IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 February 2024, accepted 10 March 2024, date of publication 13 March 2024, date of current version 19 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3376682

RESEARCH ARTICLE

Evolving Malware and DDoS Attacks: Decadal Longitudinal Study

OLUFUNSHO I. FALOWO, MURAT OZER, CHENGCHENG LI, AND JACQUES BOU ABDO
School of Information Technology, University of Cincinnati, Cincinnati, OH 45221, USA
Corresponding author: Olufunsho I. Falowo (falowooi@mail.uc.edu)

ABSTRACT This study conducts analysis of cybersecurity events from 2013 to 2023, concentrating on major incidents associated with Distributed Denial of Service (DDoS), and malware attacks. Deriving data from the Center for Strategic & International Studies (CSIS) report, it examines 925 major incidents to discern evolving cyber threat trends. A key finding is the escalation in the frequency and sophistication of attacks, with a marked increase in DDoS incidents in 2022 and a steady rise in malware attacks, peaking in 2023. This trend indicates growing threat actors' capabilities and vulnerabilities in digital infrastructures. Additionally, the aggregate of other attack methods, such as phishing and zero-day exploits, surpasses the incidence of DDoS and malware attacks, illustrating the broad spectrum of cyber threats. Employing the ARIMA model, the study projects future DDoS and malware attack trends, factoring in historical data and assumptions of minimal technological advancement and unchanged geopolitical tensions. The forecast suggests a consistent pattern of cyber attacks over the next five years. This study also correlates the nature of cyber attacks with financial motives and geopolitical dynamics, applying reliability and validity testing to affirm the robustness of these findings. Despite ARIMA providing reliable historical-based forecasts, the dynamic nature of cyber threats necessitates cautious interpretation of future trends. In conclusion, the study emphasizes the necessity for dynamic, multifaceted cybersecurity strategies. Nations and organizations must adopt adaptive approaches, bolstered by data analysis and forecasts - crucial in combating the diverse cyber threats, highlighting the need for a proactive and collaborative global cybersecurity framework.

INDEX TERMS DoS attacks, DDoS attacks, malware attacks, major cyber incidents, threat actors, zero-day exploits, incident response strategies.

I. INTRODUCTION

It is well known that the last decade (2013 to 2023) has witnessed an upsurge in sophisticated cybersecurity threats and attacks [1]. These major incidents, often involving cyber-attacks with significant financial repercussions exceeding a million dollars, represent not only a pressing concern for global security but also for global economy as well. In response, understanding the evolution and patterns of these attacks over the past decade becomes a paramount research endeavor. An exploratory study into the occurrences of cyberattacks orchestrated by these threat actors over the past ten years presents an invaluable opportunity to dissect the nature, methodologies, and implications of these incidents. These attacks in some cases have exhibited remarkable sophistication and have often targeted high-value assets across various sectors, ranging from government institutions to critical infrastructures and private enterprises [2], [3]. Analyzing the characteristics, tactics, and outcomes of these attacks can yield critical insights into the evolving landscape of cyber warfare, thereby facilitating the development of robust defense mechanisms and proactive strategies to counteract these threats effectively [2], [3]. As it has been well documented, the cumulative impact of major cyberattacks has been very profound, extending beyond financial losses to encompass geopolitical implications and socio-economic ramifications as well [1]. Hence, investigating these incidents through the lens of a longitudinal study can elucidate the modus operandi employed by these threat actors, their motivations, and the evolving strategies utilized to launch

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Yu.

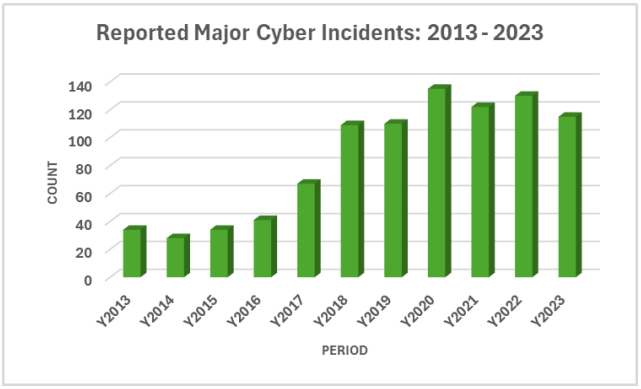


FIGURE 1. Reported major incidents: 2013 - 2023.

these cyberattacks, thus providing a foundational basis for enhanced cybersecurity measures and proactive mitigation strategies. Figure 1 below is presented as a graphical representation, drawing data from Tables 1, 2, and 3 (from subsequent pages), to effectively illustrate the yearly distribution of major cybersecurity incidents from 2013 to 2023. Totalling 925 events, the figure provides an at-a-glance overview of the data meticulously detailed in the Tables 1, 2, and 3, thereby offering a clear and immediate understanding of the temporal patterns in major cybersecurity threats over the last decade.

Our previous study [4] offered a comprehensive overview of various attack techniques employed by cybercriminals. Among these, Distributed Denial of Service (DDoS) and Malware attacks were highlighted as the most prevalent. This new study aims to build on these findings, focusing specifically on the patterns and evolution of DDoS and Malware attacks over the past decade. By further scrutinizing these particular attack vectors, we seek to provide deeper insights into their mechanisms, impacts, and the evolving strategies of threat actors.

A. SIGNIFICANCE OF DDoS ATTACKS

DDoS attacks, usually characterized by their ability to massively disrupt services by overwhelming systems with a flood of internet traffic, have become a dangerous tool of choice for cybercriminals [5], [6]. These attacks not only cause immediate operational disruptions to private and public enterprises but also serve as a smokescreen for more harmful activities, such as data security breaches [5], [6]. Over the years, there are many publicly available well-documented references that indicate how the sophistication and scale of DDoS attacks have escalated [1], [7], [8], making them a significant concern for organizations across various sectors [1]. This study delves into the trends, techniques, and advancements in DDoS attacks, analyzing how they have evolved and what this means for future cybersecurity strategies.

B. THE EVOLUTION OF MALWARE ATTACKS

Similarly, Malware attacks have shown a concerning level of advancement and diversification in recent decades, especially in last ten years [9], [10], [11]. Suffice that, from ransomware to spyware, these malicious software attacks have caused extensive damage and implications, leading to loss of sensitive data, financial losses, and erosion of consumer trust on many occasions [9], [10], [11]. The study explores the changing landscape of Malware, examining how its impacts have shifted over the last decade. This analysis is crucial for understanding the current state of Malware threats and preparing for emerging challenges face the modern world.

C. METHODOLOGY AND DATA SOURCES

To conduct this in-depth analysis, our study leverages data from the latest 2023 cybersecurity reports, incident logs, and documented expert opinions. We compare these contemporary findings with past data to identify patterns, changes, and consistencies in the behavior and strategy of threat actors. This longitudinal approach [12], [13] allows for a continuous and comprehensive understanding of the evolution of DDoS and Malware attacks, providing valuable insights into their trajectory and potential future developments.

D. THE IMPORTANCE OF THIS STUDY

The importance of this study lies in its focus on specific attack patterns over a significant period (2013 to 2023). By analyzing the evolution of DDoS and Malware attacks, we aim to equip cybersecurity professionals, policymakers, and organizations with the knowledge to anticipate and mitigate future threats. Understanding these patterns is crucial for developing more effective defense mechanisms, shaping cybersecurity policies, and ultimately safeguarding digital assets and infrastructures. This study not only contributes to the academic field of cybersecurity but also plays a vital role in enhancing real-world security practices. Figure 2 in the report serves as a detailed visual breakdown of Figure 1, categorizing the yearly cybersecurity incidents from 2013 to 2023 into three distinct types: (a) Distributed Denial of Service (DDoS) attacks, (b) malware attacks, and (c) other forms of attacks. The primary intent of this figure is to facilitate a side-by-side comparative analysis of the prevalence of DDoS and malware attacks over the specified decade. By segregating the incidents into these categories, this figure provides a clear and concise visual representation of the data, enabling readers to easily discern the yearly fluctuations in each type of attack. This breakdown not only highlights the relative frequency of DDoS and malware incidents but also underscores the presence of other significant forms of cyber threats during the same period.

E. RESEARCH QUESTION

How have the defensive strategies against DDoS and Malware attacks effectively impacted the trends of these attacks over

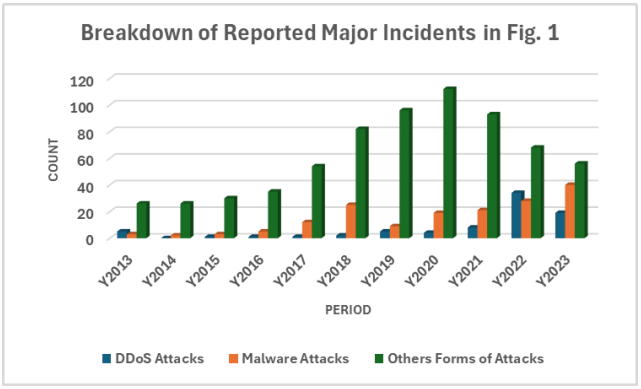


FIGURE 2. Breakdown of major incidents: 2013 - 2023.

the last decade? The research question holds significant importance in the field of cybersecurity. By focusing on this research question, this inquiry centers on evaluating the effectiveness of countermeasures in the ever-evolving battle against cyber threats. By analyzing the trends in major DDoS and Malware attacks in relation to the development and implementation of defensive strategies, this study aims to shed light on the direct impact of these strategies on reducing or altering the frequency and severity of these two types of attacks. Understanding this relationship is critical, as it not only assesses the current state of cyber defense but also guides future investments and innovations in cybersecurity measures. The availability of data regarding the count of major attacks provides a tangible metric to gauge the success or shortcomings of existing defense mechanisms, thus offering invaluable insights for organizations, policymakers, and cybersecurity professionals in fortifying their defenses against these prevalent and damaging cyber threats.

II. BACKGROUND LITERATURE

A. HISTORICAL TRENDS AND EVOLUTION OF DDoS AND MALWARE ATTACKS

Over the past decade, there are many discussion about how the global landscape of Distributed Denial of Service (DDoS) and Malware attacks has not only undergone significant evolution, but have also been marked by increasing sophistication and scale [1], [7], [8]. Historically, some security researchers have argued that DDoS attacks were primarily used as a form of digital protest or vandalism, but they have evolved into a more complex and large-scale operations in this modern era, often used in conjunction with other cyber threats [1], [4]. The advent of botnets for example, particularly those leveraging Internet of Things (IoT) devices, has dramatically increased the scale and impact of DDoS attacks [14], [15]. These botnets allow threat actors to harness a vast network of compromised devices to flood target entity with overwhelming traffic to the extent that disruption or even a data breach is caused [14], [15]. Additionally, there has also been a trend towards multi-vector DDoS attacks [16], [17] that is the act where threat actors combine or leverage different attack methodologies to bypass traditional defense mechanisms. In terms of malware, the landscape has shifted from widespread viruses and worms to more targeted ransomware and in some instances state-sponsored espionage tools [1], [4]. The proliferation of ransomware has been particularly very notable, with threat actors often targeting not just corporations, but also critical infrastructure and government systems. This shift is an indication of a move from seeking notoriety or causing disruption to pursuing significant financial gain or strategic advantage.

Comparing with DDoS attacks, the evolution of Malware attacks also reflects a parallel trajectory of increasing complexity and targeted focus. For example, the early forms of malware were often broad-brush and disruptive, but there are lots of documented evidence that indicate that modern variants of malware are more stealthy, sophisticated, and financially motivated [18], [19]. Suffice that, the rise of ransomware, a type of malware that encrypts a victim's files and demands a ransom for their release, has caused significant global impact, targeting healthcare systems, local governments, and major corporations [20], [21]. This evolution points to a shift in threat actors' motivations, from seeking to cause widespread disruption to aiming for financial gain or in some cases strategic disruption [20], [21]. Furthermore, state-sponsored malware, used for espionage and in some cases sabotage, has emerged as a significant threat [1], exemplified by incidents such as the Stuxnet attack [22], [23]. These advanced persistent threats (APTs) arguably demonstrate the use of malware for geopolitical leverage, hence highlighting the intersection of cybersecurity with international relations. Overall, these historical trends in DDoS and Malware attacks are very indicative that a cyber landscape that is increasingly complex, with threats that are more sophisticated, targeted, and intertwined with global economic and political dynamics.

B. TECHNOLOGICAL ADVANCEMENTS IN CYBER DEFENSE MECHANISMS

In response to the escalating threat of DDoS and Malware attacks, according to many experts and many academic studies, the cybersecurity industry has made significant technological advancements in defense mechanisms against these attack techniques [24], [25], [26]. One of the highly recognized advancements in combating DDoS attacks is the development of more sophisticated DDoS mitigation tools [24], [25], [26]. These tools often employ advanced machine learning algorithms to differentiate between normal and malicious traffic, enabling them to effectively filter out attack traffic while allowing legitimate traffic to pass through a designated network [26]. Given the progress made by Cloud Service Providers (CSP), Cloud-based DDoS protection services have also gained prominence, providing easily scalable solutions to absorb the large volumes of traffic associated with DDoS attacks [27], [28]. It goes without saying that advancements in artificial intelligence

and machine learning algorithms have in many ways enabled the progressive development of systems that can learn from network attack patterns and adapt their defenses accordingly [26].

Similarly, in the realm of ensuring defense against malware threats, notable progress have been made in monitoring, detection and prevention technologies. For example, antivirus and anti-malware software have evolved from relying solely on signature-based analysis and detection, which compares files against a database of known threats, to incorporating heuristic, anomalies and behavior-based monitoring and detection methods [29], [30], [31]. These advanced methods have in major ways enhanced the seamlessly identification of previously unknown malware threats by analyzing the behavior of programs and files to the extent that threats are clearly identified in near real-time. Furthermore, the use of sandboxing [32], [33] technology is another major accomplishment in the cybersecurity industry that has become a critical tool in identifying and isolating suspicious or malicious files, allowing for safe examination without risking the integrity of the main system. Another notable advancement is the integration of endpoint detection and response (EDR) systems [34], which provide continuous monitoring and response capabilities to identify and mitigate threats at the device level. These advancements and progresses, along with the increasing use of open source or comercial threat intelligence platforms that aggregate and analyze data on emerging threats, represent a comprehensive and adaptive approach to defending against the constantly changing landscape of malware threats.

C. IMPACT OF DDoS AND MALWARE ATTACKS ON DIFFERENT SECTORS

DDoS and Malware attacks have had a profound impact across various sectors globally, causing disruptions that range from temporary inconvenience to severe, long-term various types of consequences [1]. In the financial sector, for instance, DDoS attacks is capable of crippling online banking services, resulting in financial losses and eroding customer trust [1]. Malware attacks in this sector often aim at data breaches, leading to significant financial theft and compromising sensitive customer identifiable information. There are reports of the fact that healthcare sector has also been heavily impacted, particularly by malware attacks like ransomware [1]. These attacks can paralyze hospital systems, hinder access to patient records, and disrupt critical medical services, potentially putting lives at risk. In the retail sector, both DDoS and Malware attacks can disrupt online commerce, lead to theft of customer data, and cause substantial financial and reputational damage [1]. The impacts of these threats are not limited to these aforementioned sectors only, but critical infrastructure, government services, and educational institutions have all been targets, with consequences that can extend to both national security and public safety [1].

The nature and severity of the impact also vary by different regions across the globe, reflecting differences in cybersecurity preparedness and incident response capabilities [1]. For example, in regions with less developed cybersecurity infrastructure like the third-world countries, attacks may have more devastating consequences, potentially leading to longer downtimes and greater data losses across multiple sectors. On the other hand, sectors and regions with more advanced cybersecurity measures or capabilities might be better equipped to respond and mitigate these attacks but still face the challenges of evolving attack techniques and the need for continual investment in cyber defense. Hence, it is noteworthy to highlight that the interconnectedness of global systems means that an attack in one sector or region is capable of evolving to the extent of having cascading effects elsewhere, highlighting the need for a coordinated global response to these cyber threats. Therefore, these diverse impacts underscore the importance of sector-specific cybersecurity strategies and international cooperation in cyber defense to effectively counter the global threat posed by DDoS and Malware attacks.

D. CYBERSECURITY POLICIES AND REGULATORY FRAMEWORKS

There are many studies and publicly available documentation that highlight how across the globe, various continents have developed and implemented prominent cybersecurity policies and regulatory frameworks to address the growing threats of DDoS and Malware attacks. In Europe, one of the most significant frameworks is the General Data Protection Regulation (GDPR) [35], which has set a high standard for data protection and privacy of its citizens. While primarily focused on data privacy, GDPR has significant implications for cybersecurity as it mandates some notably strict security measures for protecting personal data and imposes significant financial fines for breaches of this regulation [35]. This regulatory law has prompted many organizations to enhance their cybersecurity measures, indirectly bolstering security defenses against malware and other forms of cyber threats which may include DDoS. Additionally, the NIS Directive (Directive on Security of Network and Information Systems) is another key policy in the EU [36], [37], specifically targeting the security of network and information systems which tend to require member states to improve their national cybersecurity capabilities and for operators of essential services to take appropriate security measures to manage cyber risks as best as possible in order to enhance readiness to respond to security threats [36], [37].

In North America, particularly in the United States, there are various sector-specific regulations alongside broader policies that have been put in place over the last decades. The Cybersecurity and Infrastructure Security Agency (CISA) for example plays a very notable role in enhancing the security and resilience of the nation's critical infrastructure against cyber threats [38]. Other frameworks like the

NIST Cybersecurity Framework offer detailed guidelines for organizations to manage and reduce cybersecurity risk to a very manageable level [39]. Further more, sector-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA) [40] for healthcare and the Federal Information Security Management Act (FISMA) [41] for government agencies are additional examples that provide tailored requirements for cybersecurity in respective sectors.

In Asia, there's a growing emphasis on enhancing cybersecurity policies and frameworks, though approaches can vary significantly across the continent. Countries like Singapore and Japan have established comprehensive cybersecurity laws. Singapore's Cybersecurity Act [42] for instance focuses on the protection of critical information infrastructure, while Japan's Cybersecurity Basic Act [43] aims to establish a system for ensuring cybersecurity readiness and response. In contrast, emerging economies in Asia and Africa are still developing their cybersecurity infrastructures and legal frameworks. There's an increasing effort in these regions to balance the rapid digital transformation with robust cybersecurity measures as best as possible. This includes not only implementing regulations but also promoting cybersecurity awareness and collaboration among ASEAN countries [44], [45]. It is important to echo the fact that these regional differences in frameworks and regulatory laws underscore the diverse approaches to cybersecurity policy and regulation, reflecting varying levels of technological development, cyber threat landscapes, and legal cultures.

These regulatory frameworks and policies play a crucial role in shaping how continents and individual countries respond to DDoS and Malware threats in many ways. They not only provide legal guidelines and standards for organizations to follow but also reflect the evolving understanding of cybersecurity's importance in protecting national security, economic interests, and personal privacy.

III. METHODOLOGY

A. SAMPLING THEORY

This study's methodology is grounded in Sampling Theory [46]. In other words, the relevance and use of sampling theory is well-justified given its comprehensive approach to analyzing major cybersecurity incidents. From the population of 925 major incidents, the total sample size of 80 DDoS incidents and 167 malware incidents, encompassing data from 2013 to 2023, ensure a robust and extensive dataset that is representative of the evolving nature of major DDoS and malware incidents globally. The study is built upon a robust historical foundation, comprising 680 major cyber incidents that have been previously analyzed [4], providing essential context and depth to the research. Additionally, the inclusion of 245 recent major incidents, with 130 from 2022 and 115 from 2023, ensures that the analysis is current and reflects the latest trends. This combination of historical and contemporary data allows for a comprehensive understanding of the evolving nature of cyber threats. This blend of these historical and contemporary data enhances this study's ability to identify and understand long-term patterns and emerging threats in cyber security across all geopolitical regions. The longitudinal nature of this study, spanning over a decade, is critical in capturing the dynamic and rapidly evolving landscape of cyber threats, ensuring that the findings are not only comprehensive but also reflective of the global and temporal diversity of DDoS and Malware attacks. This approach aligns with the principles of Sampling Theory by ensuring that the sample size of 80 DDoS incidents and 167 malware incidents is sufficiently large and diverse to draw meaningful, generalizable conclusions about these two threats worldwide.

B. THEORY OF RELIABILITY AND VALIDITY

The rigorous application of the Theory of Reliability and Validity [47] strongly justifies the methodology of this study on cybersecurity incidents. By adhering to consistent and standardized criteria for identifying and classifying major DDoS and Malware attacks, the study ensures high reliability, meaning that the process of data collection and analysis can be replicated with similar results. Validity is also carefully addressed, with the study accurately reflecting the phenomena it aims to investigate. The comprehensive scope of 925 incidents from 2013 to 2023, including both previously analyzed and newly added cases, underpins content validity by covering a wide range of cyber threats across different geopolitical regions. Construct validity is maintained through clear definitions and operationalization of key concepts like 'major incidents,' 'DDoS attacks,' and 'Malware attacks.' Furthermore, the large and diverse population, sample size of both DDoS and malware related events, coupled with longitudinal analysis, enhances external validity, allowing the findings to be generalized to the broader context of global cyber threats. This meticulous attention to reliability and validity ensures that the study's findings are both credible and applicable to the real-world challenges of cybersecurity [48], [49].

C. LONGITUDINAL STUDY

The importance of a longitudinal study [12], [13] of this nature cannot be overstated. By covering incidents from a period of over a decade and across all geopolitical regions, this study provides a unique and comprehensive perspective on the global evolution of cybersecurity threats, especially with reference to DDoS and malware attacks. This long-term view is essential for understanding the progression of both attack strategies and defense mechanisms. It offers invaluable insights for policymakers, cybersecurity professionals, and researchers into how cyber threats develop and adapt over time, informing more effective strategies for monitoring, prevention, mitigation, and response. Furthermore, the global scope of this study ensures that its findings are relevant across different regional contexts, reflecting the universal nature of

cybersecurity challenges. Overall, the statistical significance of this study lies in its extensive, diverse dataset and its longitudinal approach, which together provide a detailed and evolving picture of the global cybersecurity threat landscape.

D. SCOPE OF THIS STUDY

1) DESCRIPTIVE COMPONENT OF THIS STUDY

The proposed study is structured into three distinct yet interconnected parts, each focusing on different aspects of the cybersecurity landscape with regard to DDoS and malware attacks. Part 1 of the study is dedicated to providing a descriptive analysis of the cybersecurity incidents that occurred from 2013 to 2023. This section aims to detail the nature and timing of these incidents, offering a chronological narrative of events. By focusing on the descriptive aspects, this part will paint a clear picture of what happened and when, setting the stage for a deeper understanding of the trends and patterns in cyber threats during this period.

2) UNCOVERING CORRELATION

Part 2 shifts the focus to a more analytical approach, seeking to uncover correlations between the major cyber incidents and various influencing factors. This section will delve into the potential connections between the incidents and variables such as financial or monetary motivations, and the role of cyber warfare in the context of global geopolitics. This exploration aims to elucidate the underlying motives and geopolitical dynamics driving these cyber attacks, providing insights into the complex interplay of factors that precipitate such incidents.

3) USING ARIMA MODEL TO MAKE FORECAST

The third and final part of the study employs a quantitative approach, utilizing historical data on DDoS and malware attacks from the past decade to predict future trends. This predictive analysis will be conducted using the ARIMA (AutoRegressive Integrated Moving Average) model, a robust tool for forecasting based on time series data [50], [51], [52], [53]. The criteria for this forecast will include at least one or two of the following criteria:

- Historical Trend Analysis, which examines the frequency of attacks to identify trends.
- Technological Advancements, considering the evolving nature of IoT and network infrastructure that might introduce new vulnerabilities.
- Additionally, the study will consider the impact of Global Cybersecurity Policy Changes and the overall Evolution of the Cyber Threat Landscape, acknowledging the dynamic nature of cyber threats and their shifting focus.

This comprehensive approach in third part aims to provide an informed projection of major cyber incidents in the next five years, based on a thorough analysis of past trends and current factors influencing the cybersecurity domain.

E. CROSS-REFERENCING DERIVED DATA

The total 925 major incidents analyzed for this study as mentioned in prior sections were derived from our analysis of the report on "Significant Cyber Incidents" published by Center for Strategic & International Studies (CSIS). Incorporating insights, definitions, analysis and lessons from the Data Breach Investigation Report (DBIR) [54] and the Global Cybersecurity Index (GCI) [55] alongside derived data (925 major incidents) from the CSIS, significantly enhances the validity and depth of this study's review of the 925 major cyber incidents with deeper analysis or 80 DDoS attacks and 167 malware attacks. The DBIR is renowned for its detailed analysis of data breaches and cybersecurity incidents, offering granular insights into attack patterns, threat actors, and security vulnerabilities. By cross-referencing the CSIS report with the DBIR, the study benefits from a richer, more nuanced understanding of each incident, ensuring a comprehensive assessment of the attack methodologies and their impacts as well. Simultaneously, the GCI provides a macro-level view of countries' commitment to cybersecurity, ranking them based on legal, technical, organizational, capacity building, and cooperation measures. Utilizing the GCI allows this study to contextualize the 925 major incidents within the broader framework of global cybersecurity readiness and response capabilities. This multi-source approach, leveraging both the incident-specific details from the DBIR and the country-level cybersecurity insights from the GCI, ensures a well-rounded, robust validation of the 80 DDoS and 167 malware major incidents studied. It also offers a unique perspective on how individual cybersecurity events tie into the global landscape of cyber readiness and resilience, thereby enriching the study's conclusions and recommendations.

F. DATA COLLECTION

In this study, the dataset in Tables 1, 2 & 3 is meticulously derived from the CSIS report [1], with a specific set of criteria established by the authors to ensure precise and relevant data extraction. Central to this process is the application of the MITRE ATT&CK framework [56], which serves as a guiding tool to accurately categorize and distinguish the attack techniques pertinent to the dataset in Tables 1, 2 & 3. This methodological approach not only ensures that the data aligns with the study's focus on DDoS and Malware attacks but also provides a structured and standardized way to analyze and interpret the nature of each incident. By integrating this renowned framework, the study enhances the specificity and accuracy of its analysis, ensuring that each incident is assessed within a clear and comprehensive cyber threat context. Similar to the prior study [4], another important reason for the selection of the CSIS report as the primary source of major cybersecurity incidents that we analyzed is due to its inclusiveness of all the regions of the world which includes the coverage of the following regions:

1) Africa
2) America

3) Arctic
4) Asia
5) Europe
6) Middle East
7) Russia and Eurasia

G. STATISTICAL SIGNIFICANCE

This study carefully calculates the minimum sample size required to achieve statistical significance from the total population of 925 major cybersecurity incidents between 2013 and 2023. Guided by insights from [57], which underscores the importance of statistical significance in research, and utilizing the sample size calculator [58]" we set stringent parameters: a confidence level of 95% and a margin of error at 5%, with an assumed population proportion of 6%. These parameters were essential in determining the statistically significant minimum sample size of "equal to" or "greater than" number 80 as the appropriate minimum sample necessary for the two key categories of our study: (1) incidents related to Distributed Denial of Service (DDoS) attacks and (2) incidents involving malware attacks. This careful calculation ensures that the sample sizes for each category are robust enough to yield reliable and valid conclusions, reflecting a rigorous approach to understanding the trends and implications of these cyber threats. Below is the formula and how it was used to arrive at 80:

The sample size (n) is calculated according to the formula:

$$n = \frac{(\frac{(z^2 \times p) \times (1-p)}{e^2})}{1 + (\frac{(z^2 \times p) \times (1-p)}{(e^2 \times N)})}$$

where: z = 1.96 for a confidence level (α) of 95%, p = proportion (expressed as a decimal), N = population size, e = margin of error.

$$z = 1.96, p = 0.06, N = 925, e = 0.05$$

$$n = \frac{(\frac{(1.96^2 \times 0.06) \times (1-0.06)}{0.05^2})}{1 + (\frac{(1.96^2 \times 0.06) \times (1-0.06)}{(0.05^2 \times 925)})}$$

$$n = \frac{86.66}{1.09}$$

$$n \approx 80$$

IV. RESULTS

A. DESCRIPTIVE COMPONENT OF THIS STUDY

In this study spanning from 2013 to 2023, the analysis of cybersecurity incidents revealed a significant distribution between Distributed Denial of Service (DDoS) and malware-related attacks. As per our detailed findings, represented in Tables 1, 2, and 3, we identified a total of 80 incidents attributed to DDoS attacks, while a higher count of 167 incidents was associated with malware attacks. This differentiation in the incidence rate provides a clear indication of the varying scales and impacts of these two predominant cyber threat types within the studied period. Furthermore, in line with the sample size calculations outlined in our methodology section, these numbers – 80 for DDoS and 167 for malware attacks – adequately meet the minimum threshold required to attain statistical significance for our study. This adherence to rigorous statistical standards not only validates the reliability of our findings but also underscores the precision of our research approach. Suffice to say that by achieving this statistical significance, our study offers a robust and quantitatively grounded insight into the trends and dynamics of DDoS and malware threats over a decade, making a substantial contribution to the field of cybersecurity research.

TABLE 1. Dataset from previous study [4].

Year	2013	2014	2015	2016
DDoS Attacks	5	0	1	1
Malware Attacks	3	2	3	5
Other Forms of Attacks	26	26	30	35
Total	**34**	**28**	**34**	**41**

TABLE 2. Dataset from previous study [4].

Year	2017	2018	2019	2020	2021
DDoS Attacks	1	2	5	4	8
Malware Attacks	12	25	9	19	21
Other Forms of Attacks	54	82	96	112	92
Total	**67**	**109**	**110**	**135**	**122**

TABLE 3. New dataset.

Year	2022	2023
DDoS Attacks	34	19
Malware Attacks	28	40
Other Forms of Attacks	68	56
Total	**130**	**115**

B. UNCOVERING CORRELATION WITH FINANCIAL MOTIVES AND GEOPOLITICAL DYNAMIC

In this section of the study, we delve into a detailed analysis to uncover correlations within the 925 major cybersecurity incidents, particularly focusing on their association with financial motivations and geopolitical tensions. This exploration is crucial for understanding the underlying drivers of these cyber attacks, as preliminary observations suggest a significant proportion were financially motivated, while many others were intricately linked to geopolitical dynamics. By dissecting these correlations, the study aims to provide a nuanced understanding of the factors influencing cyber threat actors and their choice of targets. This analysis is vital not only for comprehending the complexities of the current cyber threat landscape but also for informing future cybersecurity strategies and policies. The findings from this breakdown will offer valuable insights into the motivations behind cyber attacks, aiding in the development of more targeted and effective countermeasures against these evolving threats.

1) FIRST ANALYSIS

In the analysis of 925 major cyber incidents from the period of 2013 to 2023, our observations indicate that only 45 incidents, which constitute approximately 4.9% of the

total, had potential monetary or financial implications for the targeted entities. This finding is particularly insignificant when considering the statistical parameters set for the study: a confidence level of 95% and a margin of error of 5%, with an assumed population proportion of 6%. Based on these statistical standards, the 45 incidents with financial implications are determined to be statistically insignificant within the larger context of the 925 major incidents. This result suggests that, while financial motivations are generally a factor in cyber attacks, they may not be the predominant driving force in the majority of the 925 major cyber incidents that were analyzed in this study. Furthermore, of these 45 incidents identified with potential monetary or financial implications, 33 incidents, accounting for 73% of this subgroup, targeted either institutions of nations, major sectors of countries, or critical infrastructure.

On the other hand, a more significant portion, comprising 780 out of the 925 incidents, which is about 84%, affected similar high-profile targets. These included institutions of various nations, key sectors in different countries, or critical infrastructure components. This distribution of targets underscores the broader strategic and geopolitical dimensions of these cyber attacks, beyond just financial gains. It highlights the extent to which cyber threats have become entangled with national security and the functioning of critical sectors worldwide, reflecting the strategic intent behind a vast majority of these incidents.

2) SECOND ANALYSIS

Continuing of the analysis of the 925 major cyber incidents recorded from 2013 to 2023, it was also found that incidents related to Distributed Denial of Service (DDoS) and malware collectively accounted for 247 cases, representing approximately 27% of the total incidents. This subset of data highlights the significant prevalence of these two types of cyber threats within the broader spectrum of major cyber incidents. However, within this specific category of DDoS and malware attacks, only 18 incidents, constituting about 7% of the 247 incidents, were identified as having potential monetary or financial implications for the targeted entities. Applying the study's established statistical standards — a 95% confidence level, a margin of error at 5%, and an assumed population proportion of 6% — these 18 incidents are deemed statistically insignificant in the context of the larger dataset. This result indicates that, while present, financial motivations in DDoS and malware attacks are not the predominant factor in the majority of cases within this particular set of major cyber threats.

Furthermore, an in-depth examination of these 247 DDoS and malware incidents reveals that a majority, numbering 214 incidents or approximately 86% of this group, targeted institutions, major sectors, or critical infrastructure of various countries. This pattern of targeting suggests a strategic approach in these cyber attacks, where the focus extends beyond mere financial gain to potentially involve geopolitical or sector-specific objectives. The high proportion of attacks on such critical and high-profile targets demonstrates the broader implications of DDoS and malware incidents, signifying their impact on national security, economic stability, and the essential functioning of targeted countries. This aspect of the findings underlines the strategic nature of a vast majority of these cyber threats, highlighting their significance in the realm of global cybersecurity.

TABLE 4. Forecast of major incident 2024 to 2028.

Year	2024	2025	2026	2027	2028
Major DDoS Incidents	22.67	22.01	22.13	22.11	22.11
Major Malware Incidents	37.84	38.58	38.33	38.41	38.38

C. USING ARIMA MODEL WITH CONFIDENCE LEVEL TO MAKE FORECAST

This Table 4 showcasing the predicted malware and DDoS attacks from 2024 to 2028, as forecasted by the ARIMA model, present a forward-looking view of the cybersecurity landscape. For malware attacks, the predictions start at 37.84 incidents in 2024 and show a slight but fluctuating increase, peaking at 38.58 in 2025 before stabilizing around 38.4 incidents in the subsequent years. In contrast, the forecast for DDoS attacks begins with a higher frequency of 22.67 in 2024, decreasing slightly to 22.01 in 2025 and then stabilizing around 22.1 incidents for the remaining years. These table provides a quantitatively informed perspective on the future trends of these cyber threats, suggesting that all-things-being-equal, a steady state with minor variations in the frequency of both malware and DDoS attacks over the next five years. This projection does not factor when, where but is instrumental in understanding potential future challenges in global cybersecurity and aids in strategic planning, international cross-collaboration and resource allocation for effective global cyber defense.

With reference to Figure 3, the ARIMA model forecast for malware attacks from 2024 to 2028, incorporating relevant criteria under the assumption of potentially slow technological advancement and continued geopolitical tensions, has been visualized in the graph. The green line represents the forecasted trend, while the shaded area indicates the 80% confidence interval, providing a range within which future major incidents based on malware attack frequencies are likely to fall. This visualization depicts not only the expected number of major incidents anticipated from malware attacks in the coming years but also the uncertainty associated with these predictions, captured by the confidence intervals. This model suggests a generally stable trend with minor fluctuations in the number of major incidents by malware attacks, reflecting the assumption of a relatively static technological and geopolitical landscape. The inclusion of confidence intervals is essential, as it underscores the inherent uncertainty in forecasting, especially in the dynamic field of cybersecurity. These predictions serve as an informative tool for strategic planning and preparedness, helping stakeholders

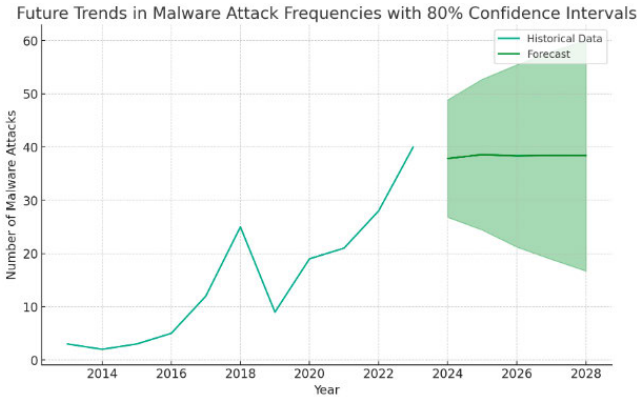


FIGURE 3. Future trend of major malware incidents: 2024 - 2028.

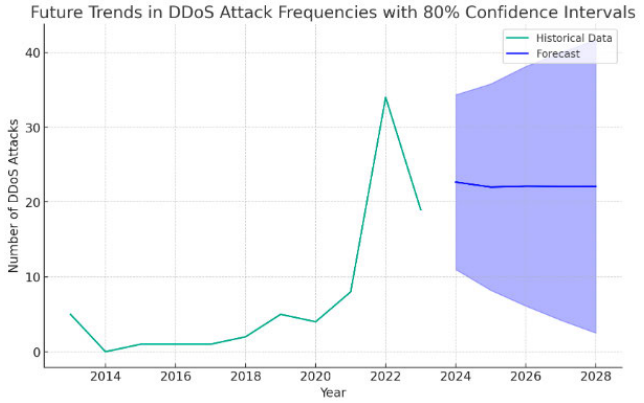


FIGURE 4. Future trend of major DDoS incidents: 2024 - 2028.

to anticipate and respond to future cybersecurity major challenges within a defined range of possibilities.

With reference to Figure 4, the ARIMA model forecast for DDoS attacks from 2024 to 2028, incorporating relevant criteria under the assumption of potentially slow technological advancement and ongoing geopolitical tensions, has been visualized in the graph. The forecasted trend, represented in blue, projects potential future frequencies of major incidents by DDoS attacks based on the historical trend. The shaded area around the forecast line indicates the 80% confidence interval, providing a range within which future notable incidents anticipated from DDoS attack frequencies are likely to fall. This visualization is indicative of the estimated trend for very notable incidents expected from DDoS attacks over the next five years, reflecting a scenario with minimal technological advancement and persistent geopolitical tensions. The inclusion of confidence intervals is important as it illustrates the range of uncertainty in these predictions, acknowledging the inherent unpredictability in forecasting complex phenomena like cyber threats. While this model provides a statistically informed estimate based on past data, the actual future occurrences may vary, underscoring the importance of ongoing monitoring and adaptation in cybersecurity strategies. This forecast serves as an insightful tool for planning and preparedness, helping stakeholders to imagine, anticipate and mitigate potential cybersecurity major challenges within a defined range of possibilities.

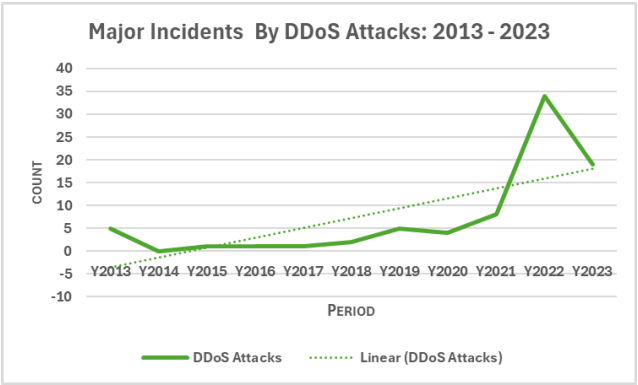


FIGURE 5. Trend of major DDoS incidents: 2013 - 2023.

V. DISCUSSION

A. IMPLICATION #1: DDoS ATTACKS' TREND

With reference to Figure 5 (plotted from Table 1, 2, & 3), the trend in DDoS attacks from 2013 to 2023, as outlined in the data, reveals a significant evolution in the frequency of these major incidents over the decade. In the early years (2013-2016), the number of DDoS attacks recorded each year was relatively low, with an average of less than two major incidents per year. There was a noticeable increase in 2019, followed by a marked surge in 2020 and 2022. The spike in 2020 could be attributed to the global shift towards increased online activity and reliance on digital infrastructure due to the COVID-19 pandemic, presenting more opportunities for attackers [59], [60]. Similarly, the high count in 2022 indicates a continued preference for this type of attack technique, potentially due to advancements in attack technologies [56] or strategies, or perhaps an increase in the vulnerabilities exposed by expanding digital infrastructures across the globe [61].

Analyzing the trend further, the substantial increase in DDoS attacks in the later years, particularly from 2019 onwards, points towards a worrying escalation in both the capability and intent of cyber threat actors in utilizing DDoS methodologies [62], [63]. This trend could be reflective of the evolving sophistication of botnets [14] and the increasing availability of DDoS-for-hire services [64], [65], making it easier for attackers to launch large-scale attacks. Additionally, the fluctuating pattern, with a notable dip in 2023, could suggest a response to improved defensive strategies or a shift in the attackers' focus to other forms of cyber threats. These observations underscore the dynamic nature of cyber threats, where attacker tactics and defender capabilities are in a constant state of flux. The data from this decade-long period highlights the need for continued vigilance, adaptation, and investment in cybersecurity measures to counteract these evolving threats.

B. IMPLICATION #2: MALWARE ATTACKS' TREND

With reference to Figure 6 (plotted from Table 1, 2, & 3), the data depicting the trend in malware-related major incidents from 2013 to 2023 offers a revealing look into the evolving landscape of cyber threats. In the initial years (2013-2016), the frequency of malware attacks exhibited a gradual but steady increase, starting from a modest three incidents in 2013 to five by 2016. This steady growth could be indicative of the increasing sophistication and proliferation of malware tools [66], [67] and techniques. The relatively low but growing numbers in these early years might reflect the development phase of more advanced malware variants [68], [69], such as ransomware and spyware, as well as an increasing awareness and reporting of such incidents.

A significant surge is observed from 2017 onwards, with a notable peak in 2018 where the count reached 25 incidents, more than double the previous year's figure. This sharp increase could be attributed to several factors, including the widespread availability of malware-as-a-service [70], [71], the growing number of vulnerabilities in rapidly expanding digital infrastructures, and the increasing value of data in the digital economy, making malware attacks more lucrative [72], [73]. The years following 2018 show some fluctuation but maintain a generally high frequency of incidents, underscoring the persistent and evolving threat posed by malware. The year 2019 shows a slight dip, which might be due to improved cybersecurity measures or shifts in attack strategies, but the overall upward trend continues.

The later years of the timeline, particularly 2022 and 2023, show a marked and continuous rise in malware incidents, with 2023 recording the highest number at 40 major incidents. This could be reflective of multiple factors: the refinement of malware techniques, the increasing digitization of various sectors making them more vulnerable to attacks, and perhaps the impact of global events like the COVID-19 pandemic which have accelerated the digitization process and potentially exposed new vulnerabilities [59]. This sustained increase over the years clearly indicates that malware remains a preferred tool for cybercriminals, evolving in complexity and impact. It underscores the necessity for continuous advancements in malware detection and prevention technologies, along with heightened vigilance and proactive measures from organizations and individuals to protect against these ever-present and evolving digital threats.

C. IMPLICATION #3: CORRELATION OF DDoS AND MALWARE ATTACKS' TRENDS

With reference to Figures 7 & 8, the trends in DDoS and malware-related major incidents from 2013 to 2023, when examined in parallel, reveal some intriguing correlations and divergences that shed light on the evolving landscape of cyber threats. Initially, from 2013 to 2016, both types of attacks showed a relatively low frequency, with malware attacks occurring slightly more frequently than DDoS attacks.

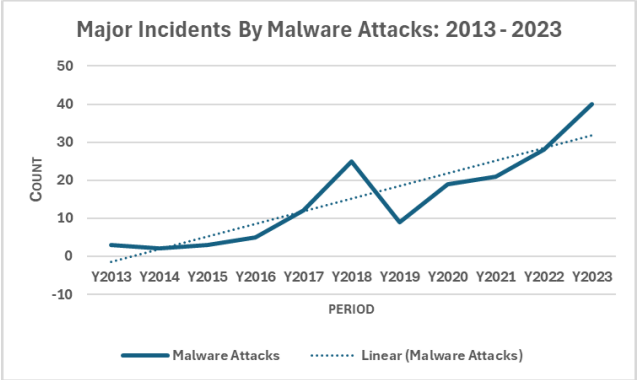


FIGURE 6. Trend of major malware incidents: 2013 - 2023.

This period could be characterized by a developing phase in the cyber threat landscape, where attackers were possibly refining their techniques and tools to cause major damages, leading to a moderate but steady occurrence of incidents. The slightly higher occurrence of malware attacks during these years might suggest an early inclination towards methods focused on data breach and financial gain, which malware typically facilitates more directly than DDoS attacks.

A notable divergence in the trends begins to emerge around 2017 and becomes more pronounced in the following years. In 2018, malware attacks spiked dramatically, more than doubling the previous year's figures, whereas DDoS attacks showed a more gradual increase. This spike in malware incidents could be attributed to the increasing value of data and the proliferation of ransomware, making such attacks more appealing to cybercriminals. In contrast, the steady increase in DDoS attacks might reflect a parallel development in attack technology, like the growing use of botnets. However, the sharp rise in DDoS attacks in 2022, reaching 34 major incidents, suggests a possible shift in attacker preferences or an increase in vulnerabilities exposed by expanding digital infrastructures, possibly accelerated by the global pandemic.

Towards the end of the timeline, in 2023, while malware attacks continue to rise, reaching their peak at 40 major incidents, DDoS attacks show a notable decrease from the previous year. This decrease could indicate a temporary shift in attacker focus or an improvement in DDoS mitigation techniques. However, the consistently high numbers of malware attacks underscore their persistent allure to cybercriminals, likely due to the lucrative prospects of data theft and ransom demands. The correlation between these trends suggests an adaptive and responsive cyber threat environment, where attackers continuously evolve their strategies, and the type of attack they favor can shift based on various factors, including technological advancements, global events, and the evolving cybersecurity landscape. This dynamic interplay highlights the need for equally adaptive and comprehensive cybersecurity strategies that address the full spectrum of potential threats.

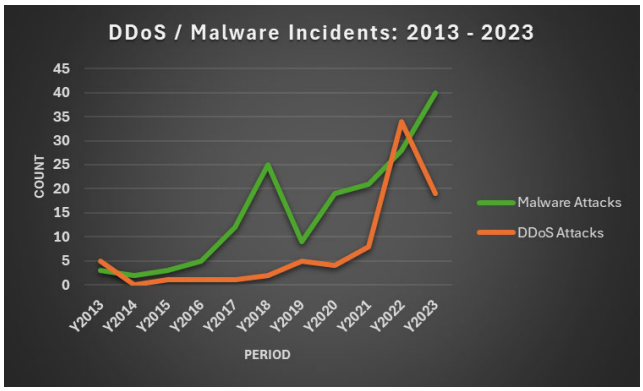


FIGURE 7. Trend of DDoS & malware incidents: 2013 - 2023.

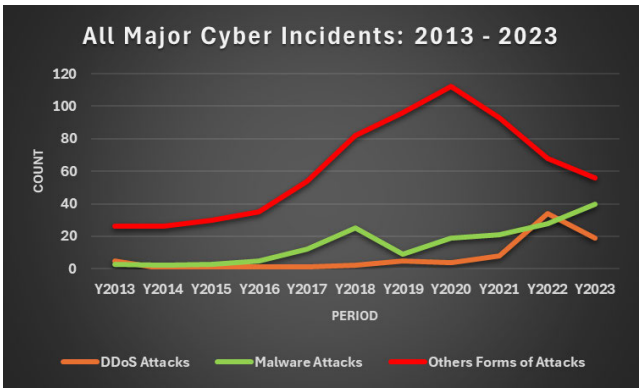


FIGURE 9. Chart of DDoS, malware & other incidents: 2013 - 2023.

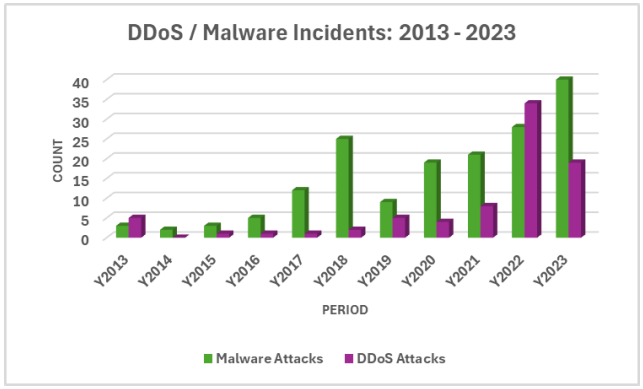


FIGURE 8. Chart of DDoS & malware incidents: 2013 - 2023.

D. IMPLICATION #4: DDoS, MALWARE AND OTHER ATTACKS' TRENDS

Although deep-diving into the other attack methodologies is outside the scope of this study but just to echo the fact that there were many other techniques used by threat actors, we briefly discuss our observation in this subsection. With reference to Figure 9, the trend in "Other Forms of Attacks" from 2013 to 2023, encompassing phishing, zero-day exploits, password-related attacks, exploitation of unpatched vulnerabilities, and IoT attacks [1], presents a comprehensive picture of the cyber threat landscape beyond DDoS and malware incidents. Initially, in 2013, these other forms of attacks were collectively significantly higher than DDoS and malware incidents, suggesting a diverse range of tactics employed by cybercriminals. The steady increase in these other collective attacks, peaking in 2020 with total 112 major incidents, indicates an expanding and evolving attack surface. This peak could be attributed to the rapid digital transformation and increased online activity prompted by the global pandemic, presenting more opportunities for varied cyber threats. The high frequency of these attacks, particularly in comparison to DDoS and malware, underscores the multifaceted nature of cyber threats, where attackers are not limited to a single type of attack but rather employ a wide array of techniques to exploit different vulnerabilities.

The implications of this trend in relation to DDoS and malware incidents are significant. The consistent high numbers in other forms of attacks suggest that while DDoS and malware are prevalent and serious threats, they are part of a broader spectrum of cybercriminal activities. The diversity in attack types reflects the adaptability and innovation of threat actors, who continually evolve their strategies to exploit new vulnerabilities and bypass security measures. For instance, the presence of zero-day exploits and attacks on unpatched vulnerabilities indicates a focus on exploiting system weaknesses before they can be addressed. Similarly, the presence of phishing and password-related attacks highlights the ongoing challenge of human-factor vulnerabilities. This diversity necessitates a multi-layered and dynamic approach to cybersecurity, where defenses are not solely focused on preventing known threats like DDoS and malware but are also equipped to anticipate and respond to a range of evolving tactics.

Furthermore, the trend in these other forms of attacks, especially the gradual decline after 2020, may reflect the improving cybersecurity measures and increased awareness among organizations and individuals. However, the consistently higher numbers compared to DDoS and malware incidents suggest that these other forms of attacks when combined as a group remain a preferred strategy for many cybercriminals, likely due to their effectiveness and the continuous emergence of new technologies and vulnerabilities. This, we argue, highlights the ongoing need for comprehensive cybersecurity strategies that address all potential attack vectors. It also underscores the importance of continued vigilance, investment in emerging security technologies, and education to mitigate the broad spectrum of cyber threats effectively. The data clearly indicates that while DDoS and malware are critical areas of focus, they represent only a part of the diverse and dynamic cyber threat landscape.

While individually, each category within the "Other Forms of Attacks" — encompassing techniques like phishing, zero-day exploits, password-related attacks, exploitation of

unpatched vulnerabilities, and IoT attacks — records fewer occurrences compared to either DDoS or malware incidents, their combined frequency paints a different picture. When aggregated, these diverse attack types collectively surpass the numbers of both DDoS and malware incidents. This aggregated data underscores a crucial aspect of the cyber threat landscape: while high-profile attack types like DDoS and malware often capture the spotlight, the cumulative impact and frequency of other, less-publicized attack methods form a significant part of the cyber threat environment. This trend highlights the importance of a comprehensive approach to cybersecurity that addresses the full spectrum of potential attack techniques, rather than focusing disproportionately on the more notorious ones.

E. IMPLICATION #5: RELIABILITY AND VALIDITY

The use of the ARIMA (AutoRegressive Integrated Moving Average) model in this study contributes to the reliability aspect of the research, particularly in the context of time series forecasting. Given how reliability in research refers to the consistency and stability of the results over time. The ARIMA model, known for its efficacy in analyzing and forecasting time series data, applies a systematic, statistical approach to understanding past trends and predicting future occurrences as echoed in the methodology section. By incorporating historical data on cyber attacks and applying a well-established statistical method, the study ensures that the forecasting process is repeatable and consistent. This adherence to a standardized, quantitative methodology enhances the reliability of the study's predictions, as the same procedure can be applied to similar datasets to obtain comparable results. Moreover, the model's ability to account for various patterns and fluctuations in the data (like trends and seasonality) further adds to its reliability, offering a robust framework for understanding and forecasting cyber threat trends.

However, the validity of the ARIMA model in this study, which refers to the accuracy and appropriateness of the model in representing the real-world phenomenon it aims to forecast, can be more nuanced. While there is no question with how ARIMA is proficient in capturing and extrapolating trends based on historical data, it is noteworthy to mention that its validity in predicting future cyber attacks like DDoS and malware hinges on the assumption that past patterns will continue into the future. This assumption may not always hold true in this rapidly evolving field of cybersecurity, where new threats, technologies, and defensive strategies continuously emerge and evolve as well. The model's validity might be challenged by unforeseen factors, such as sudden technological advancements, another major pandemic situation, shifts in attacker tactics, or changes in global cybersecurity policies. Therefore, while the ARIMA model provides a statistically sound method for forecasting based on historical data that we derived, its predictions should be interpreted with an understanding of its limitations in capturing the dynamic and unpredictable nature of cyber threats. To enhance the validity of the study, it's crucial to complement the ARIMA model with other forms of analysis that consider these evolving aspects of cybersecurity - which is one of the areas that we intend to explore in future studies.

F. BROADER CONTRIBUTION OF THIS STUDY

We think that this study marks a notable advancement in the realm of cybersecurity research by integrating a sophisticated forecasting approach to predict the future landscape of cyber threats, particularly focusing on Distributed Denial of Service (DDoS) and malware incidents. Unlike traditional analyses that predominantly offer descriptive insights into past and present cybersecurity challenges, our research employs the AutoRegressive Integrated Moving Average (ARIMA) model to project future threat trends. This methodological innovation allows for a more dynamic understanding of cyber threats, moving beyond retrospective analysis to provide anticipatory insights. The use of ARIMA models, renowned for their efficacy in time series forecasting, enables the identification of patterns and trends in historical cybersecurity incident data, thereby offering a scientifically grounded basis for predicting future occurrences.

The contribution of this study, we argue extends into the practical domain, offering substantial value to business organizations and policymakers engaged in cybersecurity planning and strategy development. By presenting a forward-looking perspective on potential cyber threats, the research equips stakeholders with the knowledge to preemptively allocate resources, enhance security protocols, and develop comprehensive risk management strategies. This proactive approach to cybersecurity, informed by robust statistical forecasting, represents a paradigm shift from reactive to anticipatory threat management. Furthermore, the study's exploration of correlations between cyber incidents and various influencing factors, such as geopolitical dynamics and financial motives, enriches the analytical depth, providing nuanced insights into the multifaceted nature of cyber threats. This detailed understanding aids in tailoring more effective and targeted cybersecurity measures, ultimately contributing to the resilience and security of digital infrastructures in an increasingly interconnected world.

VI. LIMITATION AND FUTURE STUDY

Identifying the research gap in DDoS attack detection cases and formulating recommendations for enhanced detection methodologies represent critical questions that, while outside the scope of our current study, are pivotal for advancing the field of cybersecurity. These questions underscore the necessity to explore and innovate beyond conventional detection techniques, addressing the evolving complexity and sophistication of DDoS attacks. As part of our commitment to contributing to a safer digital environment, future studies will delve into these areas, aiming to bridge the existing research gap by identifying shortcomings in current detection strategies and proposing advanced, adaptable methods for early and accurate DDoS attack identification. This

forward-looking research agenda is crucial for developing more resilient cybersecurity frameworks, ensuring that detection mechanisms keep pace with the rapid advancements in attack methodologies and continue to protect critical digital infrastructures effectively.

A. LIMITED DATA SOURCES

1) LIMITATION

The study primarily relies on data from the CSIS report, cross-referenced with insights obtained from DBIR and GCI, which might not encompass all major incidents (except the ones publicly reported) or could have inherent biases in reporting.

2) HYPOTHESIS TESTING IN FUTURE STUDY

In dealing with this limitation, future research could hypothesize that incorporating additional data sources, like other available and reputable independent cybersecurity incident databases or industry-specific reports, would provide a more comprehensive understanding of cyber threats. Statistical tests could compare findings from expanded data sets to the current study's results.

B. GEOGRAPHICAL AND SECTORAL BIAS

1) LIMITATION

The study may have unintentional geographical or sectoral biases, not fully representing certain regions or industries.

2) HYPOTHESIS TESTING IN FUTURE STUDY

A hypothesis could be formulated that including more diverse geographical and sectoral data will significantly alter the understanding of cyber threat patterns. Analyzing the variance in attack types and frequencies across different regions and sectors could test this hypothesis.

C. TIMEFRAME LIMITATION

1) LIMITATION

Focusing on the period from 2013 to 2023 may exclude emerging trends or historical patterns outside this timeframe.

2) HYPOTHESIS TESTING IN FUTURE STUDY

By hypothesizing that extending the study's timeframe (e.g., to 2003-2033) will reveal different evolution patterns in cyber threats, future research can employ statistical trend analysis to explore the validity of this hypothesis.

D. TYPE OF ATTACKS CATEGORIZATION

1) LIMITATION

The categorization of attacks into DDoS, malware, and others might oversimplify the complexity of attack techniques.

2) HYPOTHESIS TESTING IN FUTURE STUDY

Future studies could hypothesize that a more granular categorization of attack types will provide deeper insights. Statistical analysis could be used to compare the variance and significance of cyber threats within more specific categories.

E. DYNAMIC NATURE OF CYBER THREATS

1) LIMITATION

The study might not fully account for the rapidly evolving nature of cyber threats.

2) HYPOTHESIS TESTING IN FUTURE STUDY

A hypothesis could state that cyber threats evolve at a rate that significantly outpaces the development of defensive strategies. This could be tested by analyzing the rate of emergence of new types of cyber threats and the time taken to effectively respond to them, using statistical models that track evolution over time.

VII. CONCLUSION

A. HUMAN-CENTERED COMPUTING

From the perspective of Human-Centered Computing [74], our study underscores the crucial role of user behavior and interaction in the cybersecurity landscape. The presence of phishing and password-related attacks in the other forms of attacks referenced in Figure 9, in particular, highlights the need for more intuitive and user-friendly security systems that can be effectively utilized by individuals without extensive technical expertise [75], [76]. We argue that incorporating principles of human-centered design in cybersecurity solutions has potentials of significantly reducing the vulnerability to such attacks. This approach requires a deeper understanding of user behavior, proactive educational initiatives, and the development of more engaging and accessible cybersecurity tools that cater to the varied needs and skill levels of users.

B. INSIGHTS FOR POLICYMAKERS AND CYBERSECURITY INDUSTRY

For policymakers and the cybersecurity industry, this study offers pivotal insights into the evolving threat landscape and the effectiveness of current strategies. The data reveals the necessity for continuous adaptation and the implementation of very robust, multi-layered security strategies. Policymakers should consider these findings to inform the development of comprehensive cybersecurity policies (at national or sub-national levels) and frameworks, emphasizing the need for international cooperation, information sharing (at national and sub-national levels), especially given the global nature of these threats. The industry, on the other hand, can also leverage this information to innovate and improve cybersecurity products and services, ensuring they are equipped to handle the increasingly sophisticated nature of cyber threats like DDoS and malware attacks that are causing major cyber incidents.

C. DATA SECURITY AND PREVENTION OF DATA BREACHES

In terms of data security, the persistent rise in malware attacks, particularly those targeting data theft, stresses the

importance of advancing data protection measures [77] across board. We propose that organizations - both public and private sectors should enhance the prioritization of the implementation of advanced encryption techniques [78], [79], regular security audits [80], and the adoption of a zero-trust security model [81], [82] to safeguard sensitive data. Additionally, fostering a culture of security within public and private organizations, where sensitive data protection is a shared responsibility [83], [84], is crucial in minimizing the risks of data breaches.

D. ARGUMENT FOR CONTINUOUS RESEARCH

Finally, the argument for continuous research in cybersecurity is compellingly illustrated by the study's findings. The dynamic and rapidly evolving nature of cyber threats, as evidenced by the fluctuating trends in DDoS, malware, and other forms of attacks, highlights that cybersecurity is a moving target. Ongoing research is essential not only to keep pace with the evolving methodology and tactics of cybercriminals but also to anticipate potential future threats and develop both proactive and reactive security defenses [85], [86]. This requires a sustained commitment to cybersecurity research, with a focus on emerging technologies, information security threat intelligence [87], [88], and the development of more innovative defense mechanisms.

E. FINAL THOUGHTS

In conclusion, this comprehensive study of cybersecurity incidents from 2013 to 2023 provides critical insights and underscores the necessity for a holistic, adaptable, and continuously evolving approach to cybersecurity across various domains. This research addressed the research question that we posed at the beginning of this endeavor - "How have the defensive strategies against DDoS and Malware attacks effectively impacted the trends of these attacks over the last decade?" by analyzing a decade's worth of data on the publicly reported major cybersecurity incidents. The study revealed a notable evolution in both DDoS and malware attack patterns in major incidents, with fluctuations in their frequencies correlating to advancements in defensive technologies. The increased major cyber incident of DDoS attacks in later years, despite advancements in mitigation techniques, suggests a complex interplay between evolving attack strategies and defensive responses. Similarly, the steady rise in major malware attacks, despite enhanced detection and prevention tools, indicates a persistent challenge in curbing these threats. These findings suggest that while defensive strategies have significantly evolved, their effectiveness in reducing the overall incidence of these major cyber attacks has been mixed, emphasizing the need for continual advancement in cyber defense approaches and strategies.

However, the study (as already been clearly illustrated in the "Limitation & Future Study Section" of this study) identifies some limitations and gaps that future research should address. One gap not mentioned in the Limitation & Future Study Section is the limited exploration of the impact of emerging technologies like artificial intelligence and machine learning in both perpetrating and defending against major cyber attacks. Additionally, this study acknowledges a need for a deeper understanding of the role of human factors in cybersecurity, particularly in the context of increasing social engineering attacks. Future research could also benefit from a more granular analysis of sector-specific impacts and defenses against cyber threats. Addressing these gaps would provide a more comprehensive understanding of the cyber threat landscape and the effectiveness of cybersecurity defensive strategies, thereby guiding the development of more and efficiently robust and adaptive cybersecurity measures in the future.

ACKNOWLEDGMENT

The authors would like to thank to the School of Information Technology, University of Cincinnati, Cincinnati, OH, USA, for providing them with the tools, environment, and guidance to conduct this study. The primary dataset used or referenced in this study is derived from the Significant Cyber Incidents report that is consolidated by the Center for Strategic and International Studies (CSIS) but cross-referenced and validated with insights derived from Data Breach Investigation Reports (DBIR). Any perspective, findings, observation, interpretations, recommendation, and conclusion expressed in this material are those of the authors and do not necessarily reflect the views of either the CSIS or the DBIR.

REFERENCES

[1] Center for Strategic and International Studies, Significant Cyber Incidents Since 2006. (2023). *Significant Cyber Incidents*. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[2] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Comput. Secur.*, vol. 72, pp. 212–233, Jan. 2018.

[3] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The emerging threat of Ai-driven cyber attacks: A review," *Appl. Artif. Intell.*, vol. 36, no. 1, Dec. 2022, Art. no. 2037254.

[4] O. I. Falowo, S. Popoola, J. Riep, V. A. Adewopo, and J. Koch, "Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents," *IEEE Access*, vol. 10, pp. 134038–134051, 2022.

[5] S. U. Rehman, M. Khaliq, S. I. Imtiaz, A. Rasool, M. Shafiq, A. R. Javed, Z. Jalil, and A. K. Bashir, "DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU)," *Future Gener. Comput. Syst.*, vol. 118, pp. 453–466, May 2021.

[6] S. Lysenko, K. Bobrovnikova, R. Shchuka, and O. Savenko, "A cyber-attacks detection technique based on evolutionary algorithms," in *Proc. IEEE 11th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, May 2020, pp. 127–132.

[7] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: A systematic review," *Soft Comput.*, vol. 27, no. 18, pp. 13039–13075, Sep. 2023.

[8] A. B. Dehkordi, M. Soltanaghaei, and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *J. Supercomput.*, vol. 77, no. 3, pp. 2383–2415, Mar. 2021.

[9] S. Xu, Y. Xia, and H.-L. Shen, "Analysis of malware-induced cyber attacks in cyber-physical power systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 12, pp. 3482–3486, Dec. 2020.

[10] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on ransomware: Evolution, taxonomy, and defense solutions," *ACM Comput. Surv.*, vol. 54, no. 11, pp. 1–37, Jan. 2022.

[11] M. N. Alenezi, H. K. Alabdulrazzaq, A. A. Alshaher, and M. M. Alkharang, "Evolution of malware threats and techniques: A review," *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 3, pp. 326–337, Apr. 2022.

[12] B. Madnick, K. Huang, and S. Madnick, "The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process," *Inf. Secur. J., A Global Perspective*, pp. 1–22, Apr. 2023.

[13] R. Bell, E. Vasserman, and E. Sayre, "A longitudinal study of students in an introductory cybersecurity course," in *Proc. ASEE Annu. Conf. Expo.*, 2014, pp. 24–61.

[14] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS attacks: Trends and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2242–2270, 4th Quart., 2015.

[15] A. Wang, W. Chang, S. Chen, and A. Mohaisen, "Delving into Internet DDoS attacks by botnets: Characterization and analysis," *IEEE/ACM Trans. Netw.*, vol. 26, no. 6, pp. 2843–2855, Dec. 2018.

[16] M. Dimolianis, A. Pavlidis, D. Kalogeras, and V. Maglaris, "Mitigation of multi-vector network attacks via orchestration of distributed rule placement," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, Apr. 2019, pp. 162–170.

[17] K. K. Brahma, S. Sarmah, C. Kalita, and R. Ghosh, "Detection of multi-vector DDoS attack," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 6, pp. 847–851, Jun. 2019.

[18] V. S. Sathyanarayan, P. Kohli, and B. Bruhadeshwar, "Signature generation and detection of malware families," in *Proc. 13th Australas. Conf. Inf. Secur. Privacy*, Springer, 2008, pp. 336–349.

[19] M. Barat, D.-B. Prelipcean, and D. T. Gavriluţ, "A study on common malware families evolution in 2012," *J. Comput. Virol. Hacking Techn.*, vol. 9, no. 4, pp. 171–178, Nov. 2013.

[20] A. Gazet, "Comparative analysis of various ransomware virii," *J. Comput. Virol.*, vol. 6, no. 1, pp. 77–90, Feb. 2010.

[21] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," *IET Netw.*, vol. 7, no. 5, pp. 321–327, Sep. 2018.

[22] D. Albright, P. Brannan, and C. Walrond, "Stuxnet malware and Natanz: Update of ISIS December 22, 2010 report," *Inst. Sci. Int. Secur.*, vol. 15, p. 739883, Feb. 2010.

[23] S. Collins and S. McCombie, "Stuxnet: The emergence of a new cyber weapon and its implications," *J. Policing, Intell. Counter Terrorism*, vol. 7, no. 1, pp. 80–91, Apr. 2012.

[24] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," *Arabian J. Sci. Eng.*, vol. 42, no. 2, pp. 425–441, Feb. 2017.

[25] A. Mishra, B. B. Gupta, and R. C. Joshi, "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," in *Proc. Eur. Intell. Secur. Informat. Conf.*, Sep. 2011, pp. 286–289.

[26] O. I. Falowo, I. Okpala, E. Kojo, S. Azumah, and C. Li, "Exploration of various machine learning techniques for identifying and mitigating DDoS attacks," in *Proc. 20th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, Aug. 2023, pp. 1–7.

[27] M. Darwish, A. Ouda, and L. F. Capretz, "Cloud-based DDoS attacks and defenses," in *Proc. Int. Conf. Inf. Soc.*, Jun. 2013, pp. 67–71.

[28] T. Vissers, T. S. Somasundaram, L. Pieters, K. Govindarajan, and P. Hellinckx, "DDoS defense system for web services in a cloud environment," *Future Gener. Comput. Syst.*, vol. 37, pp. 37–45, Jul. 2014.

[29] A. Saracino, D. Sgandurra, G. Dini, and F. Martinelli, "MADAM: Effective and efficient behavior-based Android malware detection and prevention," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 1, pp. 83–97, Jan. 2018.

[30] S. Sen, E. Aydogan, and A. I. Aysan, "Coevolution of mobile malware and anti-malware," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2563–2574, Oct. 2018.

[31] S. Treadwell and M. Zhou, "A heuristic approach for detection of obfuscated malware," in *Proc. IEEE Int. Conf. Intell. Secur. Informat.*, Jun. 2009, pp. 291–299.

[32] N. Miramirkhani, M. P. Appini, N. Nikiforakis, and M. Polychronakis, "Spotless sandboxes: Evading malware analysis systems using wear-and-tear artifacts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 1009–1024.

[33] M. Vasilescu, L. Gheorghe, and N. Tapus, "Practical malware analysis based on sandboxing," in *Proc. RoEduNet Conf. 13th Ed., Netw. Educ. Res. Joint Event RENAM 8th Conf.*, Sep. 2014, pp. 1–6.

[34] W. U. Hassan, A. Bates, and D. Marino, "Tactical provenance analysis for endpoint detection and response systems," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 1172–1189.

[35] Intersoft Consulting. (2018). *General Data Protection Regulation (GDPR)*. [Online]. Available: https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf

[36] A. Nikolopoulou, "The Directive on security of networks and information systems (NIS Directive)," 2019.

[37] D. Markopoulou, V. Papakonstantinou, and P. de Hert, "The new EU cybersecurity framework: The NIS directive, ENISA's role and the general data protection regulation," *Comput. Law Secur. Rev.*, vol. 35, no. 6, Nov. 2019, Art. no. 105336.

[38] Cybersecurity and Infrastructure Security Agency. (2023). *Cybersecurity Advisories*. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories

[39] M. Scofield, "Benefiting from the NIST cybersecurity framework," *Inf. Manage.*, vol. 50, no. 2, p. 25, 2016.

[40] P. F. Edemekong, P. Annamaraju, and M. J. Haydel, "Health insurance portability and accountability act," 2018.

[41] J. R. Reagan, "Federal information security management act (FISMA): Policy analysis and examination of agency implementation," 2010.

[42] E. Gorian, "Singapore's cybersecurity act 2018: A new generation standard for critical information infrastructure protection," in *Proc. Int. Sci. Technol. Conf. Smart Technol. Innov. Design Control Technol. Processes Objects, Economy Prod.*, Springer, 2018, pp. 1–9.

[43] W. Aikawa, "Japan's cybersecurity policy," in *Telecommunications Policies of Japan*, 2020, pp. 133–148.

[44] J. Sunkpho, S. Ramjan, and C. Ottamakorn, "Cybersecurity policy in ASEAN countries," in *Proc. 17th Annu. Secur. Conf.*, 2018, pp. 1–7.

[45] C. H. Heinl, "Regional cybersecurity: Moving toward a resilient ASEAN cybersecurity regime," *Asia Policy*, vol. 1, no. 1, pp. 131–159, Jul. 2014.

[46] P. Minkkinen, "Practical applications of sampling theory," *Chemometric Intell. Lab. Syst.*, vol. 74, no. 1, pp. 85–94, Nov. 2004.

[47] W. J. Potter and D. Levine-Donnerstein, "Rethinking validity and reliability in content analysis," *J. Appl. Commun. Res.*, vol. 27, no. 3, pp. 258–284, Aug. 1999.

[48] F. Costin, W. T. Greenough, and R. J. Menges, "Student ratings of college teaching: Reliability, validity, and usefulness," *Rev. Educ. Res.*, vol. 41, no. 5, p. 511, Dec. 1971.

[49] T. R. Knapp and R. O. Mueller, "Reliability and validity of instruments," in *The Reviewer's Guide to Quantitative Methods in the Social Sciences*, 2010, pp. 337–342.

[50] G. Werner, S. Yang, and K. McConky, "Time series forecasting of cyber attack intensity," in *Proc. 12th Annu. Conf. Cyber Inf. Secur. Res.*, Apr. 2017, pp. 1–3.

[51] N. R. Pokhrel, H. Rodrigo, and C. P. Tsokos, "Cybersecurity: Time series predictive modeling of vulnerabilities of desktop operating system using linear and non-linear approach," *J. Inf. Secur.*, vol. 8, no. 4, pp. 362–382, 2017.

[52] R. H. Shumway, D. S. Stoffer, R. H. Shumway, and D. S. Stoffer, "ARIMA models," in *Time Series Analysis and Its Applications: With R Examples*, 2017, pp. 75–163.

[53] S. L. Ho and M. Xie, "The use of ARIMA models for reliability forecasting and analysis," *Comput. Ind. Eng.*, vol. 35, nos. 1–2, pp. 213–216, Oct. 1998.

[54] V-Business. (2023). *Verizon Data Breach Investigations Report (DBIR)*. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[55] R. Bruggemann, P. Koppatz, M. Scholl, and R. Schuktomow, "Global cybersecurity index (GCI) and the role of its 5 pillars," *Social Indicators Res.*, vol. 159, no. 1, pp. 125–143, Jan. 2022.

[56] W. Xiong, E. Legrand, O. Åberg, and R. Lagerström, "Cyber security threat modeling based on the MITRE enterprise ATT&CK matrix," *Softw. Syst. Model.*, vol. 21, no. 1, pp. 157–177, Feb. 2022.

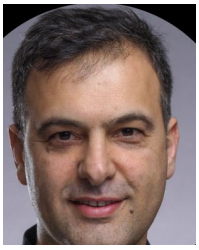
[57] R. G. Lomax and D. L. Hahs-Vaughn, *An Introduction to Statistical Concepts*. Evanston, IL, USA: Routledge, 2013.

[58] *Sample Size Calculator*. Accessed: Aug. 28, 2023. [Online]. Available: https://goodcalculators.com/sample-size-calculator/

[59] D. Strusani and G. V. Houngbonon, "What COVID-19 means for digital infrastructure in emerging markets," 2020.

[60] O. Henfridsson and B. Bygstad, "The generative mechanisms of digital infrastructure evolution," *MIS Quart.*, vol. 37, no. 3, pp. 907–931, Mar. 2013.
[61] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3723–3768, 4th Quart., 2019.
[62] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of recent detection methods for HTTP DDoS attack," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–10, Jan. 2019.
[63] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," *Expert Syst. Appl.*, vol. 34, no. 3, pp. 1659–1665, Apr. 2008.
[64] R. Brunt, P. Pandey, and D. McCoy, "Booted: An analysis of a payment intervention on a DDoS-for-hire service," in *Proc. Workshop Econ. Inf. Secur.*, 2017, pp. 6–26.
[65] D. Douglas, J. J. Santanna, R. de Oliveira Schmidt, L. Z. Granville, and A. Pras, "Booters: Can anything justify distributed denial-of-service (DDoS) attacks for hire?" *J. Inf., Commun. Ethics Soc.*, vol. 15, no. 1, pp. 90–104, Mar. 2017.
[66] T. Herr, "Malware counter-proliferation and the Wassenaar arrangement," in *Proc. 8th Int. Conf. Cyber Conflict (CyCon)*, May 2016, pp. 175–190.
[67] T. Herr, "Countering the proliferation of malware: Targeting the vulnerability lifecycle," Belfer Cyber Secur. Project, White Paper Ser., 2017.
[68] K. Alzarooni, "Malware variant detection," Ph.D. dissertation, Univ. College London, London, U.K., 2012.
[69] A. A. Al-Hashmi, F. A. Ghaleb, A. Al-Marghilani, A. E. Yahya, S. A. Ebad, M. Saqib, and A. A. Darem, "Deep-ensemble and multifaceted behavioral malware variant detection model," *IEEE Access*, vol. 10, pp. 42762–42777, 2022.
[70] R. Davidson, "The fight against malware as a service," *Netw. Secur.*, vol. 2021, no. 8, pp. 7–11, Aug. 2021.
[71] C. Karapapas, I. Pittaras, N. Fotiou, and G. C. Polyzos, "Ransomware as a service using smart contracts and IPFS," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 1–5.
[72] M. van Eeten, J. M. Bauer, J. Groenewegen, and W. Lemstra, "The economics of malware," TPRC, Aug. 2007.
[73] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The ransomware-as-a-service economy within the darknet," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101762.
[74] J. Karat and C. M. Karat, "The evolution of user-centered focus in the human-computer interaction field," *IBM Syst. J.*, vol. 42, no. 4, pp. 532–541, 2003.
[75] D. Balfanz, G. Durfee, D. K. Smetters, and R. E. Grinter, "In search of usable security: Five lessons from the field," *IEEE Secur. Privacy Mag.*, vol. 2, no. 5, pp. 19–24, Sep. 2004.
[76] K. Kostiainen, "Intuitive security initiation using location-limited channels," M.S. thesis, Helsinki Univ. Technol., Apr. 2004, vol. 14, p. 86.
[77] J. Wong, T. Henderson, and K. Ball, "Data protection for the common good: Developing a framework for a data protection-focused data commons," *Data Policy*, vol. 4, p. e3, Oct. 2022.
[78] E. Thambiraja, G. Ramesh, and D. R. Umarani, "A survey on various most common encryption techniques," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 2, no. 7, 2012.
[79] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *Int. J. Comput. Sci. Eng.*, vol. 4, no. 5, p. 877, 2012.
[80] C. Onwubiko, "A security audit framework for security management in the enterprise," in *Proc. 5th Int. Conf. Global Secur., Saf., Sustainability*, Springer, 2009, pp. 9–17.
[81] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–13, Jun. 2022.
[82] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102436.
[83] R. Thakur, "A shared responsibility for a more secure world," *Global Governance*, vol. 11, no. 3, pp. 281–289, 2005.
[84] P. T. J. Wolters, "The security of personal data under the GDPR: A harmonized duty or a shared responsibility?" *Int. Data Privacy Law*, vol. 7, no. 3, pp. 165–178, Aug. 2017.
[85] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 709–745, 1st Quart., 2020.
[86] F. Y.-S. Lin, Y.-S. Wang, and M.-Y. Huang, "Effective proactive and reactive defense strategies against malicious attacks in a virtualized honeynet," *J. Appl. Math.*, vol. 2013, pp. 1–11, Jul. 2013.
[87] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence-issue and challenges," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 10, no. 1, pp. 371–379, 2018.
[88] M. Bromiley, "Threat intelligence: What it is, and how to use it effectively," *SANS Inst. InfoSec Reading Room*, vol. 15, p. 172, Jun. 2016.

OLUFUNSHO I. FALOWO received the B.A. degree in philosophy from the University of Lagos, Nigeria, in 2004, and the M.B.A. degree from the Isenberg School of Management, University of Massachusetts, in 2021. He is currently pursuing the Ph.D. degree in information technology with the School of Information Technology, University of Cincinnati, Cincinnati, OH, USA. His research interests include cloud security, security information and event management, security incident detection and response, ethical computer hacking, and digital forensic investigation among others. He is a member of the International Information System Security Certification Consortium and the Information Systems Audit and Control Association. In 2021, he completed an executive education in Design Thinking: A Toolkit for Breakthrough Innovation at the Northwestern University Kellogg School of Management. In 2022, he completed executive education in Cybersecurity: Managing Risks in the Information Age at Harvard University. He completed an executive education in Behavioral Economics at The University of Chicago Booth School of Business, in 2022. He completed an executive education in Negotiation Strategies at The Yale School of Management, in 2022. He also completed an executive education in Building Resilience and Agility at London Business School, in 2022. He has been a Certified Information Systems Security Professional, since 2017, a Certified Information Security Manager, since 2020, a Certified Computer Hacking Forensic Investigator, since 2011, and a Certified Security Analyst, since 2010. He is also a certified ISO/IEC 27001:2005 Lead Implementer.



MURAT OZER received the first M.S. degree in public administration from the Public Administration Institute for Turkey and the Middle East, Ankara in 2006, and the second M.S. and Ph.D. degrees in criminal justice from the University of Cincinnati (UC), in 2007 and 2010, respectively. He is currently an Associate Professor with the School of Information Technology, UC. He works with law enforcement and correction agencies in the nation and develops certain web-based predictive analytical systems. His research interests include crime information to generate predictive data analytics for various public health problems, such as drug-related problems, street violence, and cybersecurity.

CHENGCHENG LI received the M.S. and Ph.D. degrees in computer science from Texas Tech University and the M.B.A. degree from the International University of Monaco. He is currently a Professor with the School of Information Technology, University of Cincinnati (UC). He developed an undergraduate track in cybersecurity that led to UC's designation as a National Center of Academic Excellence in Cyber Defense by the National Security Agency. The cybersecurity track was developed into a dedicated undergraduate degree in cybersecurity with more than 400 students enrolled, in 2022. He served as the Graduate Director of the School, from 2014 to 2020, and developed a Graduate Data-Driven Cybersecurity Certificate. He has served as the principal investigator of multiple grants funded by U.S. National Science Foundation and the National Security Agency with a total amount of more than U.S. $6 million. His research interests include cybersecurity and data science. One goal of his research is to convert cybersecurity challenges into data science tasks by using machine learning techniques.

JACQUES BOU ABDO received the Diplôme d'Ingénieur degree in electrical and electronics engineering from Lebanese University, Roumieh, Lebanon, in 2009, the B.B.A. degree in management from Lebanese University, Beirut, Lebanon, in 2010, the M.E. degree in telecommunication networks from the Saint Joseph University of Beirut, in 2011, the first Ph.D. degree in computer science (cybersecurity) from Sorbonne University, Paris, France, in 2014, and the second Ph.D. degree in management sciences (network economics, competition, and complexity economics) from Paris-Saclay University, Paris, in 2021. He is currently an Assistant Professor with the School of Information Technology, University of Cincinnati. He is an interdisciplinary researcher with expertise in complex systems, cybersecurity, cyber warfare, computational economics, and network economics. He is interested in the universality of laws governing networks and systems. His research has multiple applications, such as cyber and strategic deterrence, the flow of information and disinformation in irregular warfare, the flow of cyberattacks and network resiliency in cyber warfare, the flow of infectious diseases in biological warfare, and the resilience of supply chains.