2024 11th International Conference on Future Internet of Things and Cloud (FiCloud) | 979-8-3315-2719-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/FiCloud62933.2024.00013

The Practical Requirements of a Malware Training Platform Tailored to Industry and Education

1st Alexander Cameron
School of Computing & Engineering
University of Gloucestershire
Cheltenham, United Kingdom
ORCID 0000-0002-3091-6509

2nd Dr Abu Alam
School of Computing & Engineering
University of Gloucestershire
Cheltenham, United Kingdom
ORCID 0000-0002-5958-7905

3rd Dr Qublai Ali Mirza
School of Computing & Engineering
University of Gloucestershire
Cheltenham, United Kingdom
ORCID 0000-0003-3403-2935

***Abstract*—Malware attacks continue to damage organisations and individuals. Whilst existing training such as phishing training is useful to users, it's applicability to malware attacks is limited. Whilst cyber ranges and cyber training platforms utilising simulation have emerged to provide more realistic cyber training, the use of such technologies is limited within the field of malware. Therefore, researchers have surveyed individuals working within and outside of the cyber security sector to identify the demand for such a solution and what key requirements of such a solution would be. The results indicate 80 percent of respondents would be interested in using a malware training platform capable of simulating malware attacks to enhance their awareness, with only 12 percent of respondents believing that current forms of malware training are adequate. Furthermore, respondents indicated a clear preference for an ability to record the interactions with malware, as well as the ability to design and share training packages. Regarding non functional requirements, respondents identified the ability to utilise such a solution through a web browser as the most in demand requirement, with the ability to self-host the solution and to understand which malware types a user is most at risk by being highly ranked.**

***Index Terms*—cyber security, malware, malware analysis, cyber training**

I. Introduction

Malicious software is increasingly commonplace, often used by cyber criminals to commit crimes and subvert the legitimate control of computer systems [1]. Whilst various forms of technical solution exist to mitigate against malware, users themselves often contribute to an infection which may have been avoidable if users had a greater level of malware awareness [2]. Training exists to partially mitigate against commonplace attacks such as phishing, with users taught basic cyber hygiene with the intention of changing a users behaviours to be more secure and by extension, the security of an organisation [3].

However, within the context of malware awareness and training, limited training exists that directly provides awareness and education of malware to users [4]. For individuals working or learning within the cyber security sector, being able to identify key signs of a malware attack and understand commonplace behaviours of malware is essential in order to detect and ultimately prevent future attacks [5]. The researchers have surveyed respondents operating within the cyber security industry to understand if a dedicated malware training tool would assist them, as well as what capabilities and features such a tool would need to achieve in order to be useful to them.

II. Literature Review

As the world we live in becomes more interconnected and leverages increasing use of computer systems and networks, the potential for cyber attacks increase significantly. Cyber attacks offer a unique method of attack compared to traditional kinetic weaponry, characterized by a greater level of anonimity afforded to an attacker, as well as the difficulty in detecting such an attack [6], [7]. Since the inception of computer systems, cyber criminals have sought to develop methods to increase their rate of successful compromises, leading to the formation of malware [8]. Malware, a portmaneu of "malicious" and "software", is a primary example of such developments. Malware enables cyber criminals to house malicious code within executable programs that can be disseminated to victims directly or indirectly [9]. Once activated, malware can begin execution in the same manner as any legitimate program, performing the relevant tasks the program was designed for, potentially including data theft, destruction of data and many more malicious actions [10].

To mitigate against malware, several forms of malware training have emerged. Conventional malware training can be observed in items such as phishing training, in which individuals are informed of potential warning signs associated with an attacker and the need to avoid opening unknown programs [11], [12]. Whilst this has proved useful and beneficial when compared to no training at all, such training mechanisms lack engagement from users and are often limited within the context of malware, thereby limiting the realism offered to users [13], [14].

To address the shortcomings of such conventional training, organisations and initiatives have emerged to support simulated training, such as Immersive Labs and other cyber range providers [15], [16]. Such solutions offer individuals the ability to experience highly realistic cyber security training through the provisioning of dedicated virtual environments, however offer a highly limited set of malware related training as their primary focus is wider cyber security [17], [18].

979-8-3315-2719-8/24/$31.00 ©2024 IEEE
DOI 10.1109/FiCloud62933.2024.00013

Due to these reasons, whilst cyber security training has seen advancements using simulated training, the same advancements have not been readily incorporated into malware training [19]. Potential reasons attributed to the lack of simulation in malware training include the potential risk posed to users, a presumed lack of demand from organisations for such training due to a lack of awareness of it's importance and therefore a lack of demand for organisations to implement such a tool [20]–[22].

Therefore, a research gap exists in this area where the feasibility of such a tool, as well as it's advantages and disadvantages are largely unknown by the wider research community. The researchers seek to provide clarity in this area through detailed survey data, defining the potential requirements of a prototype malware training platform and respondents views upon this tool.

III. Research Methodology

The undertaken research methodology involves a survey containing 35 questions of qualitative and quantitative response types, which will be used to capture data for statistical analysis of responses and discussion regarding quantitative responses. The survey was conducted within England, United Kingdom and surveyed 51 respondents studying or working within the cyber security industry, or with some form of IT experience. Respondents were selected through a combination of convenient sampling and snowball sampling to address the difficulties associated with finding a suitable pool of respondents. A flowchart of the methodology can be seen within figure 1.

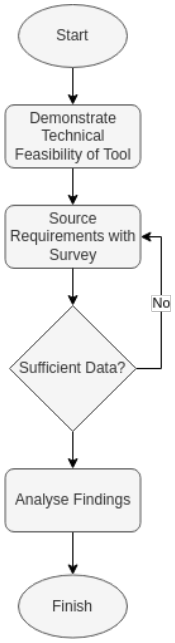

Fig. 1. A flowchart illustrating the methodology utilised.

The research strategy of utilising surveys was chosen to collect a range of requirements from users for a malware training platform from a wide variety of individuals. Whilst other research strategies such as interviews could enable a greater level of depth for specific requirements, the aim of the research was not to focus in depth on any specific requirement and instead to understand the overarching needs and demands of users for such a tool. Following development of such a solution, interviews may be advisable to focus on specific requirements and gain greater insight.

Experience Level	Count
No experience	12
Under 6 months	6
1-2 years	12
3-4 years	4
5-6 years	6
7-8 years	5
Over 10 years	6

TABLE I
Respondent experiences within cyber security.

Employment Type	Count
I am a student studying cyber	9
I am a student, not studying cyber	1
I work within the public sector	11
I work within the private sector at an organisation with more than 50 people (including Universities)	22
I work within the private sector at an organisation with 11-50 people	5
I work within the private sector at an organisation with less than 10 people	3

TABLE II
Respondent employment types.

IV. Respondent Demographics

Demographic information regarding respondents has been included in tables I, II and III. Demographic data contained within the aforementioned tables indicates that the sample is mostly composed of individuals with moderate levels of experience within cyber security, with the largest employment type being large private sector organisations, followed by public sector employees and students studying cyber security. The largest self reported sectors of employment are 25% within education and 15% within IT, with the remaining percentages relatively evenly distributed between a variety of different sectors.

A majority of 71% of individuals self described themselves to be technical, however due to the potential for bias and over representation of technicality, the researchers determined that respondents technicality should be evaluated based upon their supplied job role and a requirement of over 2 years experience within cyber to ensure data quality. This substantially altered the number of respondents meeting the assessment criteria to be assessed as technical, resulting in 31% of individuals being classified as technical and 69% classed as non technical.

Employment Sector	Count
Education	13
IT	8
Retail	5
Undisclosed	4
Consultancy	3
Cyber	3
Health	3
Government	3
Manufacturing	2
Arts	1
Charity	1
Construction	1
Defence	1
Financial Services	1
Legal	1
Transport	1

TABLE III
SELF-REPORTED SECTORS OF EMPLOYMENT FOR RESPONDENTS

V. RESULTS & ANALYSIS

From the 51 individuals surveyed, 80% stated they would be interested in using a malware training platform capable of simulating malware attacks to enhance their awareness. Fifteen percent of the remaining respondents answered maybe, with only 4% of respondents stating they would not be interested in using such a tool.

Regarding the usage of cyber and malware training platforms, 49% of respondents affirmed their use of some form of cyber training platform or tool, however only 20% of respondents affirmed usage of malware training platforms or tools, as indicated in figure 2. This potentially indicates that whilst cyber security training is more widely recognised, malware training is relatively unknown to a majority of respondents.

This argument can be strengthened further through figure 3, in which only 12% of respondents believe malware training is adequate. Analysing responses further indicates that 55% of respondents answered they were unsure, whilst 33% answered no. Therefore, it appears that whilst malware training tools are uncommon, figure 4 illustrates that respondents overwhelmingly affirm an interest in a tool capable of simulating malware attacks to support training.

A. High Demand Training Areas

Respondents were asked to identify the areas of malware training they wished to undertake training in the most, with results visible in table IV. Results indicate that general malware awareness, responding to malware attacks and malware based user training were the most in demand areas. It is notable that general malware awareness ranked highest, with this potentially aligning with the possibility that individuals currently have a low level of awareness of malware attacks and that bespoke training for such areas is relatively unknown.

The results within table IV appear to indicate that malware training platforms and supporting tools should incorporate a

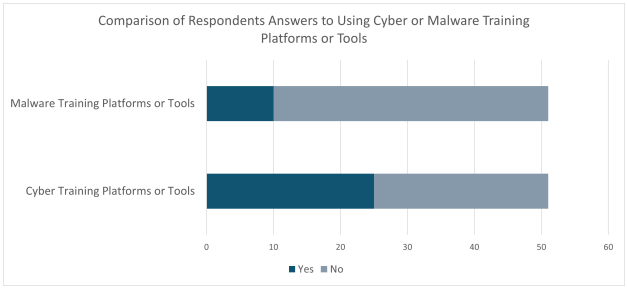

Fig. 2. Comparison indicating that only 20% of respondents utilise malware training platforms or tools.

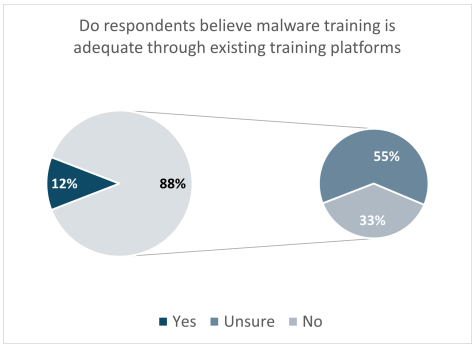

Fig. 3. Results indicating only 12% of respondents believe malware training is adequate through existing training platforms.

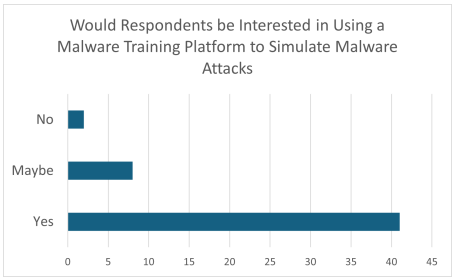

Fig. 4. Results indicating a majority of respondents would be interested in utilising a form of malware training platform to enhance their malware awareness.

Demand Ordering	Training Area
General Malware Awareness	24
Responding to Malware Attacks	19
Malware based User Training	18
All of the above	17
How to recover from a Malware Attack	14
Reverse engineering Malware	12
How to harvest indicators of compromise	4
None	3
Other	1

TABLE IV
RESULTS INDICATING HIGH DEMAND MALWARE TRAINING AREAS.

wide range of malware training possibilities. Less technical malware training items such as general malware awareness should be combined with more technical options such as responding and recovering from malware attacks to ensure such a tool can remain effective to individuals with an existing background within cyber security and malware, as well as individuals beginning to enter these sectors.

B. Functional Requirements Analysis

Respondents were asked to rank various functional requirements relating to a potential malware training platform, with results visible in figure 5. From such results, it is apparent that the most in demand feature would be the ability to screen record interactions with malware. Such a feature would enable retrospective analysis of a users interaction with malware, which could be used to identify mistakes in analysis, as well as validating a user has completed the training successfully. Overall, respondents did not clearly identify a low priority functional requirement.

The abilities to store history and progress, utilise role based access control and the ability to share training packages with other individuals were all ranked second highest. Account based features such as role based access control and user history are commonplace within applications and are crucial to ensure isolation of privileges. Notably whilst role based access control did receive a number of votes as the second highest functional requirement, it also held the largest number of votes as the lowest functional requirement. The researchers suggest that this may be because items such as role based access control may be an implicit expectation by respondents within such a tool, rather than being seen as a functional requirement.

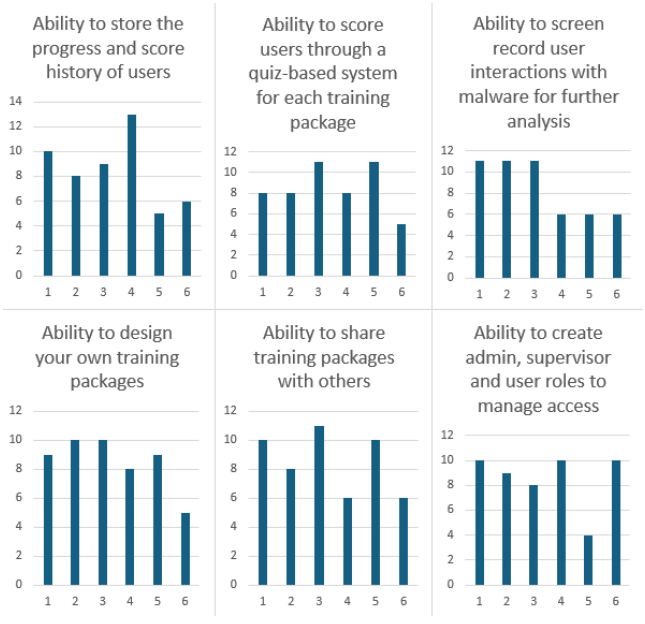

Fig. 5. Aggregate results of respondents highly ranked functional requirements.

Notably, the functional requirements receiving the least number of votes for the lowest ranking were the ability to store the progress and history of users, as well as the ability for respondents to design their own training packages. As these requirements received the least number of votes for the lowest ranking, it can be interpreted that respondents assigned a high importance to such requirements and were unwilling to rank them in low positions.

C. Non Functional Requirements Analysis

Regarding non functional requirements, respondents clearly ranked the ability to interact with the platform through a web browser, with no requirement for software installation as the highest item, as shown in figure 6. This is likely due to the complexity of installing and maintaining such software, especially with the potential for malware simulation. Furthermore, organisations often enact technical controls preventing individuals from installing additional software, or may utilise hardware such as laptops which may be computationally unsuitable to run intensive applications such as the simulation aspects of malware. Operating through a web browser assists in mitigating such issues, as users already experience familiarity with web browsers through day to day activities, as well as offloading the operation of the platform to a web server, thereby reducing the complexity of use for end users.

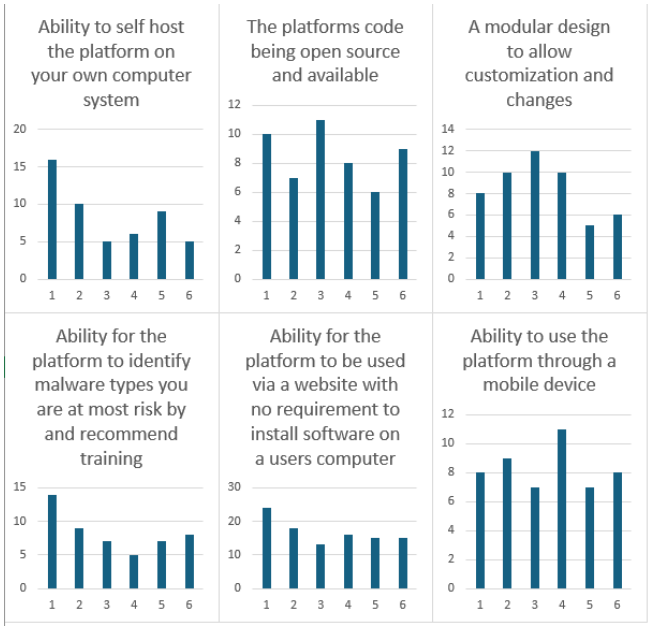

Fig. 6. Aggregate results of respondents highly ranked non functional requirements.

Respondents also assigned the second highest voted non functional requirement as the ability to self host the malware platform on respondents own computer systems. This is a significant shift compared to existing cyber training platforms, which primarily operate under a software-as-a-service (SASS) business model. It is assumed that respondents have assigned

this item as the highest priority due to the ability to exercise greater control over their own data within such a platform, as well as the ability to operate such a tool within their own environments, without the need for a network connection.

Furthermore, respondents identified the ability for a platform to identify the malware types an individual is most at risk of attack from and recommend training in-line with such malware types as the second highest ranking item. Presumably respondents wish to receive training within relevant areas, which could be addressed by this requirement.

Respondents ranked the requirement for the malware training platforms code to be open source and available as the fourth highest item. It is suggested that respondents wish to be able to modify the platform to support their own needs, as well as being able to scrutinize source code and gain a greater level of transparency and assurance compared to tools and platforms that do not offer such a capability.

Notably, respondents also selected the requirement for the malware training platforms code being open source as the requirement with the greatest number of votes in the lowest category. This may be similar to the ranking of role based access control within section V-B, in which respondents may expect such a requirement by default. However, it could also be reasonably determined that the respondents are less concerned with such a platform being open source, provided the platform can be self hosted to afford a greater level of control.

VI. Limitations & Future Work

The research sampling method is susceptible to potential bias from respondents, who may experience a form of acquiescence bias or expectancy bias. To mitigate against this, the researchers utilised question order randomisation systems and deployed neutral language within questions, however it is advised that future work with access to a larger pool of respondents utilises a form of random sampling to gain a more representative sample. Furthermore, the majority of the available respondents are relatively inexperienced within the field of cyber security, with the majority of respondents either having no direct experience or 1-2 years of experience. It is advised to increase the number of respondents with greater experience in cyber, which could then be compared to existing data to determine if sentiments and opinions differ with experience.

The researchers have developed such a solution, which has been successfully prototyped within the previous year. Results from this research will be incorporated into a malware training platform to support the implementation of additional features and provides evidence to support the creation of such a tool.

References

[1] S. Anson, *Applied incident response*, 1st ed. John Wiley & Sons, 2020.

[2] T. Sardar and L. A. Wahsheh, "Design of a cyber security awareness campaign to be implemented in a quarantine laboratory," *J. Comput. Sci. Coll.*, vol. 35, no. 9, p. 11–18, 2020.

[3] W. M. Al-Rahmi, N. Alias, M. S. Othman, A. I. Alzahrani, O. Alfarraj, A. A. Saged, and N. S. Abdul Rahman, "Use of e-learning by university students in malaysian higher educational institutions: A case in universiti teknologi malaysia," *IEEE Access*, vol. 6, pp. 14 268–14 276, 2018.

[4] S. S. Noesgaard and R. Ørngreen, "The effectiveness of e-learning: An explorative and integrative review of the definitions, methodologies and factors that promote e-learning effectiveness," *Electronic Journal of E-learning*, vol. 13, no. 4, pp. pp277–289, 2015.

[5] G. Kiryakova, N. Angelova, and L. Yordanova, "Gamification in education," in *Gamification in education*, Proceedings of 9th International Balkan Education and Science Conference. Edirne, Turkey: International Balkan Education and Science Conference, 2014.

[6] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic malware analysis in the modern era—a state of the art survey," vol. 52, no. 5, 2019. [Online]. Available: https://doi.org/10.1145/3329786

[7] A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso, "The world of malware: An overview," in *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*. Barcelona, Spain: IEEE, 2018, pp. 420–427.

[8] A. Lee, V. Varadharajan, and U. Tupakula, "On malware characterization and attack classification," in *Proceedings of the First Australasian Web Conference - Volume 144*, ser. AWC '13. AUS: Australian Computer Society, Inc., 2013, p. 43–47.

[9] T. Reshmi, "Information security breaches due to ransomware attacks-a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100013, 2021.

[10] M. F. Ansari, "A quantitative study of risk scores and the effectiveness of ai-based cybersecurity awareness training programs," *International Journal of Smart Sensor and Adhoc Network*, vol. 3, no. 3, 2022.

[11] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: a comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022.

[12] M. Alohali, N. Clarke, S. Furnell, and S. Albakri, "Information security behavior: Recognizing the influencers," in *2017 Computing Conference*. IEEE, 2017, pp. 844–853.

[13] R. Shinde, P. Van der Veeken, S. Van Schooten, and J. van den Berg, "Ransomware: Studying transfer and mitigation," in *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, 2016, pp. 90–95.

[14] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *Journal of information security and applications*, vol. 42, pp. 36–45, 2018.

[15] S. Steiner, A. Jillepalli, and D. C. de Leon, "A survey of cloud-hosted, publicly-available, cyber-ranges for educational institutions," *Journal of Computing Sciences in Colleges*, vol. 38, no. 1, pp. 68–77, 2022.

[16] G. Gerontakis, P. Yannakopoulos, and I. Voyiatzis, "Evaluating cybersecurity certifications: A framework for extracting educational scenarios in cybersecurity training," in *Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics*, 2023, pp. 243–248.

[17] A. Stott and C. Neustaedter, "Analysis of gamification in education," *Surrey, BC, Canada*, vol. 8, p. 36, 2013.

[18] P. Wake, S. Black, and J. Young, "Work in progress: Evaluation of security standards through a cyber range using hackers' tactics, techniques and procedures," in *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2023, pp. 653–658.

[19] V. Dumitrasc and R. Serral-Gracià, "User behavior analysis for malware detection," in *European Symposium on Research in Computer Security*. Springer, 2023, pp. 92–110.

[20] F. L. Lévesque, S. Chiasson, A. Somayaji, and J. M. Fernandez, "Technological and human factors of malware attacks: A computer security clinical trial approach," *ACM Transactions on Privacy and Security (TOPS)*, vol. 21, no. 4, pp. 1–30, 2018.

[21] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, and M. F. Costabile, "Human factors in phishing attacks: a systematic literature review," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–35, 2021.

[22] J. L. Marble, W. F. Lawless, R. Mittu, J. Coyne, M. Abramson, and C. Sibley, "The human factor in cybersecurity: Robust & intelligent defense," *Cyber Warfare: Building the Scientific Foundation*, pp. 173–206, 2015.