**“Examining Adversary Command and Control Servers using Twitter Threat Intelligence Sources”**   
Abhiram Pasaladi, Jayadeep Mallela, Shivani Korimi, Sai Krishna Sayempu  
 IT 7021C: Enterprise Security and Forensics University of Cincinnati

Abstract:

Threat actors continue to exploit Command and Control (C2) servers as powerful tools to execute malicious activities, posing significant risks to individuals, organizations, and critical infrastructure worldwide. This paper investigates the methods, techniques, and procedures used by adversaries to set up, operate, and obfuscate C2 servers. By leveraging the vast amount of information shared on Twitter as a source of threat intelligence, we aim to uncover insights into C2 infrastructure. Our methodology involves collecting and analyzing real-time conversations, indicators of compromise (IOCs), and other relevant data from Twitter accounts dedicated to sharing cyber threat information. Through this approach, we examine 60 C2 servers, focusing on aspects such as IP ranges, geographic locations, protocols, and detection by antivirus vendors. Our findings reveal that IP ranges like 198.13.32.0/19 and countries like Japan, China, and the United States are commonly involved in hosting malicious C2 servers. Additionally, both IP addresses and domain names are utilized, with a preference for HTTPS (443) protocol for encrypted communication. We conclude that continuously monitoring social media platforms and collaborating among cybersecurity stakeholders are crucial for staying vigilant against evolving C2 server activities and enhancing defensive strategies.

Introduction:

The continuous rise in cyber threats has become one of the most difficulty challenges in the modern digital era, posing some great risks to the individuals, organizations, and critical infrastructure all over the world [3]. In the middle of these malicious activities lies the exploitation of Command-and-control (C2) servers by many well-known threat actors [1]. These servers mainly function as the central communication hubs which enable the attackers to execute any type of commands on the compromised systems within any environment [6]. Also allowing the theft of data, the use of viruses, and many other criminal acts can take place within a compromised environment. The Colonial Pipeline and Equifax hacks serve as the important remainders of the catastrophic consequences which can come when the threat actors gain access to some unauthorized data through the C2 servers highlighting how important and urgent it is to deal with this serious problem [7].

The issue of C2 servers is very important because threat actors are still using them as one of the most powerful and important tools which serves them as their toolkit to commit hacking and operations that cause serious problems [1]. A lot of attackers use these sites because they make it easy to plan and perform some difficult attacks, steal private data and keep access to systems that have been hacked [6]. Even though this is a very important problem which has caused a lot of damage to a lot of groups and countries, there is not a lot of research that has been done in detail about C2 servers and how they work [2]. Currently in the present time studies have not completely shown the complicated nature of these activities, which is making it difficult for them to come up with more efficient ways to identify the problem and protect against the growing risks [8].

Our paper aims to contribute to the literature by using the huge amount of information shared on Twitter, taking that as a source of threat intelligence to know more about other C2 servers [5]. By observing the real-time changes, conversations, and indicators of compromise (IOCs) about C2 infrastructure, it is possible to learn a lot about the methods, techniques, and procedures that threat actors can use to set up and run, also hide the servers [4].

It is very important to address the C2 server problem because attackers are constantly evolving and coming up with new strategies, taking advantage of new vulnerabilities, and devising new ways to avoid detection and circumvent defenses [6]. There is an immediate need to learn more about their operations, especially when it comes to C2 infrastructure, which is a crucial part of their attack procedures [4]. Researchers and security experts can gain insight into these attackers' goals, targets, and methods by examining the C2 servers they typically use [9]. This may assist them in developing more effective defenses. There have been many studies that consider Twitter as a source of threat intelligence, but this approach has not been extensively applied to the analysis of C2 servers [5].

Existing research has mostly discussed using Twitter to gather general threat information or monitor specific types of threats such as malware campaigns, phishing attacks, or distributed denial-of-service (DDoS) events [5]. However, this tool has not been utilized to fully understand C2 computers and the associated activities [10]. By examining C2 servers and leveraging information on Twitter, this paper seeks to fill the gaps in the existing literature and provide a comprehensive understanding of this critical aspect of cybersecurity [4]. Furthermore, this study aims to demonstrate the significance of utilizing open-source intelligence (OSINT) and social media platforms as reliable sources of threat intelligence, potentially helping security professionals and researchers to stay ahead of emerging cyber threats.

Data Collection:

Research on C2 servers, which was conducted by Twitter, using information-sharing accounts that are specifically qualified to provide information related to cyber threats and their consequences. The account "@drb\_ra" was an automate feed that ran to collect data that prevented accidental clicks. Every tweet with C2 server addresses were collected and stored for future analysis. These addresses along with timestamps and the rest of the data about the servers, were put into an Excel sheet. It was done systematically expecting to achieve a well arranged set of data all for analysis. Every single piece of significant information was carefully entered.

To make 100% sure of data reliability, the address of each C2 server was crosschecked using VirusTotal which is known for its detailed security analysis. This was performed to check if these addresses had been reported by the security community as already malicious. Following the validating, all the information was then processed in different ways: the duplicates were removed and data was sorted according to the type of the address (IP or domain) and the location of the server.

The below given table has the total number of 60 C2 servers , where the columns were labeled whether they are IP address or the domain address. Through the following simple act, we were able to discover that the IP addresses were more common and totalled 35 while the domain addresses amounted to 25. The realization of this difference is important in developing methods for resisting cyber criminals and in securing the cyber space. This huge number of C2 servers analyzed shows that a significant amount of work was put into covering nearly every important element of the C2 server activity type in the study.

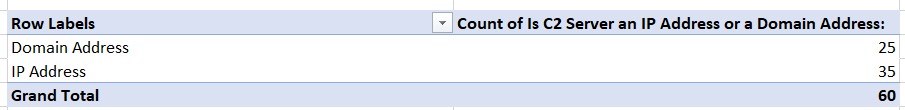


Fig 1: Shows the count of C2 servers' IP or domain addresses.

The data shown in the related picture clearly shows that most of the servers that were examined and recorded were identified by their IP addresses. The study shows that the C2IntelFeedsBot account on Twitter regularly shares updates, primarily related to IP address-based servers.

A pie chart with text and numbers

Description automatically generated

Fig 2: Shows the count of IP/Domain Address in Percentage.

Data Examination and Results:

1) Are there any specific IP ranges used to create malicious C2 servers:  
From the collected data of drb\_ra source, the number of IP ranges used for creating malicious C2 servers are 49. Among these 49, 198.13.32.0/19 IP range was used the most, which is 4 times and the IP ranges 119.3.0.0/16, 43.136.0.0/13, 149.28.128.0/17, 43.156.0.0/15, 162.244.80.0/22, 38.27.163.0/24, 45.32.0.0/16, 35.72.0.0/13 are used by 2 C2 servers each and the remaining servers are with 1 value.

A graph with numbers and a bar

Description automatically generated

Fig 3: Shows the count of IP ranges used for C2 servers.

2) What are the common IP regions/countries used to create C2 servers:  
Out of the sixty collected c2 server dataset, there are 11 countries involved in it, where most of the C2 servers are from Japan valuing to 19, next comes China with 12 C2 servers and next comes the United States with 11 counts. Remaining all countries like Canada, Germany, Hong Kong, Singapore, United Kingdom, Turkey, Poland and Lithuania constitute to less than 10 values. The order of the common regions involved in C2 servers' creation is shown below.

A pie chart with numbers and text

Description automatically generated

Fig 4: Shows the countries used to create C2 servers.

3) Are the C2 servers run on IP or domain? What are the rates?

The C2 server data set consists of 60 servers running on both domain address and IP address. Out of these 60, 25 C2 servers are running on 25 Domain Addresses and the remaining 35 are from IP Addresses. Calculating the values in percentages, 58% is coming from IP Address and 42% coming from the Domain Address as shown in below charts.  
  
A screenshot of a computer

Description automatically generated

Fig 5: Shows the count of IP/Domain Address in Percentage.

4) Are the C2 servers run on HTTP (80) or HTTPS (443) protocols?  
C2 servers run on both HTTP (80) and HTTPS (443) protocols. Most of the servers run on HTTPS (443) and HTTP (80) occupies the second position as shown in the charts below.

A pie chart with numbers and a number of different colors

Description automatically generated with medium confidence

Fig 6: Shows the percentage of protocols used in C2 server.

5) Were the C2 servers already detected by antivirus vendors based on VirusTotal.com results?

According to the results of VirusTotal.com, The C2 servers were already detected by the antivirus vendors and the 162[.]244[.]80[.]235:80 C2 server was detected 26 times followed by 43[.]156[.]150[.]242:2096 for 14 times. 154[.]88[.]24[.]89:53 and 117[.]50[.]163[.]113:8443 were detected by 11 vendors. 38[.]27[.]163[.]244:8443 was detected by 10 vendors and all the remaining ones are detected by less than 10 vendors.

A graph with blue and black lines

Description automatically generated

Fig 7: Shows the total of each C2 servers’ detection by antivirus vendors at VirusTotal.com.

6) How many people do like and retweet threat feeds?

Retweet Results:  
 A total of 125 people retweeted the threat feeds. Most of the retweets were on the C2 servers from Singapore and United States with 39 retweets in total. Japan takes the second place.   
 A screenshot of a computer

Description automatically generated

Fig 8: Shows the total of retweets in twitter threat feeds for each C2 server region.

LikeResults:  
A total of 333 Likes were given to all threat feeds. Most of the likes were given to the Japan C2 Server tweets and Singapore, United States occupy the second place with 78 likes.

A screenshot of a computer

Description automatically generated

Fig 9: Shows the total of likes in twitter threat feeds for each C2 server region.

7) Were the C2 server reported with the other Twitter accounts?  
 All of the C2 servers were reported with other Twitter accounts with most being 82[.]157[.]110[.]128:80 reported by 7 Twitter accounts. Followed by 84[.]32[.]188[.]210:443, 104[.]41[.]174[.]165:80, 34[.]85[.]102[.]18:8889 being reported by 4 accounts and the remaining ones were all less than 4.

A graph with numbers and lines

Description automatically generated

Fig 10: Shows the total of C2 server Twitter Address Reporting for each C2 server.

8) Are there any similarities among C2 servers?

Considering the similarities in IP region, most of the C2 servers are from Japan region with 32% rate and the second most are from the China constituting to the 20% of total. Next comes the United States with 18%. Considering the similarities in IP or Domain Address, 35 are IP Addresses and the remaining 25 are Domain Addresses. Considering the similarities in protocols, most of the C2 servers used protocol is HTTP (443) contributing to 28% of the total, HTTP (80) contributing to 15% of the total C2 servers' protocol.

Conclusion:

The above research in Command and Control (C2) servers revealed important findings by considering 60 C2 servers from drb\_ra source. Firstly, the IP range 198.13.32.0/19, was most used for creating malicious C2 servers. Also, most of these C2 servers are from Japan, followed by China and the United States. More interestingly, both domain and IP addresses were used, with IP addresses being the most. Additionally, Both HTTP and HTTPS protocols were used, with HTTPS (443) used the most, which shows that C2 servers prefer using encrypted communication. To enhance research further, it would be beneficial to use more data sources and advanced analytics. However, it is also important to acknowledge limitations, like preferring only specific data sources. Considering the future research scope, doing research using the relationship between C2 infrastructure and Malware families could provide important insights. Recommendations would include ongoing alertness against C2 activities and collaborating among Cybersecurity stakeholders. Remarkable similarity would be that the Japan came up as a main branch for C2 server activity, with most of the HTTPS protocol usage.

References:

[1] S. Yamaguchi, "A Basic Command and Control Strategy in Botnet Defense System," 2021 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2021, pp. 1-5, doi: 10.1109/ICCE50685.2021.9427667.

[2] A. Sidhardhan, K. S and J. M. Kannimoola, "Weaponizing Real-world Applications as C2 (Command and Control)," 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023, pp. 458-463, doi: 10.1109/ICIDCA56705.2023.10100279.

[3] X. Wang, K. Zheng, X. Niu, B. Wu and C. Wu, "Detection of command and control in advanced persistent threat based on independent access," 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016, pp. 1-6, doi: 10.1109/ICC.2016.7511197.

[4] M. Carvalho et al., "MTC2: A command and control framework for moving target defense and cyber resilience," 2013 6th International Symposium on Resilient Control Systems (ISRCS), San Francisco, CA, USA, 2013, pp. 175-180, doi: 10.1109/ISRCS.2013.6623772.

[5] Jun Zhao, Qiben Yan, Jianxin Li, Minglai Shao, Zuti He, Bo Li. TIMiner: Automatically Extracting and Analyzing Categorized Cyber Threat Intelligence from Social Data: 2020. <https://doi.org/10.1016/j.cose.2020.101867>

[6] H. R. Zeidanloo and A. A. Manaf, "Botnet Command and Control Mechanisms," 2009 Second International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 2009, pp. 564-568, doi: 10.1109/ICCEE.2009.151

[7] D. T. Vollmer and M. Manic, "Human interface for cyber security anomaly detection systems," 2009 2nd Conference on Human System Interactions, Catania, Italy, 2009, pp. 654-659, doi: 10.1109/HSI.2009.5091055.

[8] E. Coyne and T. Weil, "An RBAC Implementation and Interoperability Standard: The INCITS Cyber Security 1.1 Model," in IEEE Security & Privacy, vol. 6, no. 1, pp. 84-87, Jan.-Feb. 2008, doi: 10.1109/MSP.2008.2.

[9] P. Beraud, A. Cruz, S. Hassell, J. Sandoval and J. J. Wiley, "Cyber defense Network Maneuver Commander," 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, San Jose, CA, USA, 2010, pp. 112-120, doi: 10.1109/CCST.2010.5678724.

[10] C. W. Johnson, "Tools and techniques for reporting and analysing the causes of cyber-security incidents in safety-critical systems," ​​9th IET International Conference on System Safety and Cyber Security (2014), Manchester, UK, 2014, pp. 1-7, doi: 10.1049/cp.2014.0975.