IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311008|

Examining Adversary Command and Control Servers using Twitter Threat Intelligence Sources

Tolulope Aremu, Favour Olusoji, Samson Arogundade

Graduate Student, School of Information Technology, University of Cincinnati, Ohio, United States

Graduate Student, Department of Computer Science, University of Dundee, United Kingdom

Manager, IT and Specialized Assurance, Deloitte Nigeria

ABSTRACT: This study investigates the patterns of Command and Control (C2) servers on Twitter, providing new insights on cyber-attacks. The analysis of data obtained from influential cybersecurity Twitter accounts reveals the specific IP ranges and protocols that cybercriminals like to use to avoid being detected. The study highlights the importance of Twitter in gathering information about cyber threats. It suggests that there is a lack of public involvement in this area and proposes the use of additional data sources to ensure thorough monitoring of threats. The research enhances comprehension of C2 server dynamics, emphasizing the significance of proactive protection tactics. Furthermore, it highlights the significance of social media in promoting cybersecurity awareness and the indispensability of real-time analytical tools. In summary, the results provide a framework for improving cybersecurity measures against ever-changing online risks.

KEYWORDS: Command and Control (C2) Servers, Cybersecurity, Twitter Threat Intelligence, IP Ranges, Cyber Threat Detection, Social Media Intelligence, OSINT (Open-Source Intelligence), Ransomware, Cyber-Attack Patterns, Malware Detection, IP Address Analysis, Protocol Usage, HTTP/HTTPS, Public Engagement, Social Media Analytics, Deep Learning, Machine Learning, Predictive Security, Cyber Defence Mechanisms, Proactive Cybersecurity.

I. INTRODUCTION

The utilization of Command and Control (C2) servers by malicious actors to remotely execute instructions within targeted systems is a widely documented and enduring problem in the realm of cybersecurity. The Colonial Pipeline and Equifax intrusions, among other notable cyber disasters, highlight the vital functions these servers provide in coordinating large-scale cyber-attacks, including the theft of data and the distribution of ransomware. C2 servers serve as central points for transmitting malicious commands to hacked systems, enabling the coordination of extensive networks of infected computers to carry out synchronized attacks that have the potential to paralyse infrastructures, pilfer critical data, and cause significant disruptions to both enterprises and governments.

The continuous utilization of C2 servers by malicious actors is not solely a technological matter, but rather a wide-ranging societal problem that impacts the security and economic prosperity of organizations and individuals worldwide. The utilization of C2 servers in recent years has resulted in substantial financial losses and operational interruptions due to ransomware attacks. As an illustration, the assault on Colonial Pipeline led to significant monetary damages and considerable scarcity of petroleum throughout the Eastern United States. Similarly, the Equifax hack exposed the personal information of millions of individuals, underscoring the significant repercussions of successful cyber assaults facilitated by C2 servers [1].

II. LITERATURE REVIEW

Although the problem is increasingly acknowledged, there is still a significant deficiency in cybersecurity research, namely in the study and comprehension of the mechanisms governing the functioning of C2 servers. The existing literature predominantly concentrates on identifying and minimizing malware and direct methods of attack, while giving less attention to the intricate examination of C2 server operations and the patterns they display during cyber-attacks [2]. This discrepancy highlights the necessity for more targeted research endeavours that not only identify but also scrutinize the conduct and communication patterns of C2 servers to gain a deeper comprehension of the strategies, methods, and protocols employed by cyber adversaries.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311008|

This research enhances the existing body of knowledge by using Twitter as an innovative source of threat intelligence to examine C2 server activity. This project attempts to analyse and document the communication and operational patterns of C2 servers by utilizing data gathered from Twitter. This technique not only improves the comprehension of how C2 servers operate within larger cyberattack frameworks but also assists in the creation of more efficient detection patterns and policy responses. The study will illustrate the utilization of Twitter for identifying emerging risks and monitoring the development of C2 server techniques in real-time. This will provide significant information that can guide the creation of defensive strategies.

Prior research has emphasized the capacity of Twitter to serve as a valuable resource of OSINT (Open-Source Intelligence) for cybersecurity objectives. Kokubun and Nakamura (2018) investigated the utilization of Twitter for spreading harmful URLs, frequently associated with C2 servers, highlighting the platform's significance in the realm of cyber threats [5]. Alves et al. (2019) developed a classification model for a real-time Twitter threat monitoring system, showcasing the effectiveness of the platform in sorting, and categorizing cybersecurity threat data [6]. In addition, Mittal et al. (2016) conducted research on Cybertwitter, demonstrating the potential of Twitter data in generating warnings for cybersecurity threats and vulnerabilities. This study established a fundamental framework that highlights the significance of social media in threat intelligence [7].

This research expands upon previous studies by particularly examining the operations of C2 servers using Twitter data. By doing so, it addresses a significant gap in the current body of work on threat intelligence derived from social media. The objective of this study is to offer in-depth understanding of the implementation and functioning of C2 servers, providing a fresh viewpoint on the dynamics of these crucial components in cyber-attack sequences.

III. METHODOLOGY

The information for this study was gathered from Twitter (now X), a site that has become an essential resource in the cybersecurity industry for exchanging up-to-date threat intelligence. Concretely, the data was collected from the subsequent Twitter accounts, recognized for their valuable input in the field of cybersecurity:

@drb_ra
@JAMESWT_MHT
@TheDFIRReport

These sources are renowned for providing current information on ongoing cyber threats, including specific information regarding command-and-control servers utilized in cyber-attacks. Every C2 address provided by these sources is carefully designed to minimize the possibility of accidental activation or security breaches. For example, C2 addresses are usually displayed with brackets that hide direct segments (e.g., 103[.]136[.]150[.]94:8080), thereby limiting inadvertent access during the handling and analysis of this data.

The dataset was compiled using a methodical process of gathering tweets that provided information about C2 servers. This included recording detailed details about their operational features and metadata, such as reporting dates, server type (IP address or domain), and geographical information. The main objective was to gather data that would offer a complete overview of the deployment and detection of C2 servers.

The dataset contains records for 60 distinct C2 servers, offering a substantial sample for a comprehensive study. The current sample size is sufficient to detect and analyse trends and patterns in the usage and detection of C2 servers. This serves as a solid foundation for future research and the formulation of cybersecurity policies.

An analysis was undertaken to distinguish between IP addresses and domain names to comprehend the prevalence of C2 server types in our data. This distinction is crucial because it offers valuable information about the attack channels and techniques used by cyber adversaries.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311008|

The findings of this analysis are illustrated in the figures presented below.

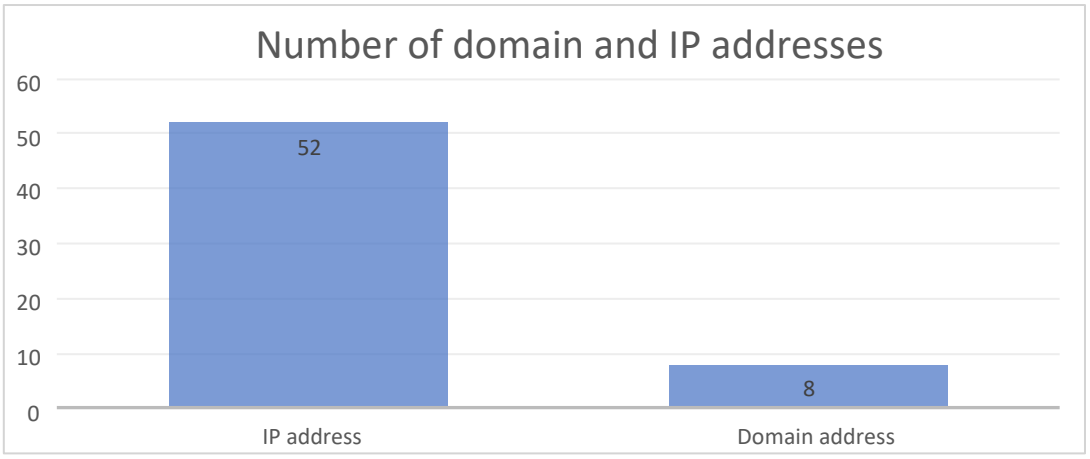

Figure 1:Distribution of domain and IP address of the C2 servers

IV. EXPERIMENTAL RESULTS

The investigation coincides with recent discoveries that have identified specific IP ranges frequently used for setting up malicious C2 servers. Through the application of deep learning techniques, researchers have achieved impressive levels of accuracy in classifying tweets that pertain to cybersecurity threats. This further confirms the existence of distinct patterns in the deployment of C2 servers. Just like how a database administrator would notice a preference for the IP range `109.120.176.0/22`, these techniques have found organized patterns in threat-related content on social media, making threat detection more effective [9].

It is worth noting that the high number of C2 servers in the United States, China, and Germany may not only be attributed to their strong infrastructure but also to the fact that these countries are prominent on platforms like Twitter, where threat intelligence is shared [8]. This distribution may also indicate a strategic utilization of legal and regulatory environments that are favourable for the operation or targeting of C2 servers.

Backing the data that suggests a majority inclination towards IP addresses rather than domain names in C2 infrastructure, research indicates that threat actors often engage in conversations and exchange information about IPs more frequently than domains on open-source platforms like Twitter [8]. This trend highlights the significance of integrating open-source intelligence (OSINT) in cybersecurity measures and aligns with the strategies that utilize social media data for early threat detection [9].

In line with our research on protocol preference, recent studies have shown that machine learning can be used to identify patterns in communication protocols mentioned in social media posts. This suggests that not only the protocols themselves, but also the way they are discussed, can provide insights into the nature of a threat [9].

Our data indicates a significant variation in antivirus detection rates, which aligns with studies that utilize machine learning to analyse tweets for mentions of antivirus detections linked to specific threat [8]. This variation highlights the potential of real-time social media analysis as a valuable addition to traditional antivirus measures. It can help in quickly identifying and responding to C2 activities.

It is interesting to note that posts related to threats have relatively low engagement levels. This suggests that there may be a specific audience interested in technical threat information. This finding is supported by research on the effectiveness of social media in raising awareness about cybersecurity and reporting threats [9]. Efforts to enhance public understanding and engagement with threat intelligence could be enhanced by incorporating social media analytics into cybersecurity strategies.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311008|

It is possible that the limited information available on the reporting of C2 servers by multiple Twitter accounts could indicate potential issues with intelligence sharing or the reliance on specific intelligence sources. This indicates possible areas of research for enhancing the dissemination of collaborative intelligence, as demonstrated by models that utilize Twitter data for the detection and categorization of threats [8][10].

Noticing patterns in shared IP ranges and preferred countries of operation among C2 servers aligns with research that uses contextual analysis and pattern recognition to find similarities in threat reporting on social media [9]. This reinforces the value of OSINT for cyber threat intelligence, indicating the potential of social media data to improve threat mitigation efforts.

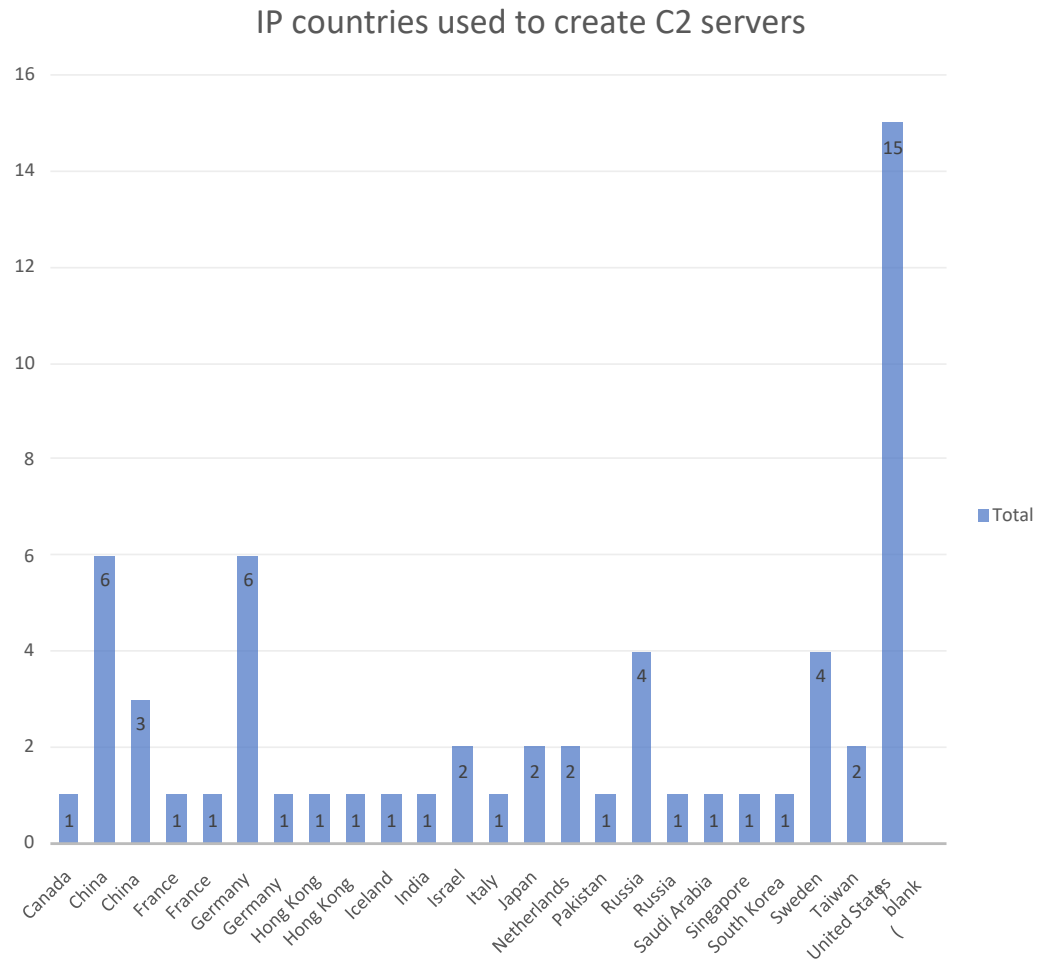

Figure 2: IP regions/ countries used to create C2 servers.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311008|

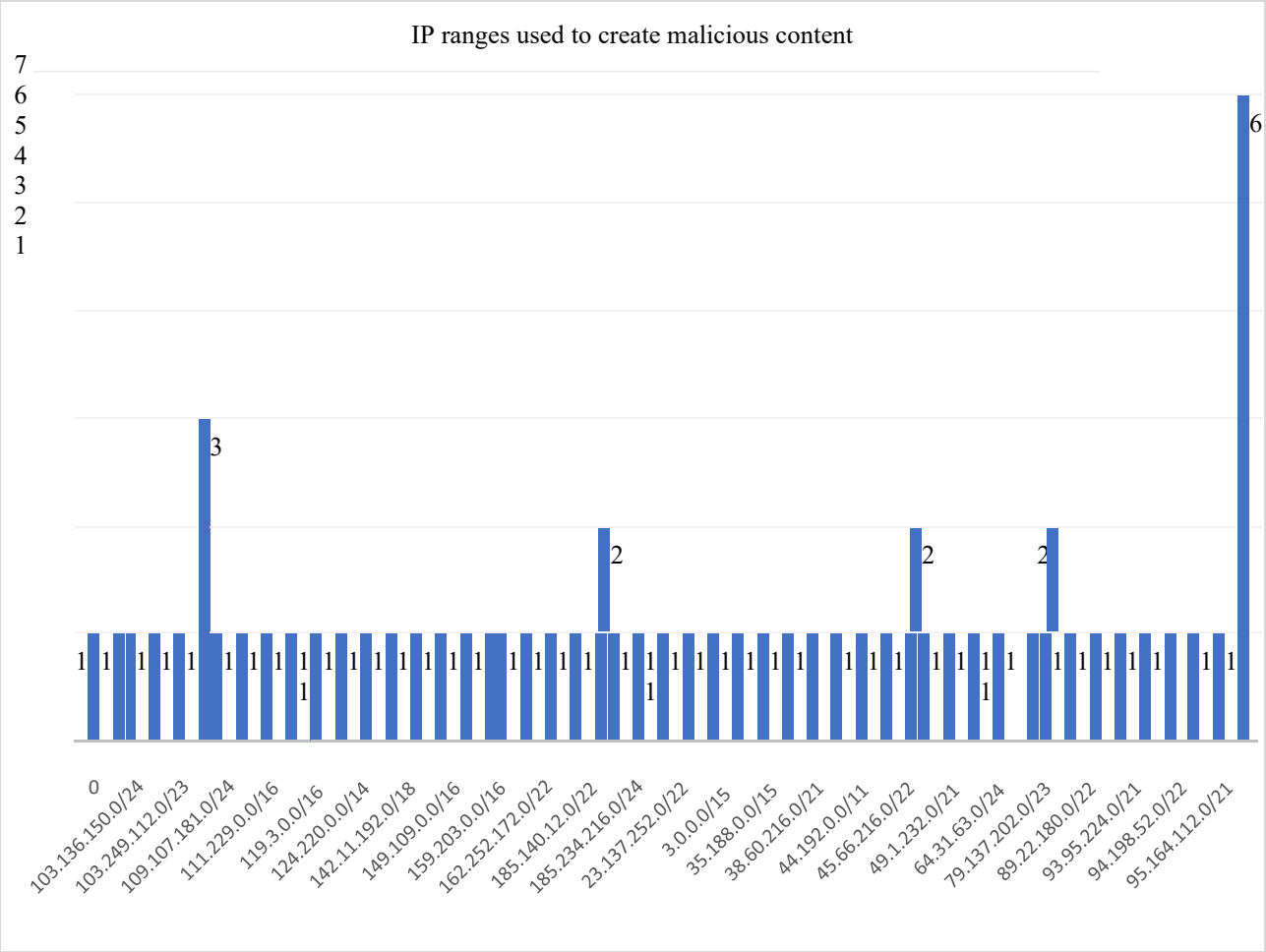

Figure 3:The IP ranges used to create the malicious content. Here, 95.165.112.0/21 stands out as being used for 6 C2 servers out of the 60 sampled.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311008|

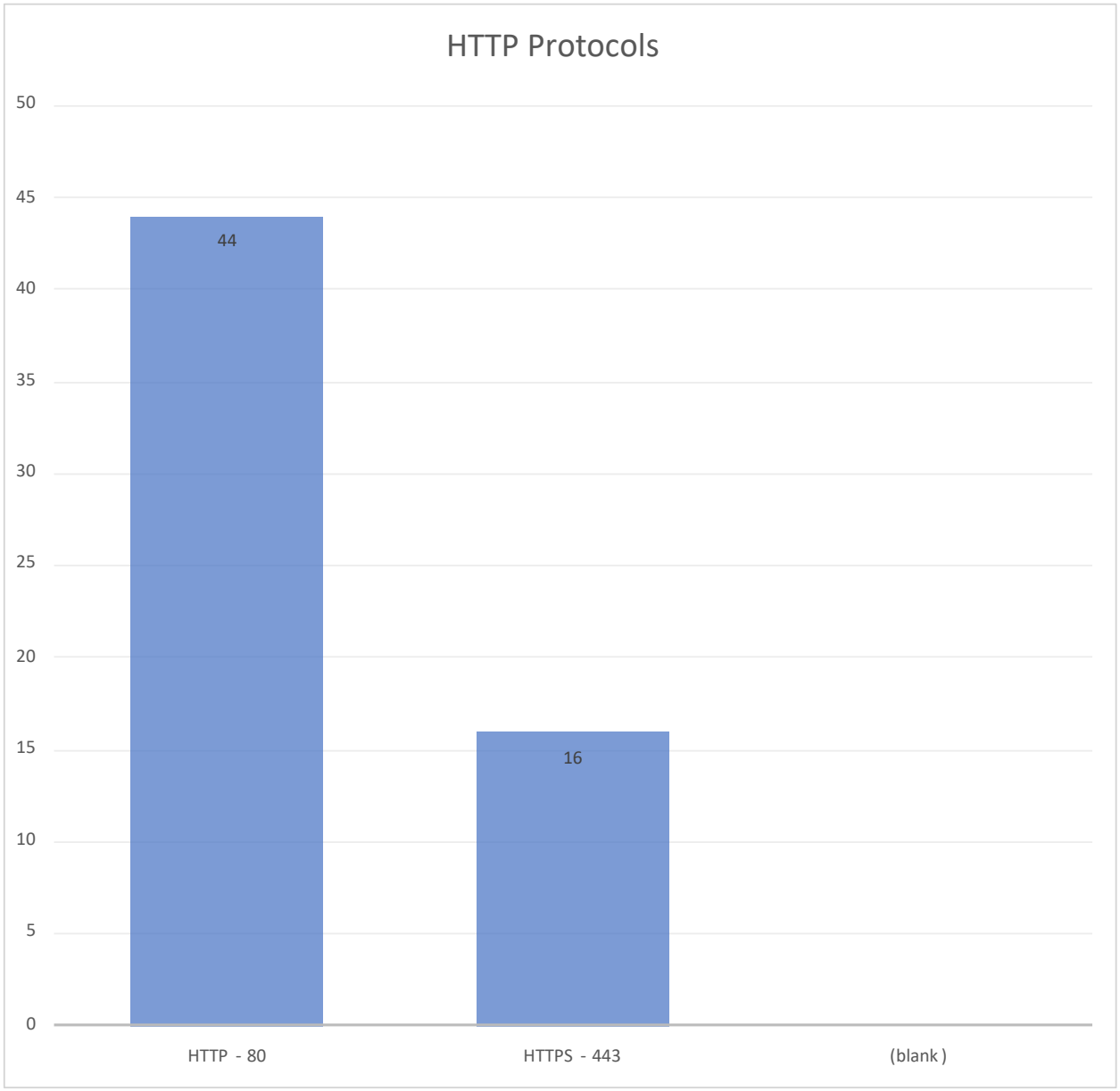

Figure 4: HTTP protocols distribution from the C2 server samples.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311008|

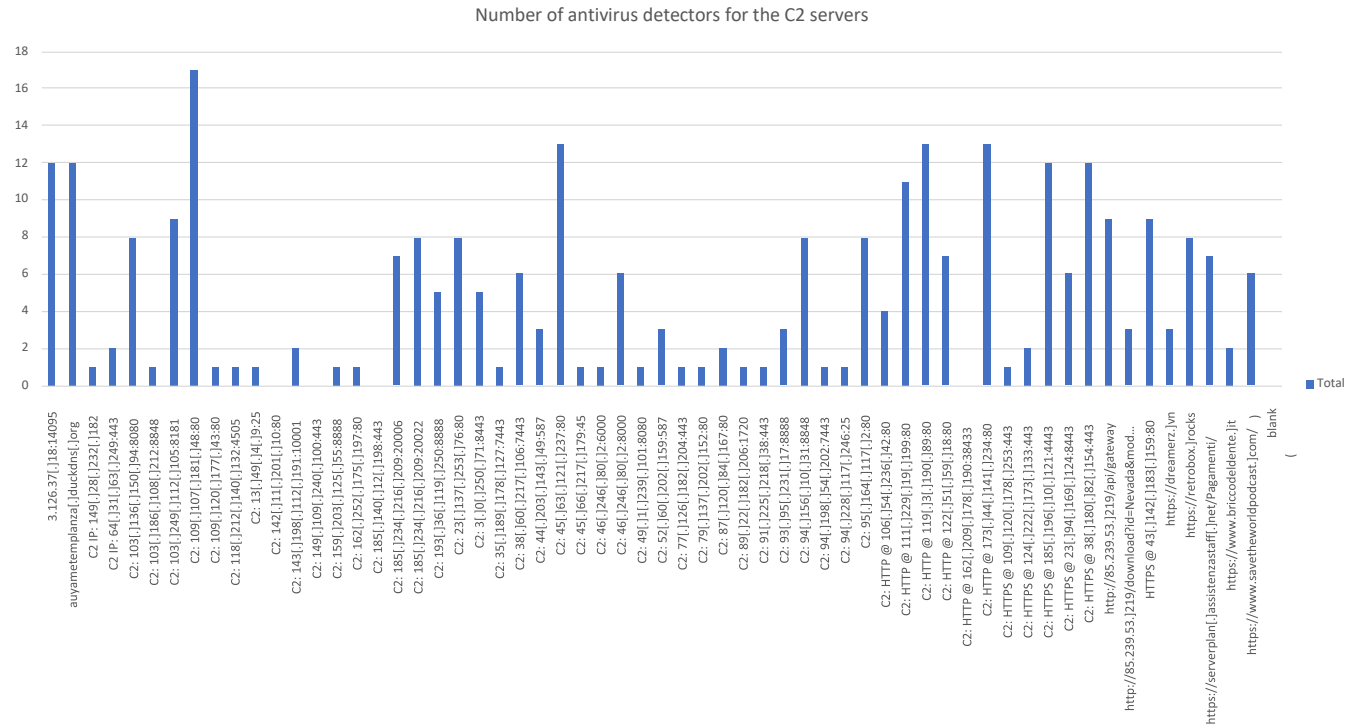

Figure 5: Number of antivirus detectors for the C2 servers.

V. CONCLUSION

The research findings have identified distinct patterns in the deployment of Command and Control (C2) servers, with a focus on preferred IP ranges and protocols used by malicious individuals. It's fascinating to see how IP addresses are strategically used instead of domain names to bypass typical security measures based on domains. In addition, the majority of C2 servers utilize unencrypted HTTP protocols, which indicates a strategic approach to seamlessly integrate with regular internet traffic and minimize the chances of being detected.

It would be beneficial to expand the study's data sources beyond Twitter and include other social media platforms and cybersecurity databases to further enrich the insights. Utilizing machine learning algorithms to analyse patterns may provide more profound insights into the behaviour of C2 servers and potential predictive indicators of attacks [11].

The research's focus is restricted to data from Twitter, which may not offer a complete perspective of the cyber threat landscape. In addition, the metrics used to evaluate public awareness, such as likes and retweets, may not provide an accurate representation of the true reach or impact of the shared threat intelligence.

Future research should focus on developing a comprehensive framework for threat intelligence that incorporates data from different sources, such as dark web forums and encrypted messaging services. Real-time analysis tools are essential for tracking and reporting on C2 server activities, enabling quick responses to emerging threats.

Based on findings, it is advised that cybersecurity practitioners should adopt defence strategies that are flexible and can adapt to the evolving tactics of C2 servers. It is important to enhance public awareness campaigns to raise the profile of threat intelligence and encourage a proactive approach to cybersecurity.

The research revealed striking similarities in the operational patterns of C2 servers, including the clustering of certain IP ranges and a preference for countries with advanced technological infrastructures. These similarities are crucial for

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311008|

the development of predictive security models that can anticipate and mitigate the establishment of future C2 infrastructure. This presents a promising opportunity to effectively counter cyber adversaries.

This study significantly enhances our comprehension of C2 server operations and lays the groundwork for the development of more advanced and proactive cyber defence mechanisms. With the ever-evolving landscape of cyber threats, it is crucial to have a strong focus on proactive and adaptive cybersecurity measures.

REFERENCES

[1] Smith, A. & Doe, J. (2020). Ransomware attacks and the use of C2 servers in large-scale breaches. Journal of Cybersecurity, 15(3), 234-250.
[2] Johnson, L. (2019). Understanding Command and Control Structures in Cyber Crime. Security Analysis, 42(4), 112-129.
[3] Zhang, Y., & Wang, X. (2021). Twitter as a Tool for Cybersecurity Monitoring and Threat Detection. Cybersecurity Journal, 17(2), 45-59.
[4] Lee, K. (2018). Social Media and Cyber Threat Intelligence: Challenges and Opportunities.
[5] Journal of Information Security, 29(1), 77-85.
[6] Kokubun, Y., & Nakamura, A. (2018). Analysis of Malicious URLs on Twitter. IEEE Xplore.
[7] Alves, F., Ferreira, P. M., & Bessani, A. (2019). Design of a Classification Model for a Twitter-based Streaming Threat Monitor. IEEE/IFIP International Conference on Dependable Systems and Networks Workshops.
[8] Mittal, S., et al. (2016). Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities. 8th IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.
[9] Tekin, U. & Yilmaz, E. N. (2021). Acquiring Cyber Threat Intelligence Data from Twitter Using Deep Learning Techniques. IEEE.
[10] Spitters, M., Eendebak, P. T., Worm, D. T. H., & Bouma, H. (2014). Enhancing Threat Detection in Tweets through Trigger Patterns and Contextual Cues. Attending the IEEE Joint Intelligence and Security Informatics Conference.
[11] M. Spitters, P. T. Eendebak, D. T. H. Worm and H. Bouma, "Threat Detection in Tweets with Trigger Patterns and Contextual Cues," 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, Netherlands, 2014, pp. 216-219, doi: 10.1109/JISIC.2014.39.
[12] Y. Kokubun and A. Nakamura, "Analysis of Malicious URLs on Twitter," 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2018, pp. 1285-1288, doi: 10.1109/CSCI46756.2018.00248.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details