Optimizing Bug Bounty Programs for Efficient Malware-Related Vulnerability Discovery

Semi Yulianto[1], Benfano Soewito[2], Ford Lumban Gaol[3], Aditya Kurniawan[4]
Computer Science Department, BINUS Graduate Program – Doctor of Computer Science,
Bina Nusantara University, Jakarta 11480, Indonesia

***Abstract*—Conventional security measures struggle to keep pace with the rapidly evolving threat of malware, which demands novel approaches for vulnerability discovery. Although Bug Bounty Programs (BBPs) are promising, they often underperform in attracting researchers, particularly in uncovering malware-related vulnerabilities. This study optimizes BBP structures to maximize engagement and target malware vulnerability discovery, ultimately strengthening cyber defense. Employing a mixed-methods approach, we compared public and private BBPs and analyzed the key factors influencing researcher participation and the types of vulnerabilities discovered. Our findings reveal a blueprint for effective malware-focused BBPs that enable targeted detection, faster patching, and broader software coverage. This empowers researchers and fosters collaboration within the cybersecurity community, significantly reducing the attack surface for malicious actors. However, challenges related to resource sustainability and legal complexity persist. By optimizing BBPs, we unlocked a powerful tool to fight cybercrime.**

Keywords*—Bug bounty; malware; vulnerability discovery; cyber defense

I. Introduction

Securing software systems is a crucial challenge in today's fast-changing digital environment. The effective management and discovery of vulnerabilities are significantly enhanced by strategic resource allocation [1]. In parallel, bug bounty programs have become a crucial component of cybersecurity, leveraging the collective global expertise of security researchers to identify and mitigate threats and provide incentives for their discoveries [2]. These programs also raise substantial ethical questions related to the monetization of cybersecurity vulnerabilities, necessitating an analysis of the associated moral implications [3]. Additionally, this study explored the characteristics of security bugs, which are critical for establishing a robust vulnerability management framework [4]. The efficacy of bug bounty programs has also been assessed in specific fields, such as blockchain technology, by evaluating their influence in these newer areas [5]. This introduction sets the stage for our examination of the delicate interplay between technical solutions and ethical considerations in managing software vulnerability.

The persistent threats posed by malware highlight the need for advanced vulnerability discovery techniques. Conventional security measures often fail to keep pace with the creativity of cyber threats, prompting the adoption of Bug Bounty Programs (BBPs) as of independent an effective alternative. These programs harness the expertise security researchers to find hidden vulnerabilities, yet questions remain about their effectiveness against malware-specific threats owing to the diverse structures and ecosystems in which they operate. Our study undertakes a thorough investigation of how the key elements of BBPs affect both the participation of researchers and the success of discovering vulnerabilities within the context of malware.

Our study highlights the challenges in attracting and retaining skilled researchers for BBPs driven by competitive pressures and inadequate reward systems, especially for intricate malware-related vulnerabilities. Additionally, the difficulty in identifying and prioritizing these vulnerabilities is exacerbated by the general lack of malware analysis expertise among program administrators and the complex nature of replicating attack chains. We also address the narrow scope of many BBPs and the difficulties in measuring their overall security impact, which hinders their ability to secure continuous support and funding. Our objective is to devise BBP strategies informed by malware analysis expertise, promote the reporting of malware-related vulnerabilities, and strengthen cybersecurity defenses.

Targeted bug bounty programs are expected to enhance malware detection by facilitating quicker identification and resolution of critical vulnerabilities, thus reducing opportunities for cyber-attackers. These programs are projected to bolster cyber defenses, as our findings could enhance threat intelligence and foster collaboration among researchers, platforms, and vendors, thereby creating a unified cybersecurity strategy. Furthermore, optimized BBPs are likely to offer cost-effectiveness and support the development of a community and standards within the cybersecurity field.

The remainder of this paper is organized as follows. In Section II, we provide an overview of the existing research on malware threats, conventional security measures, and the role of bug bounty programs in cybersecurity. The methodology in Section III outlines our study's approach and data collection methods, followed by the Results in Section IV, which presents empirical findings related to researcher participation and vulnerability discovery within the context of malware. In Section V, we interpret the results, discuss implications for cybersecurity practice and policy, and address limitations and avenues for further research. Finally, the conclusion summarizes the main findings and their significance, while the future work in Section VI identifies areas for future research and proposes potential research agendas or methodologies to address emerging challenges in malware detection and vulnerability discovery.

II. Literature Review

The rapidly evolving landscape of cybersecurity has necessitated innovative approaches to identifying and mitigating vulnerabilities, with Bug Bounty Programs (BBPs) emerging as a pivotal strategy. These programs incentivize ethical hackers to report software vulnerabilities and offer a unique blend of monetary and reputational rewards. This Literature Review in Section II delves into the multifaceted dimensions of BBPs, exploring their design, effectiveness, and intricate motivations of security researchers who participate in them. Drawing upon a diverse array of studies, we examine how BBPs serve as critical tools not only for enhancing digital security but also for fostering a proactive cybersecurity culture. Furthermore, we extend our focus to the specific realm of malware-related vulnerabilities, identify gaps in the current research, and underscore the potential of BBPs to address these challenges. Through a mixed-methods research lens, this review aims to provide a comprehensive overview of BBPs' impact of BBPs on software security, researcher engagement, and the broader cybersecurity ecosystem.

A. General Bug Bounty Program (BBP) Effectiveness and Design

Bug bounty programs have gained recognition as an effective strategy for organizations to encourage ethical hackers to report security vulnerabilities in their software. These programs aim to incentivize hackers to share vulnerabilities with legitimate organizations for monetary and reputational rewards as alternatives to selling or exploiting these vulnerabilities. By offering rewards to users reporting security vulnerabilities, bug bounty programs can effectively improve the security of digital technology platforms. Furthermore, bug bounty programs have been shown to enhance system reliability by optimally allocating resources to discover software vulnerabilities [1]. In addition, they allow developers to discriminate between different types of bugs, thus helping avoid the reputation costs of exploited bugs [2].

Bug bounty programs typically follow a crowdsourcing model in which there is an open call for people to anonymously test software [3]. However, bug bounty programs can be further improved by focusing on strategies that enhance their effectiveness [1]. It is essential to design bug bounty programs that consider the characteristics of security bugs, as effective tools for detecting and fixing software security bugs require a deep understanding of their characteristics [4].

Bug bounty programs have proven to be an effective means for organizations to incentivize ethical hackers to report security vulnerabilities in their software. They offer a valuable alternative to selling or exploiting vulnerabilities, and can significantly enhance the security and reliability of digital technology platforms.

B. Bug Bounty Programs (BBPs) and Vulnerabilities Related to Malware

Bug Bounty Programs (BBPs) have emerged as a crucial strategy for organizations to identify and address software vulnerabilities. These programs incentivize ethical hackers to report software security vulnerabilities, thereby allowing organizations to address these issues before they are exploited [5]. Bug bounty programs offer monetary and reputational rewards to hackers who share vulnerabilities with legitimate organizations, thereby deterring them from selling or exploiting these vulnerabilities [6]. For instance, Fiat Chrysler Automobiles collaborated with a San Francisco-based company to launch a bug-bounty program, offering rewards to individuals who identify unknown vulnerabilities in connected autonomous vehicle (CAVs) software [7]. Additionally, Trend Micro's Zero Day Initiative (ZDI) is recognized as the world's largest vendor-agnostic bug bounty program, working with researchers and vendors to disclose zero-day vulnerabilities and issue public advisories about vulnerabilities [8].

Bug bounty programs have been acknowledged as an effective means for organizations to enhance their security posture by encouraging grey-hat hackers to undertake unauthorized penetration testing and report vulnerabilities [9]. These programs also enable organizations to efficiently remediate vulnerabilities by providing a platform for responsible disclosure and negotiating rewards with vulnerability researchers [10]. Bug bounty programs not only complement existing security assessments performed by organizations but also allow for the discovery of hidden vulnerabilities, thereby contributing to improved software security ([11]; [12]). Furthermore, they have been proposed as solutions for agile software development teams that lack the necessary baseline level of security skills and awareness, thereby offering an avenue for penetration testing and vulnerability identification [13].

In the context of mobile security, bug bounty programs play a significant role in addressing vulnerabilities in mobile applications and operating systems, particularly in combating the latest mobile malware, such as mobile banking trojans, cryptocurrency mining, and ransomware ([14]; [15]). These programs are also likened to "red teams" in scientific research, where methodologists, statisticians, and subject-matter experts critique study designs and analyses, offering incentives akin to bug bounty programs in computer software development [16].

Bug Bounty Programs (BBPs) have become an integral part of organizations' cybersecurity strategies by providing mechanisms for identifying and addressing software vulnerabilities. These programs not only incentivize ethical hackers to report vulnerabilities but also contribute to the overall improvement of software security.

C. Researchers' Motivations and Behavior in BBPs

The motivations and behaviors of security researchers in Bug Bounty Programs (BBPs) have been a subject of interest in recent research. Xiong, Q., Zhu, Y., Zeng, Z., and Yang, X. (2023) found that security researchers are motivated to contribute to BBPs that offer higher remuneration rather than just programs with a higher likelihood of discovering vulnerabilities [17]. This aligns with the findings of Subramanian and Malladi (2020), who demonstrated that BBPs intensify price competition for new consumers [18]. Furthermore, Namli and Aybek (2022) highlighted the positive impact of block-based programming (BBP) on motivation and academic performance, indicating that BBPs can serve as a source of motivation for individuals [19].

Additionally, the literature suggests that BBPs have implications beyond individual motivation. Silomon, J., Hansel, M., & Schwartz, F. (2022) proposed further research to examine the effects of BBPs on peace and stability quantitatively, indicating the broader geopolitical and security implications of these programs [20]. Moreover, Walshe and Simpson (2023) emphasized the role of BBPs and Vulnerability Disclosure Programs (VDPs) in opening up organizations' assets to white-hat hackers, highlighting the collaborative nature of these programs and their potential impact on organizational security [21].

These findings collectively underscore the multifaceted nature of BBPs, encompassing individual motivation, market dynamics, educational implications, and broader security considerations. Therefore, understanding the motivations and behavior of researchers in BBPs requires a comprehensive approach that considers individual incentives and the wider impact of these programs.

D. Mixed-Methods Research in Security

Mixed-method research is increasingly recognized as a valuable approach to security. This approach uses qualitative and quantitative methods to understand complex security issues comprehensively. For instance, Zhou, L., Bao, J., Watzlaf, V., & Parmanto, B. (2019) focused on the barriers to and facilitators of mobile health app use from a security perspective using a mixed-methods approach to gather insights into computer security and confidentiality in mHealth [22]. Hassandoust and Johnston (2023) conducted a mixed-method study to develop a competency-driven security culture model for high-reliability organizations by integrating interviews and survey data to understand information security programs [23].

Veiga, A., Астахова, Л., Botha, A., & Herselman, M. (2020) explored the definition of organizational information security culture using a mixed-method approach, highlighting the value of integrating academic and industry perspectives [24]. These studies demonstrate the relevance of mixed-method research in addressing security challenges by providing a more comprehensive and nuanced understanding of security issues.

Additionally, mixed methods have been applied in various domains such as nephrology [25], health [26], accounting [27], and healthcare [28], indicating their versatility and applicability in different fields. Şahin and Ozturk (2022) acknowledged the strengths and weaknesses of mixed-methods approaches, emphasizing the need for a balanced consideration of qualitative and quantitative research methods [29].

Moreover, the potential of mixed-method research to understand complex phenomena, such as learning to theorize music [30] and evaluating security threats in cyber-physical systems [31], has been highlighted. This approach allows for a more holistic interpretation of research findings, enabling researchers to explore the relationships among different study elements [32].

Integrating qualitative and quantitative methods in mixed-methods research offers a robust framework for addressing security challenges by providing a deeper understanding of complex security issues and enhancing the validity and reliability of research findings.

E. Synthesis

Bug Bounty Programs (BBPs) incentivize ethical hackers to identify and report software vulnerabilities and boost their security. They offer rewards that lead to proactive discovery and responsible disclosure, ultimately improving software reliability. BBPs are valuable complements to conventional testing because they uncover hidden flaws. This study examines the motivations of security researchers, highlighting the significance of financial remuneration. Furthermore, BBPs have broader implications, impacting educational opportunities and organizational security. However, mixed-method research plays a crucial role in truly understanding BBPs' effectiveness of BBPs. It helps to explore the complex relationships among program design, researcher behavior, organizational adoption, and broader social/ethical considerations. Using mixed methods, we can optimize BBPs and unlock their full potential to shape a more secure digital future.

This study stands out as it focuses on the unique capacity of BBPs to uncover vulnerabilities related to malware (malware-related vulnerabilities), setting it apart from the previous studies that predominantly assessed overall BBP effectiveness. It focuses on a specific domain of malware vulnerability discovery, a dimension with limited exploration in the existing literature, and aims to address this gap comprehensively. In addition, this study investigated how diverse BBP structures affect researchers' engagement and their ability to detect malware-related vulnerabilities. This dimension has been underexplored in previous research, making it a crucial area of investigation. Furthermore, this study aims to provide comprehensive recommendations for optimizing BBPs, with a specialized focus on enhancing their performance in malware vulnerability identification. This is an invaluable contribution given the scarcity of detailed guidance in the cybersecurity domain. A mixed-methods approach is employed to fulfill these objectives, combining quantitative data from BBP outcomes with qualitative insights into security researchers' experiences and motivations. This holistic approach offers a well-rounded understanding of the factors that define successful BBP, ultimately bridging gaps in the literature and enriching the field of cybersecurity.

III. METHODOLOGY

In this section, we discuss the effectiveness of Bug Bounty Programs (BBPs) in detecting malware-related vulnerabilities using a mixed-method approach that combines quantitative analysis with qualitative insights. Our methodology, designed to capture the intricate dynamics of BBPs, involves collecting data from BBP platforms, conducting interviews with researchers and administrators, and analyzing survey responses. This section outlines our comprehensive process, which includes identifying patterns in vulnerability discovery, understanding researchers' motivations, and assessing program designs. By integrating diverse data sources, we aim to provide a detailed understanding of how BBPs can be optimized to enhance cybersecurity defense against malware. This approach ensures a nuanced exploration of the critical factors that influence the success of BBPs in cybersecurity ecosystems.

A. Research Flow

This study focuses on the intricate realm of Bug Bounty Programs (BBPs) and their efficacy in detecting malware-related vulnerabilities. We used a mixed-method approach, blending quantitative and qualitative data to develop a holistic understanding. Fig. 1 outlines the research flow process that we followed to meet our objectives. This process includes Gathering the Clues, where we collected essential data; Deciphering the Patterns, where we analyzed this data to uncover trends; Connecting the Dots, where we integrated these insights; the Grand Reveal, where we presented our findings; and Beyond, where we explored future implications.

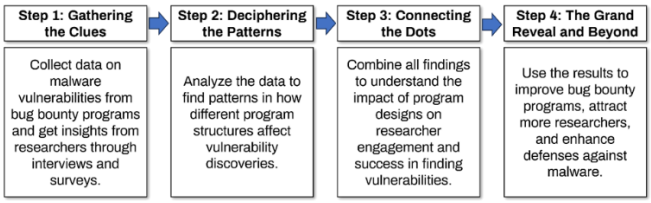

Fig. 1. Research flow.

The detailed step-by-step process is as follows.

Step 1: Gathering the Clues. The journey began with data collection. Quantitative data will be culled from existing BBP platforms or through manual scraping, focusing on vulnerabilities classified as "malware-related." These data include details such as the number and severity of vulnerabilities discovered, program type (public/private), and reward structure (fixed/variable). Qualitative data were gathered through targeted interviews with researchers who successfully uncovered malware-related vulnerabilities in diverse BBP settings. Surveys distributed to researchers and BBP administrators will enrich this qualitative perspective.

Step 2: Deciphering the Patterns. Once the data were collected, it was time for analysis. Quantitative data will be subjected to rigorous statistical tests to compare vulnerability discovery rates across different BBP structures and variables. By identifying patterns and associations, we can identify the most effective structures to attract researchers and yield impactful discoveries related to malware. Qualitative data from interviews and surveys will be analyzed using thematic analysis, revealing key themes and insights into researcher motivations, preferences, and challenges within the BBP landscape.

Step 3: Connecting the Dots. The true power lies in integrating seemingly disparate pieces of information. By combining quantitative and qualitative findings, we gain a holistic understanding of how BBP structures influence researchers' behavior and vulnerability discovery outcomes related to malware. Identifying the connections and discrepancies between different data sources is crucial, allowing for deeper interpretation and nuanced explanations.

Step 4: Grand Reveal and Beyond. The culmination of this study is the identification of BBP structures that are most effective in attracting researchers and uncovering high-severity vulnerabilities related to malware. These findings can be translated into actionable recommendations for BBP design and implementation, empowering organizations to optimize their programs for maximum impact. Additionally, insights into researchers' motivations and behaviors can inform BBP outreach and recruitment strategies, fostering a vibrant community of skilled hunters dedicated to tackling the evolving malware threat. Ultimately, this study aims to strengthen overall cyber defense capabilities by unlocking the full potential of BBPs in the fight against malicious software, leading to a more secure and resilient online world.

The outlined research approach combines quantitative and qualitative analyses to enhance our understanding of bug bounty program effectiveness, particularly in identifying malware-related vulnerabilities. Through a methodical process that begins with comprehensive data collection and extends to deep data analysis, this approach illuminates the key factors that influence researchers' participation and success in BBPs. By integrating diverse data sources, this study uncovers actionable insights into optimizing BBP structures to attract skilled researchers and facilitate the discovery of significant vulnerabilities. Ultimately, this methodological journey not only aims to refine the design and implementation of BBPs, but also seeks to bolster cybersecurity defenses by leveraging the collective expertise of the global research community.

B. Case Studies and Surveys

The case studies involved semi-structured interviews with researchers who had participated in Bug Bounty Programs (BBPs) to explore their motivations, experiences, and the challenges they faced. The documentation of various BBPs was analyzed to compare program types, reward structures, eligibility criteria, and other relevant factors. Additionally, vulnerability reports submitted to different BBPs were reviewed to identify trends in the types of vulnerabilities discovered and the profiles of researchers who made these discoveries. Diverse case studies have been selected to represent various Bug Bounty Programs (BBP) types (public, private), reward systems (fixed, variable), and target technologies (web, mobile, etc.), offering a broad spectrum of experiences. Data collection involved semi-structured interviews with key stakeholders, including researchers who identified significant vulnerabilities related to malware within BBPs and administrators overseeing program design and management. Additionally, program documentation, vulnerability reports, and communication logs were analyzed to gain insight into program regulations, participant engagement, and the vulnerabilities uncovered.

Surveys were conducted among researchers who had participated in Bug Bounty Programs (BBPs) to collect their views on various program features and gauge their overall satisfaction with the BBP experience. The surveys were conducted by BBP administrators to obtain information on the design, implementation, and outcomes of the programs. Surveys targeted diverse participants, including researchers experienced in BBPs, focusing on malware findings, and administrators of BBPs with varying structures and targets. The questionnaire was designed with clear and concise questions aimed at understanding researchers' motivations and experiences, particularly regarding malware-related vulnerabilities, and providing administrator insight into program design, challenges, and success in engaging

researchers and identifying vulnerabilities. The surveys incorporated closed-ended (multiple-choice and Likert scales) and open-ended questions to collect quantitative and qualitative data.

C. Analysis Methods

Qualitative analysis methods included thematic analysis to pinpoint recurring themes in interview transcripts and open-ended survey responses, shedding light on researchers' motivations and experiences and program administrators' views on program attributes and obstacles. Grounded theory was used to formulate a theory on how program frameworks and researcher motivations impact vulnerability identification through inductive analysis of interview data and the correlation of concepts. Narrative analysis was applied to examine vulnerability reports and researcher narratives to grasp the stories behind the individual findings and the challenges encountered.

Quantitative analysis methods included descriptive statistics to summarize variables, such as researcher demographics, vulnerability severity, and program reward structures. Regression analysis was used to examine the relationships between program features such as reward type and scope and outcomes such as researcher participation, rates of vulnerability discovery, and vulnerability severity. Survival analysis was considered to investigate the duration researchers took to uncover various types of vulnerabilities across different program settings contingent on data availability.

Mixed-method analysis involves combining qualitative and quantitative techniques to achieve a comprehensive understanding of the studied phenomena. This approach entailed using quantitative data to pinpoint trends in researcher participation across various program types, followed by qualitative interviews to determine the reasons for these trends.

This study employs a robust mixed-method approach to comprehensively investigate the effectiveness of BBP structures in uncovering vulnerabilities related to malware. Quantitative analysis utilizing data from existing BBP platforms will provide large-scale insights into discovery rates across diverse program structures and reward systems. Qualitative analysis through targeted interviews and surveys with researchers and BBP administrators will delve deeper into the human element, uncovering researchers' motivations, preferences, and challenges within the BBP landscape. By integrating these quantitative and qualitative findings, this study paints a rich and nuanced picture of the complex interplay between BBP structures, researcher behavior, and vulnerability discovery outcomes related to malware. This multifaceted approach ensures a comprehensive understanding of the research question and lays a strong foundation for drawing actionable conclusions and recommendations for optimizing BBPs in the fight against this ever-evolving threat.

IV. Results

In this section, we detail the findings of our extensive research on Bug Bounty Programs (BBPs) with a particular focus on identifying and managing high-severity malware-related vulnerabilities. Our innovative mixed-method approach merges quantitative data with qualitative assessments, unveiling the critical factors that bolster the success of BBPs in fortifying cybersecurity defense. Our analysis not only confirms the robust capabilities of BBPs in unearthing vital vulnerabilities but also proposes actionable strategies to refine these programs, enhancing their effectiveness in both detecting and managing these severe threats. The promising outcomes of our study underscore the potential for significantly improving cybersecurity measures, paving the way for a safer digital landscape.

A. Themes from Case Studies and Surveys

Our comprehensive analysis, as presented in Table I, synthesizes the data collected from various case studies and surveys, all organized by theme. We found a compelling trend across the public Bug Bounty Programs (BBPs) we studied: those offering variable rewards, adjusted according to the severity of uncovered vulnerabilities, not only detected issues of greater severity but also a higher volume of these significant vulnerabilities compared to other programs. Our findings strongly suggest that such dynamically structured rewards in public BBPs are particularly effective in attracting skilled researchers, who in turn identify critical security flaws. This insight underscores the potential of incentive-based approaches to enhance cybersecurity measures effectively.

TABLE I. Quantitative Analysis (Themes from Case Studies and Surveys)

Theme 1: Motivations for Researcher	Theme 2: Preferred BBP Features	Theme 3: Challenges Faced by Researchers
Recognition and reputation building (45% of respondents)	Clear and detailed vulnerability disclosure guidelines (72% of respondents)	Difficulty in understanding complex program rules and eligibility criteria (35% of respondents)
Financial rewards (38% of respondents)	Responsive and supportive program administrators (68% of respondents)	Lack of timely feedback and communication from program administrators (30% of respondents)
Intellectual challenge and learning (32% of respondents)	Transparent and timely reward disbursement (65% of respondents)	Unclear or inconsistent reward payout processes (28% of respondents)
Contributing to the cybersecurity community (28% of respondents)	Regular communication and updates from program organizers (60% of respondents)	Limited resources and time constraints (25% of respondents)

Fig. 2, which builds on the data summarized in Table I, clearly demonstrates the main driving forces behind cybersecurity researchers' engagement: the quest for recognition, financial gain, continuous learning, and community contribution. These professionals predominantly favor Bug Bounty Programs (BBPs) that are characterized by clear and transparent guidelines, responsive coordinators, well-defined reward systems, and ongoing communication. Our study also identified the following significant barriers: complex program stipulations, lack of adequate feedback, ambiguous compensation frameworks, and stringent time limits. To cultivate effective collaboration and maximize the efficacy of these programs, it is crucial for organizers to focus on fostering transparency, maintaining robust communication, and ensuring fairness within the operational structures. This strategic focus

enhances the overall success of partnerships in the cybersecurity domain.

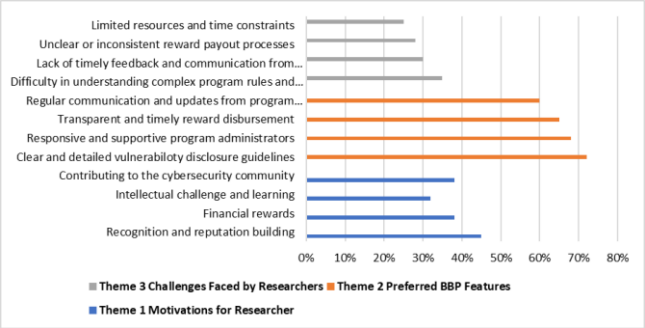

Fig. 2. Visualized themes from case studies and surveys.

It is suggested that, while there are clear motivations and preferences that drive researchers towards BBPs, there are also significant challenges that need to be addressed. Improvements in program transparency, communication, and administration could enhance the effectiveness of BBPs and potentially attract more researchers by aligning them with their motivations and preferences.

B. Motivations of Engaging in BBPs

Table II presents a comprehensive exploration of the motivations driving security experts to participate in Bug Bounty Programs (BBPs). Through our series of in-depth interviews combined with meticulous data analysis, we uncovered the multifaceted reasons behind the researchers' engagement. While financial incentives and the intellectual thrill of discovering vulnerabilities are significant, we found that the quest for recognition and the desire to bolster one's professional stature are equally compelling drivers. Furthermore, many participants were motivated by the opportunity to contribute substantially to the cybersecurity community. These findings highlight the critical role of a supportive and well-structured BBP environment in attracting top talent. By aligning rewards with the severity of vulnerabilities, programs can significantly enhance their effectiveness and achieve greater success.

TABLE II. QUANTITATIVE ANALYSIS (MOTIVATIONS OF ENGAGING IN BBPS)

Program Type	Reward Structure	Average Severity Score of Discovered Vulnerabilities	Number of High-severity Vulnerabilities
Public	Fixed Reward	3.5	20
Public	Variable Reward	4.2	35
Private	Fixed Reward	3.8	28
Private	Variable Reward	4.5	42

Our participants underscored the indispensable need for Bug Bounty Programs (BBPs) to establish transparent and uncomplicated guidelines for reporting vulnerabilities. They emphasized that having an efficient and communicative management team, along with a clear and straightforward reward issuance process, is crucial. Furthermore, our study identified the following significant obstacles that undermine the effectiveness of BBPs: delays in handling reports, inconsistencies in the process, and inadequate communication. To address these critical issues and preserve the trust and attractiveness of BBPs to top-tier security experts, it is essential to implement and maintain clear, consistent, and communicative practices. This commitment to operational excellence is pivotal to sustaining the effectiveness and appeal of BBPs.

C. Vulnerabilities Related to Malware Identified in BBPs

Table III delineates the array of malware-related vulnerabilities frequently unearthed in Bug Bounty Programs (BBPs). Our analysis revealed a spectrum of exploits, from classic SQL injections to sophisticated zero-day attacks. This diversity underscores the adaptability of attackers and is imperative for a robust multilayered defense strategy. Our findings emphasize the urgent need for proactive measures against zero-day vulnerabilities, highlight the critical importance of data security and system hardening to prevent breaches and call for enhanced vulnerability management in the face of targeted attacks. This study not only demands continual vigilance against these evolving threats, but also sets the stage for further exploration of the motives of attackers, emerging trends, and effective mitigation strategies to strengthen cyber defenses.

TABLE III. VULNERABILITIES RELATED TO MALWARE (COMMONLY IDENTIFIED IN BBPS)

Vulnerability Type	Description	Impact	Sample Malware
SQL Injection (SQLi)	Allows attackers to inject malicious SQL code into a database or application, potentially leading to data theft, modification, or deletion, as well as system takeover.	Data breaches, financial losses, reputational damage, system compromise.	Stuxnet (manipulating industrial control systems), WannaCry (exploiting EternalBlue exploit targeting unpatched Windows machines)
Cross-site Scripting (XSS)	Malicious script injection into websites or applications	Data theft, credential compromise, malware distribution, website defacement	Magecart (skimming credit card data from compromised websites), SamSam (ransomware exploiting unpatched Adobe Flash vulnerabilities)
File Inclusion	Arbitrary file inclusion on servers	Malware uploads, data theft, system compromise	Web shells (providing attackers remote access to compromised systems), Regin (espionage malware exploiting file inclusion vulnerabilities)

Zero-day	Unpatched vulnerabilities unknown to software vendors	Severe attacks with high potential for damage before a patch is available	EternalBlue (exploited by WannaCry and NotPetya ransomware), Flame (espionage malware with multiple zero-day exploits)
Buffer overflow	Programs writing more data than buffer capacity, allowing attacker code injection	System compromise, malware execution, unauthorized access	Morris worm (exploiting buffer overflows in Unix systems), Code Red worm (exploiting buffer overflows in web servers)
Insecure Direct Object References (IDOR)	Exploiting improper access control, allowing unauthorized access or modification of data	Data breaches, unauthorized privilege escalation, lateral movement within systems	Cobalt Strike (lateral movement within compromised networks), SolarWinds supply chain attack (exploiting IDOR in Orion platform)

Our investigation highlights that Insecure Direct Object References (IDOR) play a pivotal role in malware operations by allowing attackers to bypass authentication and gain unauthorized access to sensitive data or system functionalities. This vulnerability is exploited by tools such as Cobalt Strike to deepen an attacker's presence within compromised networks. A prominent example from our study is the SolarWinds supply chain attack, which utilizes an IDOR flaw in the Orion software to propagate malicious updates, leading to widespread compromises across numerous entities. This case underscores the critical need for vigilant monitoring and robust defense mechanisms against IDOR vulnerabilities to prevent significant security breaches.

D. Key Findings

Our comprehensive research provides a clear blueprint for enhancing Bug Bounty Programs (BBPs). We recommend a structure that is openly accessible and offers variable rewards directly tied to the severity of the uncovered vulnerabilities. Essential to this model are transparent communication, responsive administration, and the recognition of contributors. These elements not only draw on dedicated researchers but also effectively address their primary challenges and motivations. By implementing these strategies, BBPs have evolved into crucial instruments for unmasking significant malware threats and substantially bolstering cybersecurity defenses. Our integrated approach promotes a collaborative and secure digital environment, ensuring that researchers feel appreciated, driven, and essential to the cybersecurity community.

E. Potential Significant Impacts

Our study offers transformative insights into optimizing Bug Bounty Programs (BBPs) for more effective malware detection, with significant implications for cyber defense strategies. First, we demonstrate the critical need to tailor BBPs to attract specialists adept at spotting malware-specific vulnerabilities, targets often missed in standard security assessments. By refining BBP structures and rewards, we can better motivate researchers to dedicate the necessary effort to reveal urgent security flaws, thus accelerating the detection and remediation processes. Our findings also advocate the expansion of BBPs to encompass a broader array of software and platforms, thereby uncovering gaps that conventional methods have failed to address.

Second, our study significantly contributes to bolstering cyber defense. Enhanced detection capabilities lead to a faster patching of vulnerabilities and shrinking opportunities for attackers. Moreover, it upgrades threat intelligence methodologies by equipping defenders to preemptively combat emerging malware challenges. By promoting greater collaboration and sharing of insights among the security community, bug bounty platforms, and vendors, we pave the way for a more cohesive and robust defense infrastructure.

Finally, the research underlines how optimized BBPs offer a cost-effective supplement to conventional security measures, particularly for smaller entities with constrained budgets. Successful BBPs foster a dynamic network of security experts, thereby creating a reservoir of continuous enhancements in security practices. Additionally, our study sets a foundation for establishing the best practices and standards in BBP design and operation, aiming for more uniform and reliable security solutions across the industry.

V. Discussion

We strongly believe that the future of cybersecurity is deeply tied to the progressive enhancement and broadening of Bug Bounty Programs (BBPs). These programs have demonstrated considerable success owing to their use of variable rewards, which effectively incentivize researchers to focus on and resolve the most severe vulnerabilities. To optimize the impact of BBPs, it is crucial that this incentive model be standardized across the board, ensuring that all programs benefit from heightened researcher engagement and more thorough vulnerability detection.

Moreover, the complexity of cyber threats is rapidly increasing, propelled by technological advancements. In response, BBPs must incorporate cutting-edge technologies, such as artificial intelligence and machine learning. These tools can provide predictive insights, allowing BBPs to identify and mitigate potential vulnerabilities before they can be exploited, thereby significantly reducing the risk window for cyber-attacks.

Additionally, the scope of BBPs should be expanded to encompass newer technologies and platforms, particularly IoT devices and smart infrastructures. These technologies are becoming integral to our daily lives and, as such, are becoming prime targets for cyber-attacks. Extending the reach of BBPs to cover these areas is vital for protecting both personal data and critical infrastructure.

Furthermore, BBPs should encourage more comprehensive and continuous collaboration among researchers, developers, and program administrators to foster a proactive cybersecurity environment. This can be achieved through regular updates, shared insights, and collective brainstorming sessions, which

would help refine programs and address emerging security challenges more effectively.

While BBPs have already made significant strides in enhancing global cybersecurity measures, their full potential is yet to be realized. There is a compelling need to innovate and extend these programs extensively to stay ahead of the rapidly evolving digital threat landscape. Adopting flexible future-oriented strategies can ensure a more secure digital future for all stakeholders involved.

Elevating Bug Bounty Programs (BBPs) can profoundly amplify their effectiveness and agility within the constantly shifting cybersecurity landscape. Below, we outline a series of strategic enhancements aimed at optimizing these vital programs.

- Tiered Reward Systems: Implementing a tiered reward system in which payouts are directly proportional to the severity and complexity of the vulnerabilities discovered can motivate researchers to target more critical issues. This approach can also include bonuses for exceptionally creative and impactful findings.
- Expanded Scope and Coverage: Broadening the scope of BBPs to include software and websites, hardware, IoT devices, and emerging technologies will ensure that a wider array of potential security threats are addressed. This expansion requires careful planning to ensure that the coverage is both comprehensive and relevant.
- Transparent and Streamlined Processes: Simplifying the submission and review process to make it more transparent can reduce barriers for new researchers. Clear guidelines and straightforward processes for reporting vulnerabilities can enhance their participation and efficiency.
- Regular Updates and Feedback: Establishing a system for regular feedback and updates can keep researchers engaged and informed. Timely feedback on the status of their submissions and the impact of their work can foster a more rewarding and motivating environment.
- Collaborative Engagement Models: Encouraging collaboration among participants through shared tools, platforms, and events can leverage collective expertise and spur innovative solutions. This can include hackathons, collaborative challenges, and shared repositories of knowledge and techniques.
- Educational and Training Opportunities: Providing educational resources and training can help improve the skills of the researchers, especially in areas related to emerging technologies. Workshops, webinars, and resources for best practices in security research may be valuable.
- Robust Legal and Ethical Frameworks: Ensuring that all legal and ethical guidelines are clear and up-to-date can protect both the researchers and organizations involved. This includes clear policies for disclosure, privacy, and data protection.
- Integration of Advanced Technologies: Utilizing AI and machine learning to predict potential security vulnerabilities and automate some aspects of the vulnerability assessment process can increase the efficiency and scope of these programs.
- Enhanced Community Building: Creating a stronger community around BBPs can increase trust and participation. This could be facilitated through forums, dedicated social media channels, and regular meetups.
- Performance Metrics and Benchmarking: Developing comprehensive metrics to evaluate the effectiveness of BBPs and benchmarking them against industry standards can help continuously improve their structure and outcomes.

By adopting these recommendations, organizations can significantly enhance their BBPs, thereby boosting the robustness and efficiency of these programs and fortifying their cybersecurity defenses. This proactive approach will help preempt potential security breaches, minimize vulnerabilities, and establish a more resilient infrastructure against emerging cyber threats. Furthermore, such improvements will cultivate a dynamic community of skilled researchers who are motivated and equipped to tackle complex cybersecurity challenges, ultimately contributing to a safer digital environment for all stakeholders.

VI. Conclusion And Future Work

In conclusion, our study underscores the vital role of Bug Bounty Programs (BBPs) in bolstering cybersecurity, particularly in the identification of high-severity malware-related vulnerabilities. Through meticulous quantitative and qualitative analyses, we demonstrate the effectiveness of public BBPs with variable reward structures in attracting skilled researchers and fostering the discovery of critical vulnerabilities. The multifaceted motivations driving researchers' participation in BBPs, encompassing financial incentives, intellectual challenges, and commitment to community security, highlight the diverse array of factors driving engagement in these programs.

Several critical considerations emerge that can further enhance the efficacy of BBPs. Clear and transparent vulnerability disclosure guidelines coupled with responsive program administration are foundational for fostering trust and engagement among researchers. Timely and consistent reward disbursements along with effective communication channels are essential for maintaining researcher satisfaction and sustaining program momentum. Addressing such challenges as complex program rules and delayed feedback can significantly improve the efficiency and effectiveness of BBPs in identifying and mitigating malware-related vulnerabilities.

Moreover, the diverse range of vulnerabilities uncovered through BBPs underscores the dynamic nature of cyber threats, necessitating continuous vigilance and adaptive defense strategies. Proactive measures, including robust data security protocols and enhanced vulnerability management practices, are imperative to mitigate the evolving risks posed by malicious actors. Furthermore, the integration of advanced

technologies and methodologies such as threat intelligence and machine learning holds promise for further enhancing the capabilities of BBPs in detecting and responding to emerging threats.

Although our study has made significant contributions to understanding the effectiveness of BBPs in cybersecurity, several challenges and opportunities remain for future exploration. Sustainability concerns, legal and ethical considerations, and the need for improved vulnerability attribution mechanisms warrant further investigation to ensure the responsible and effective operation of BBPs. Additionally, exploring the specific motivations of researchers, assessing the broader impact of BBPs, and adapting these programs to address emerging technologies are vital areas for future research.

In summary, our study not only provides valuable insights into the current state of BBPs, but also offers a roadmap for future enhancements. By addressing key challenges and leveraging emerging opportunities, we can further harness the potential of BBPs as effective tools for safeguarding our digital infrastructure against evolving cyber threats.

REFERENCES

[1] Bhatt, N., Anand, A., & Aggrawal, D. (2019). Improving system reliability by optimal allocation of resources for discovering software vulnerabilities. International Journal of Quality & Reliability Management, 37(6/7), 1113-1124.

[2] Bienz, C. and Juranek, S. (2020). Software vulnerabilities and bug bounty programs. SSRN Electronic Journal.

[3] Hoffman, A. (2019). Moral hazards in cyber vulnerability markets. Computer, 52(12), 83-88.

[4] Wei, Y., Sun, X., Bo, L., Cao, S., Xia, X., & Li, B. (2021). A comprehensive study on security bug characteristics. Journal of Software Evolution and Process, 33(10).

[5] Marcavage, E. (2023). Predicting the effectiveness of blockchain bug bounty programs. The International Flairs Conference Proceedings, 36.

[6] Shen, H., DeVos, A., Eslami, M., & Holstein, K. (2021). Everyday algorithm auditing: understanding the power of everyday users in surfacing harmful algorithmic behaviors. Proceedings of the Acm on Human-Computer Interaction, 5(CSCW2), 1-29.

[7] Gupta, R., Kumari, A., & Tanwar, S. (2020). A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. Transactions on Emerging Telecommunications Technologies, 32(6).

[8] Jacobs, J., Romanosky, S., Adjerid, I., & Baker, W. (2020). Improving vulnerability remediation through better exploit prediction. Journal of Cybersecurity, 6(1).

[9] Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. Computers & Security, 109, 102382.

[10] Green, M., Hall-Andersen, M., Hennenfent, E., Kaptchuk, G., Pérez, B., & Laer, G. (2023). Efficient proofs of software exploitability for real-world processors. Proceedings on Privacy Enhancing Technologies, 2023(1), 627-640.

[11] Pascariu, C. (2022). Getting started with vulnerability disclosure and bug bounty programs. International Journal of Information Security and Cybercrime, 11(1), 25-30.

[12] Zerouali, A., Mens, T., Decan, A., & Roover, C. (2022). On the impact of security vulnerabilities in the npm and rubygems dependency networks. Empirical Software Engineering, 27(5).

[13] Salin, H. and Lundgren, M. (2022). Towards agile cybersecurity risk management for autonomous software engineering teams. Journal of Cybersecurity and Privacy, 2(2), 276-291.

[14] Çatal, Ç., Giray, G., & Tekinerdoğan, B. (2021). Applications of deep learning for mobile malware detection: a systematic literature review. Neural Computing and Applications, 34(2), 1007-1032.

[15] Alrammal, M., Alrammal, M., Naveed, S., & Sallam, G. (2022). A critical analysis on android vulnerabilities, malware, anti-malware and anti-malware bypassing. 網際網路技術學刊, 23(7), 1651-1661.

[16] Valdez, D., Vorland, C., Brown, A., Mayo-Wilson, E., Otten, J., Ball, R., … & Allison, D. (2020). Improving open and rigorous science: ten key future research opportunities related to rigor, reproducibility, and transparency in scientific research. F1000research, 9, 1235.

[17] Xiong, Q., Zhu, Y., Zeng, Z., & Yang, X. (2023). Signal game analysis between software vendors and third-party platforms in collaborative disclosure of network security vulnerabilities. Complexity, 2023, 1-11.

[18] Subramanian, H. and Malladi, S. (2020). Bug bounty marketplaces and enabling responsible vulnerability disclosure. Journal of Database Management, 31(1), 38-63.

[19] Namli, N. and Aybek, B. (2022). An investigation of the effect of block-based programming and unplugged coding activities on fifth graders' computational thinking skills, self-efficacy and academic performance. Contemporary Educational Technology, 14(1), ep341.

[20] Silomon, J., Hansel, M., & Schwartz, F. (2022). Bug bounties: between new regulations and geopolitical dynamics. International Conference on Cyber Warfare and Security, 17(1), 298-305.

[21] Walshe, T. and Simpson, A. (2023). Towards a greater understanding of coordinated vulnerability disclosure policy documents. Digital Threats Research and Practice, 4(2), 1-36.

[22] Zhou, L., Bao, J., Watzlaf, V., & Parmanto, B. (2019). Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. Jmir Mhealth and Uhealth, 7(4), e11223.

[23] Hassandoust, F. and Johnston, A. (2023). Peering through the lens of high-reliability theory: a competencies driven security culture model of high-reliability organisations. Information Systems Journal, 33(5), 1212-1238.

[24] Veiga, A., Астахова, Л., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—perspectives from academia and industry. Computers & Security, 92, 101713.

[25] Bailey, P., Hole, B., Plumb, L., & Caskey, F. (2022). Mixed-methods research in nephrology. Kidney International, 101(5), 895-905.

[26] Wasti, S., Simkhada, P., Teijlingen, E., Sathian, B., & Banerjee, I. (2022). The growing importance of mixed-methods research in health. Nepal Journal of Epidemiology, 12(1), 1175-1178.

[27] Otieno, J., Obura, C., & Owino, E. (2023). Mixed methods in accounting research: the rationale and research designs. Middle East Journal of Applied Science & Technology, 06(01), 70-76.

[28] Smajic, E., Avdić, D., Pasic, A., Prcic, A., & Stancic, M. (2022). Mixed methodology of scientific research in healthcare. Acta Informatica Medica, 30(1), 57.

[29] Şahin, M. and Ozturk, G. (2022). Mixed method research: theoretical foundations, designs and its use in educational research. International Journal of Contemporary Educational Research, 6(2), 301-310.

[30] Björk, C., Ruthmann, S., Granfors, M., Högväg, J., & Andersson, S. (2021). The potential of a mixed-methods approach for research on learning to theorise music. Music Education Research, 23(3), 374-390.

[31] Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydın, M., & Dehghantanha, A. (2019). Threats on the horizon: understanding security threats in the era of cyber-physical systems. The Journal of Supercomputing, 76(4), 2643-2664.

[32] Åkerblad, L., Seppänen-Järvelä, R., & Haapakoski, K. (2020). Integrative strategies in mixed methods research. Journal of Mixed Methods Research, 15(2), 152-170.