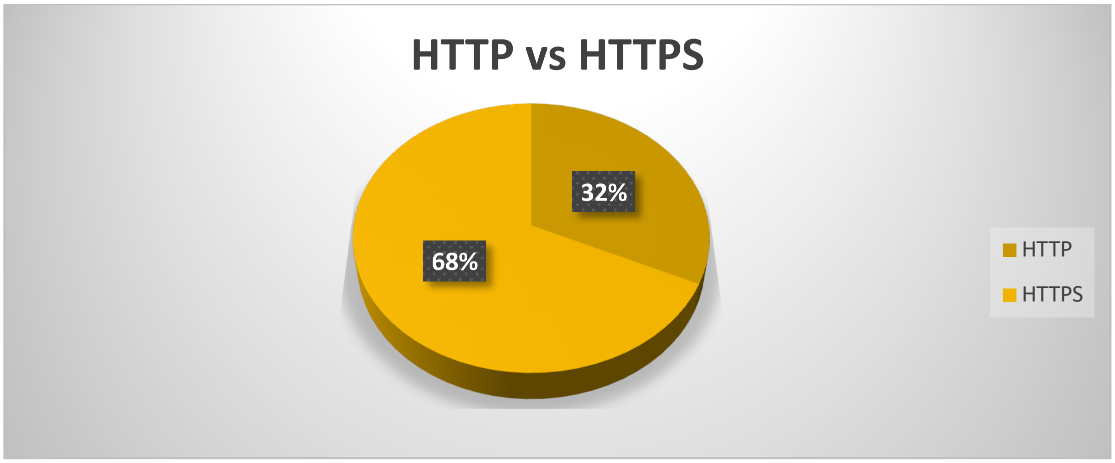
China and Singapore are the greatest offenders, with China being among being dominant in hosting or claiming to be hosting C2 servers.

3) **Will the C2 servers be IP or domain-based? What constitutes the costs.?**

There are 58 (80.5%) IP addresses and 14 (19.5%) domain addresses.



4) **Were the C2 servers configured to use the HTTP (80) or HTTPS (443) protocols?**



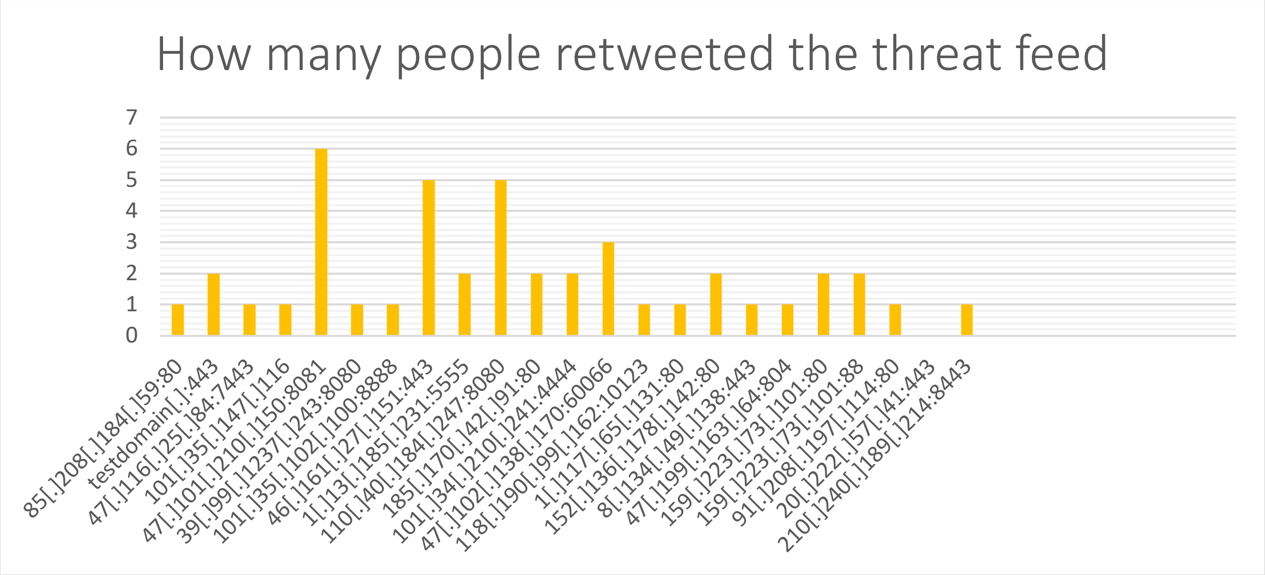
PORT	NUMBERS
HTTP - 80	27
HTTP- 443	45
TOTAL	72

Out of the 72 tweets, 27 were HTTP with approximately 32% on the other hand 45 are HTTPS protocols with 68% placements

5) **Based on VirusTotal.com statistics, were the C2 servers already discovered by antivirus suppliers?**

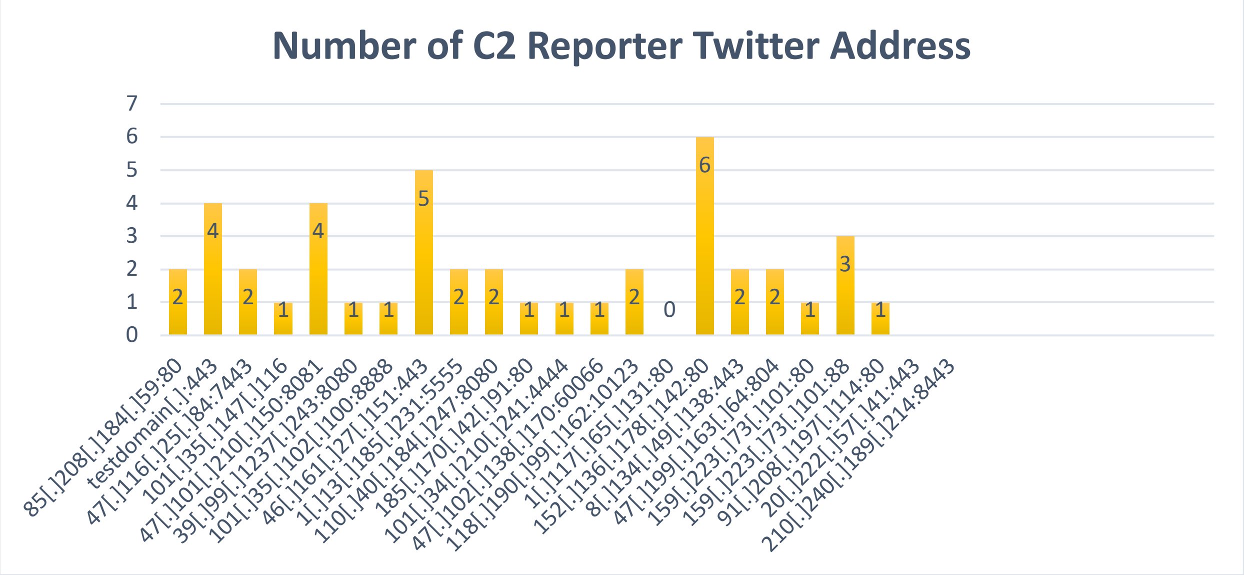
It was discovered that every single one of the c2 servers was malignant.

6) **What percentage of people like and tweet back threat keeps feeding?**



The most retweets were for 47[.]101[.]210[.]150[.]88081 with six, followed by 110[.]40[.]185[.]247:8080 & 46[.]161[.]27[.]151:443 with five retweets is in second place, next to the remaining servers.

7) Were the C2 server and the other accounts on Twitter mentioned?



The "drb_ra" account on Twitter claimed almost all the C2 servers that were included in the information set, plus some additional C2 servers claimed through different Twitter accounts as well. Much is understood regarding the other Twitter accounts purporting to be from the exact same C2 servers.

8) Is there any resemblance between C2 servers?

Indeed, according to in the statistics, many internet protocol addresses had a connection with other harmful IP addresses in a brief region. It's uncertain whether these constituted malware networks or merely an ensemble of C2 servers, but they suggest there are multiple IP addresses for more than a single server.

Conclusion and Discussion

What conclusions were made?

Everything was dismantled. Just a few of the 72 IP addresses were utilized twice, and the rest were utilized once. According to the visual facts, China has the most workstations The eleventh American country follows Singapore, Japan, and the Netherlands. Internet Protocol (IP) addresses are used by 80.5 percent of C2 servers, whereas domain addresses are used by 19.5 percent. The HTTP (80) and HTTPS (443) protocols are used by almost all of C2 hosts Additional HTTP and HTTPS protocol codes are in circulation.

Which are the intriguing outcomes?

According to the data set I gathered, the outcomes for two among the 72 C2 sites have been overlooked by any antivirus vendor.

We identified significant similarities between C2 servers that use HTTP or HTTPS, which happens to be the way most C2 services operate in bigger systems, as well as those that use IP domains, and antivirus vendors imply.

How this research can be improved?

The numbers form the present investigation may be enhanced by expanding the search field to encompass novel risks that might have connections to C2 or additional networks, as well as collecting details from various Twitter feeds and evaluating unprocessed data from an array of locations.

Whatever are the findings of the study boundaries?

The data form the profile on Twitter paints a picture of where attacks on C2 services originate from in general; at the bottom of the tower were C2 servers with inadequate location data as well as others which. Content produced by users, on the other hand, is frequently brief, inaccurate, and unorganized. As a result, programs to acquire immediate accessibility to the information they need.

What exactly are the implications of future studies?

The next research may concentrate on gathering information regarding cyber dangers from businesses, freely accessible sources, and public security firms. Future research on live malware networks could focus on oneself, dangerous live bot research. Future study may aid malware detection tools for usage in real life by offering particular signs (heuristics) while an identical install an unexpected group of connected bots Internet.

What are the recommendations?

According to a particularly recent study presented in this work, I can state that, despite significant advances in our comprehension of network leadership techniques and the C2 infrastructure that support them, hackers have maintained the advantage.

Unexpected parallels between C2 servers?

Everything was actually lost. Just three of the 72 IP ranges were used twice; the remainder were utilized only individually. China possesses the largest systems as a whole according to the above statistical numbers obtained by means of data collection (28). Protocol numbers for HTTP and HTTPS were recently added. Except for three, the remaining 72 IP addresses were all utilized on one occasion. These data-driven graphics reveal that China possesses the most workstations. 80.5 percent of C2 servers use IP addresses for communication, while 19.5 percent use domains. C2 servers commonly employ the HTTP (80) and HTTPS (443) technologies. HTTP and HTTPS protocol identifiers are also utilized.

Bibliography

A Menon. (2019). Thwarting C2 Communication of DGA-Based Malware using Process-level DNS Traffic Tracking. 7th International Symposium on Digital Forensics and Security (ISDFS), 1-5.

Ali Zand, G. V. (2013). Extracting probable command and control signatures for detecting botnets. In Proceedings of the 29th Annual ACM Symposium on Applied Computing (SAC '14).

Alothman, B. &. (2015). Towards using transfer learning for botnet detection. International Conference for Internet Technology and Secured Transactions (ICITST), , 281-282.

F. Benevenuto , G. M. (2011). Detecting spammers on Twitter. Detecting spammers on twitter," in Collaboration, electronic messaging, anti-abuse, and spam conference (CEAS), vol. 6, 12.

G. Vormayr, T. Z. (2017). Botnet Communication Patternr ," in IEEE Communications Surveys & Tutorials. IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2768-2796.

K. Xu, P. R. (2014). DNS for Massive-Scale Command and Control. DNS for Massive-Scale Command and Control," in IEEE Transactions on Dependable and Secure Computing, 143-153.

N. Känzig, R. N. (2017). Machine Learninǵ-based Detection of C&C Channels with a Focus on the Locked Shields Cyber Defense Exercise. 2019 11th International Conference on Cyber Conflict (CyCon), 1-19.