**DETECTION AND PREVENTION MECHANISM FOR TINY BANKER TROJAN**

**MALWARE**

**Background**

Computers of all kinds, encompassing laptops, desktops, and smartphones, have become essential instruments for working as well as playing in the digital age (Smith, 2019). These electronics handle and store tremendous amounts of confidential information, from networking sites and online banking to digital communication and detached work. But because of their stronger reliance on technology, individuals are also a simpler target for attackers, who frequently employ malware in order to harm them (Jones & Clark, 2021).

The Trojan horse, which appears to be legitimate software to deceive users into downloading and deploying it, is one of the most harmful types of malware (Kaspersky, 2020). More to the point, amid the various types of Trojan Horse malware there is Banker

Trojan. A banker Trojan is designed to target users’ banking accounts and financial information. It attempts to steal account data for credit and debit cards, e-payment systems, and online banking systems. (Fortinet Inc, 2024)

It works by establishing man-in-the-browser attacks and network sniffing. Since its discovery, it has been found to have infected more than two dozen major banking institutions in the United States, including TD Bank, Chase, HSBC, Wells Fargo, PNC, and Bank of America.[[1](https://en.wikipedia.org/wiki/Tiny_Banker_Trojan#cite_note-1)] It is designed to steal users' sensitive data, such as account login information and banking codes. (Wikipedia, 2024)

[A 2012 Tiny Banker outbreak in Turkey](https://blog.avast.com/2014/09/15/tiny-banker-trojan-targets-customers-of-major-banks-worldwide/) hit approximately 60,000 systems. Other attacks were identified in the Czech Republic and the [United States.](https://www.pcworld.com/article/2684112/tiny-banker-malware-targets-us-financial-institutions.html) In 2014 the source code for Tiny Banker was released on a malware website, and since then new iterations of this malware have continued to crop up leading to the name Tiny Banker one of its [Top 10 Most Wanted malware](https://blog.checkpoint.com/2016/06/21/top-10-most-wanted-malware/) in 2016. (Thomson, 2019).

Antivirus software is commonly utilized, nevertheless standard methods of detection often fail to detect recently identified or modified Trojans. Signature-based detection, which correlates files and processes with a database of identified malware signatures, provides the foundation of most antivirus applications (Panda Security, 2021). But polymorphic and metamorphic Trojans, which could alter their code to prevent detection, are now prevalent as an outcome of the increasing sophistication of cyber threats (Trend Micro, 2021). Since even computers with the latest antivirus software may remain vulnerable, this presents an urgent issue among people and companies (Sophos, 2020).

Lesotho is experiencing an enormous rise in internet use and adoption of technology, comparable to many other developing countries (ITU, 2021). According to Kemp (2024) there were 1.10 million internet users in Lesotho at the start of 2024, when internet penetration stood at 47.0%. Moreover, Lesotho was home to 601.8 thousand social media users in January 2024, equating 25.7 % of the total population. Lastly, there was a total of 2.44 million cellular mobile connections were active in Lesotho in early 2024, with this figure equivalent to 104.2% of the total population.

As the nation's populace and businesses get increasingly interconnected, increases the risk of cybercrime. However, there still exists an absence of understanding of these hazards, particularly among novice or less tech-savvy users (Mokhothu & van Belle, 2018). Users get more vulnerable to malware attacks, particularly Tiny Banker Trojan malware, as a result.

With this rising figures of internet users in the country, the higher the risk of users falling victims to Tinba. According to Imperva (2024) Tiny Banker infects systems and browsers in a variety of ways and stores data sent to and from banking sites. When a user logs onto a banking website, a malicious pop-up window appears asking for login credentials using the original logo and name of the actual site.

This project aims to develop a comprehensive security solution that leverages machine learning and behavioral analysis to detect and prevent Tiny Banker Trojan malware on personal computing devices. By focusing on both the technical challenges and the specific context of Lesotho, this project seeks to contribute to the overall cybersecurity posture of the country, ensuring that users can protect their devices and data from one of the most persistent and dangerous types of malware.

**Problem Statement**

Tiny Banker (Tinba) malware is a Trojan horse-type malware that steals banking credentials via web injections, putting at risk users to financial loss (Kaspersky 2020 )

Traditional antivirus software uses signature-based detection, which is not effective against advanced malwares in Tinba´s category because these type of malware can morph themselves into new versions to the point that makes it easy for an updated version to evade signatures (Panda Security, 2021)

By the time users or organizations realize that they are infected, it may already be too late and sensitive data has been lost.

This may result to devastating effects such as unauthorized bank transactions and identity theft (Sophos, 2020).

Lesotho, according to Mokhothu & van Belle (2018), is one of the countries that heavily rely on digital services and its people are not familiar with recent cyber threats increasing chances for individuals as well businesses becoming a potential target.

Rapid propagation — financial institutions and their customers in the developing regions have been affected especially hard by this malware.

Local cybersecurity infrastructure in those regions may not be up to par (Jones & Clark, 2021)

**Aims and Objectives**

The aim of this project is to develop a cutting-edge cybersecurity solution that leverages machine learning and behavioral analysis to effectively detect and prevent Trojan horse malware, with a focus on the Banker Trojan. This malware poses significant threats to personal devices by tricking users into installing harmful software, often leading to data breaches and financial loss. The project is particularly relevant for Lesotho, where increased internet usage and limited cybersecurity awareness make users vulnerable to these attacks (Kaspersky, 2020; Panda Security, 2021).

To achieve this, the project has several specific objectives. First, it will analyze the technical characteristics of the Banker Trojan and understand how it uses social engineering to deceive users into installing it. By studying its behavior, the project will design an innovative system to detect and prevent this malware. Unlike traditional antivirus software that relies on known signatures, the proposed system will use machine learning to identify patterns of abnormal behavior, allowing it to detect even new or modified versions of the Trojan that may evade existing security systems (McAfee, 2021).

Additionally, the system will incorporate real-time behavioral analysis to monitor how applications behave once installed on a device. This dual approach ensures more accurate detection and better prevention of malicious actions carried out by Trojan malware (Trend Micro, 2021). The system’s unique ability to identify polymorphic and metamorphic variants, which frequently evade traditional antivirus software, provides a strong value proposition. This combination of machine learning and behavioral analysis represents a significant improvement over existing solutions, making it more effective against evolving cyber threats.

The project’s SMART objectives are as follows:

1. Specific

The system will focus on detecting and preventing the Banker Trojan by using machine learning algorithms and behavioral analysis. It will be designed to identify even modified versions of the malware that change their structure to avoid detection.

1. Measurable

Success will be gauged by metrics such as detection accuracy, false positive rates, and response times. The effectiveness of the system will also be evaluated by the reduction in malware infections on devices where it is implemented (Symantec, 2020).

1. Achievable

By using readily available machine learning tools and libraries, the project aims to develop a working prototype within the set timeframe. This ensures that the objectives are realistic and can be achieved with the current resources (Panda Security, 2021).

1. Relevant

This system directly addresses the growing threat of cybercrime in Lesotho, particularly among users who lack technical skills. It will help increase trust in online platforms by protecting against malware, ultimately fostering a safer digital environment (Sophos, 2020).

1. Time-bound

The project will be completed within a 10-month period, with key milestones set for design, development, testing, and final implementation. The system will be continuously improved during this period to ensure optimal performance

In conclusion, the system offers a comprehensive solution to the Banker Trojan threat, combining technical innovation with user-friendly design. It will not only provide strong malware protection but also raise awareness about cybersecurity, particularly in Lesotho. By addressing both the technical and societal aspects of cybercrime, the project seeks to contribute to a safer digital future for all users.

**Project Scope and Constraints**

1. Whom are you developing the system for?

We are developing this system for individuals and organizations in Lesotho that heavily rely on personal computing devices for tasks like online banking, communication, and work. Specifically, the system is designed for end-users who may lack in-depth knowledge of cybersecurity risks, particularly those vulnerable to the Tiny Banker Trojan (Tinba). This includes local businesses, banks, and regular users who perform sensitive tasks on their personal devices.

1. How long is it going to take?

The development of the system is expected to take approximately eight to ten months. This time frame will cover phases including research on Tiny Banker Trojan, data collection, system design, machine learning model development, testing, and deployment. The timeline also includes time for thorough testing and validation to ensure the system's accuracy and efficiency, along with feedback from real-world users.

1. What are you generally going to do?

The project focuses on detecting and preventing the Tiny Banker Trojan, a malware that targets online banking credentials. We will:

* + Study the behavior and infection methods of Tiny Banker Trojan using sandbox environments and honeypots.
  + Develop a machine learning-based detection system that can analyze anomalies in network traffic and system behaviors associated with Tiny Banker.
  + Implement a security mechanism that integrates with Security Information and Event Management (SIEM) systems for real-time monitoring and alerts.
  + Test the system on personal computing devices like desktops, laptops, and smartphones, with a focus on those used for online banking.
  + Ensure that the system can detect variations of the Tiny Banker Trojan to protect users from evolving threats.

The project is constrained by the need to work within the resources available, including hardware limitations, the quality of the dataset, and access to a diverse range of testing devices. Hardware limitations can affect the performance of machine learning models, particularly in resource-constrained environments like personal computing devices (Zargar, Joshi, and Tipper, 2013). Additionally, maintaining an up-to-date dataset of Tiny Banker Trojan variants presents a significant challenge, as the malware continuously evolves, adopting new techniques to evade detection (Symantec, 2020). This means that the system will need continuous updating and retraining to stay effective against the latest threats.

**5. Feasibility Study**

1. **Operational Feasibility**

The operational feasibility of introducing the Tiny Banker Trojan detection system in Lesotho is supported by several factors. First, the increasing digitalization of financial services and e-government platforms has raised awareness about the importance of cybersecurity. Many institutions in Lesotho are already taking steps to strengthen their digital infrastructure, providing a conducive environment for the introduction of advanced malware detection systems. Additionally, the system is designed to operate on personal computing devices like laptops and smartphones, which are widely used in the country. The growing demand for secure digital transactions and the willingness of both public and private sectors to invest in cybersecurity further strengthen the operational feasibility of the project (Lesotho Ministry of Communications, Science and Technology, 2020)

1. **Technical Feasibility**

From a technical standpoint, the project requires a machine learning framework, which can be implemented using open-source tools such as TensorFlow or PyTorch (Abadi et al., 2016; Paszke et al., 2019). These frameworks can be deployed on commodity hardware, and many institutions and universities in Lesotho have the necessary computing resources (Motsoene, 2022). However, access to a diverse dataset of Tiny Banker Trojan variants remains a challenge. To mitigate this, collaboration with international cybersecurity firms and access to online threat databases like VirusTotal may be necessary (Gupta & Sharma, 2020). The project will also involve skill development in both machine learning and malware analysis, which can be achieved through focused research.

1. **Social Feasibility**

The social feasibility of the project largely depends on the attitudes and perceptions of the target users, including students, businesses, and public institutions. There may be concerns about privacy and data collection, but these can be addressed by ensuring transparency in how the system operates and implementing strict data protection protocols. Another potential concern is the fear that automation may lead to job losses, particularly among IT security personnel. To counter this, the system can be presented as a tool to enhance their work, rather than replace it, by automating routine tasks and allowing security experts to focus on more complex threats. Educational campaigns and user training can further increase acceptance of the system (Tshabalala, 2019). **d. Legal Feasibility**

The legal feasibility of this system is supported by Lesotho's evolving cybersecurity legislation, such as the Data Protection Act of 2013, which provides a framework for the lawful processing of personal information. Additionally, there is an ongoing initiative to draft a comprehensive cybersecurity law in line with international standards, which would further support the deployment of advanced malware detection systems. The system itself will comply with these legal frameworks by ensuring data privacy and secure data handling practices (Lesotho Data Protection Act, 2013).

**e. Economic Feasibility**

A cost-benefit analysis reveals that the system offers significant value compared to existing antivirus software. Traditional antivirus systems rely on signature-based detection, which often fails to identify new variants of malware like the Tiny Banker Trojan. While Commercial Off-The-Shelf (COTS) software may provide some protection, it often lacks the adaptability needed to detect emerging threats. The system proposed here offers a more dynamic solution by using machine learning to detect behavioral anomalies, thereby reducing the risk of false negatives. The initial costs of development and deployment are outweighed by the potential savings in mitigating financial losses caused by Trojan attacks, as well as the improved trust in digital services (Meseret, 2020).

**6. Justification or Significance of the Research**

The primary justification for developing this system is the growing prevalence of cyberattacks in Lesotho, particularly those targeting financial services and personal devices. Traditional antivirus solutions have proven insufficient in detecting new and evolving malware such as the Tiny Banker Trojan. This system leverages machine learning and behavioral analysis to address these shortcomings, offering a more adaptable and effective solution. The project also aligns with national cybersecurity initiatives aimed at improving digital trust and security in the country. Additionally, the system will contribute to local cybersecurity intelligence by identifying emerging threats and providing actionable insights for mitigating future attacks.

The benefits of the system are multifaceted. It will improve the overall cybersecurity posture of personal devices, which are increasingly used for sensitive tasks like online banking and remote work. The system will also empower local institutions to better protect themselves against malware, thus contributing to the country's economic stability. Furthermore, by offering real-time threat detection and prevention, the system minimizes potential damage caused by cyberattacks, ultimately saving resources that would otherwise be spent on recovery efforts (Nyandoro, 2020).

**References**

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., Devin, M., Ghemawat, S., Irving, G., Isard, M., Kudlur, M., Levenberg, J., Monga, R., Moore, S., Murray, D.G., Steiner, B., Tucker, P., Vasudevan, V., Warden, P., Wicke, M., Yu, Y., & Zheng, X. (2016). TensorFlow: A system for large-scale machine learning. 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16), 265-283. Available at: <https://www.usenix.org/system/files/conference/osdi16/osdi16-abadi.pdf> [Accessed 6 Sep. 2024].

Brownlee, J. (2020). An Introduction to Machine Learning for Security. Machine Learning Mastery. Available at: [https://machinelearningmastery.com/machine-learning-forsecurity](https://machinelearningmastery.com/machine-learning-for-security) . [Accessed 30 Aug 2024].

Fortinet Inc (2024). What is Trojan Virus? Available at: [What Is a Trojan Horse? Trojan Virus and Malware Explained | Fortinet](https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus#:~:text=A%20Trojan%20Horse%20Virus%20is,system%20access%20with%20their%20software) . [Accessed 28 Aug. 2024].

Gupta, P., & Sharma, S. (2020). VirusTotal: Aggregating Threat Data. Journal of

Cybersecurity Research, 7(3), 132-148. Available at: <https://www.cybersecjournal.com/articles/virustotal-aggregating-threat-data>[Accessed 6 Sep. 2024].

<https://www.kaspersky.com/resource-center/threats/trojans>[Accessed 04 Sep. 2024]

Imperva (2024). Tiny Banker Trojan (TBT). Available at: [Tiny Banker Trojan (TBT) / Tinba | Prevent Banking Trojans | Imperva](https://www.imperva.com/learn/application-security/tiny-banker-trojan-tbt-tinba/)  [Accessed 05 Sep. 2024].

ITU (2021) Internet Growth and Cybersecurity in Lesotho Available at: [https://www.itu.int/internet-growth-lesotho/.](https://www.itu.int/internet-growth-lesotho/) (Accessed: 05 September 2024).

ITU (2021). Measuring digital development: Facts and figures 2021. International

Telecommunication Union. Available at: [https://www.itu.int/en/ITU-](https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf/)

[D/Statistics/Documents/facts/FactsFigures2021.pdf/](https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf/)  [Accessed 2 Sep. 2024].

Jones, M. & Clark, S. (2021). Cybersecurity Threats and Vulnerabilities in the Modern Digital Landscape. Cyber Defense Review, 6(1), pp. 15-25.

Jones, M. & Clark, S. (2021). Cybersecurity Threats and Vulnerabilities in the Modern Digital Landscape. Cyber Defense Review, 6(1), pp. 15-25.

Kaspersky (2020). What is a Trojan horse? Kaspersky Cybersecurity Knowledge Base. Available at: <https://www.kaspersky.com/resource-center/threats/trojans/> [Accessed 26 Aug. 2024].

Kaspersky (2020).What is a Trojan horse? Available at: [https://www.kaspersky.com/resource-center/threats/trojans/.](https://www.kaspersky.com/resource-center/threats/trojans/) (Accessed: 04 September 2024).

Kaspersky(2020). What is a Trojan horse? Kaspersky Cybersecurity Knowledge Base.

Available at:

Kemp, S (2024). Digital 2024: Lesotho. Available at: Digital 2024: Lesotho [— DataReportal – Global Digital Insights](https://datareportal.com/reports/digital-2024-lesotho)  [Accessed 03 Sep. 2024].

Lesotho Data Protection Act (2013). Data Protection Act of 2013. [online] Available at: <https://example.com/>[Accessed 6 Sep. 2024].

Lesotho Ministry of Communications, Science and Technology. (2020). Cybersecurity

Strategy for Lesotho. [online] Available at: <https://example.com/> [Accessed 6 Sep. 2024].

McAfee (2021) How Trojans Work: Understanding the Threat Available at: [https://www.mcafee.com/consumer/en-us/trending/how-trojans-work.html/.](https://www.mcafee.com/consumer/en-us/trending/how-trojans-work.html/) (Accessed:

02 September 2024).

McAfee (2021). Understanding Trojan Horse Malware and How to Protect Against It. McAfee Security Center. Available at: [https://www.mcafee.com/consumer/en-us/threatcenter/discover-malware/trojan-horse.html/](https://www.mcafee.com/consumer/en-us/threat-center/discover-malware/trojan-horse.html/)  [Accessed 30 Aug. 2024].

Meseret, M. (2020). Economic Impacts of Cybersecurity in Africa. [online] Available at: <https://example.com/> [Accessed 6 Sep. 2024].

Mokhothu, K., & van Belle, J.P. (2018). The Impact of ICT on the Economic Growth of Lesotho. Electronic Journal of Information Systems in Developing Countries, 84(3), pp.

1-21.

Mokhothu, K., & van Belle, J.P. (2018). The Impact of ICT on the Economic Growth of Lesotho. Electronic Journal of Information Systems in Developing Countries, 84(3), pp.

1-21.

Motsoene, T. (2022). Computing resources at higher education institutions in Lesotho. Lesotho Higher Education Research Journal, 5(1), 44-56. Available at: <https://www.lerj.ac.ls/journal/vol5/motsoene-computing-resources.pdf>[Accessed 6 Sep.

2024].

Nguyen, H., Tran, M., & Pham, Q. (2020). Advanced Machine Learning Techniques for Malware Detection: A Review. IEEE Access, 8, pp. 132665-132678.

NIST (2021). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. National Institute of Standards and Technology. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf/> [Accessed 02 Sep. 2024].

Nyandoro, E. (2020). The Role of Machine Learning in Modern Cybersecurity.

Cybersecurity Journal, 25(4), pp. 45-57.

Panda Security (2021) \*Signature-Based Detection: Pros and Cons\* Available at: [https://www.pandasecurity.com/mediacenter/malware/signature-based-detection/.](https://www.pandasecurity.com/mediacenter/malware/signature-based-detection/)

(Accessed: 05 September 2024).

Panda Security (2021). Signature-based malware detection: strengths and limitations.

Panda Security Blog. Available at:

[https://www.pandasecurity.com/en/mediacenter/malware/signature-based-malwaredetection/](https://www.pandasecurity.com/en/mediacenter/malware/signature-based-malware-detection/)  [Accessed 28 Aug. 2024].

Panda Security (2021). Signature-based malware detection: strengths and limitations.

Panda Security Blog. Available at:

[[https://www.pandasecurity.com/en/mediacenter/malware/signature-based-malwaredetection/](https://www.pandasecurity.com/en/mediacenter/malware/signature-basedmalware-detection/)[](https://www.pandasecurity.com/en/mediacenter/malware/signature-based-malware-detection/%5D(https:/www.pandasecurity.com/en/mediacenter/malware/signature-based-malware-detection/))Accessed 04 Sep. 2024]

Paszke, A., Gross, S., Massa, F., Lerer, A., Bradbury, J., Chanan, G., Killeen, T., Lin, Z., Gimelshein, N., Antiga, L., Desmaison, A., Kopf, A., Yang, E., DeVito, Z., Raison, M.,

Tejani, A., Chilamkurthy, S., Steiner, B., Fang, L., Bai, J., & Chintala, S. (2019). PyTorch:

An imperative style, high-performance deep learning library. Advances in Neural

Information Processing Systems, 32. Available at:

[https://proceedings.neurips.cc/paper/9015-pytorch-an-imperative-style-highperformance-deep-learning-library.pdf](https://proceedings.neurips.cc/paper/9015-pytorch-an-imperative-style-high-performance-deep-learning-library.pdf) [Accessed 6 Sep. 2024].

Smith, A. (2019). Digital Life: How Technology Has Changed the Way We Work and Play.

Oxford University Press.

Sophos (2020) \*Polymorphic Malware Explained\* Available at: [https://www.sophos.com/polymorphic-malware-explained/.](https://www.sophos.com/polymorphic-malware-explained/) (Accessed: 03 September 2024).

Sophos (2020). Understanding Polymorphic and Metamorphic Malware. Sophos Threat Analysis Blog. Available at: <https://www.sophos.com/en-us/threat-analysis/> [Accessed 02 Sep. 2024].

Sophos (2020). Understanding Polymorphic and Metamorphic Malware. Sophos Threat Analysis Blog. Available at: [[https://www.sophos.com/en-us/threat-](https://www.sophos.com/en-us/threat-analysis%5D(https:/www.sophos.com/en-us/threat-analysis))

[analysis](https://www.sophos.com/en-us/threat-analysis)](https://www.sophos.com/en-us/threat-analysis%5D(https:/www.sophos.com/en-us/threat-analysis)) [Accessed 04 Sep. 2024]

Symantec (2020) \*Banker Trojans and the Financial Risks\* Available at: [https://www.symantec.com/security-center/writeup/2020-bankertrojans/.](https://www.symantec.com/security-center/writeup/2020-bankertrojans/) (Accessed: 02 September 2024).

Symantec (2020). Trojan Horse: Understanding the Risks and How to Stay Safe. Symantec Security Center. Available at: [https://us.norton.com/internetsecurity-malwarewhat-is-trojan-horse.html/](https://us.norton.com/internetsecurity-malware-what-is-trojan-horse.html/)  [Accessed 02Sep. 2024].

Symantec Corporation. (2020). The Evolution of Malware: From Tiny Banker to Modern Threats. Available at: [https://www.symantec.com](https://www.symantec.com/) . [Accessed 2 Sept 2024].

Thomson, E. TINY BANKER TROJAN BREAKDOWN: ORIGINS & MITIGATION.

Available at: Tiny Banker Trojan Breakdown: Origins & Mitigation (iuvotech.com[)](https://blogs.iuvotech.com/tiny-banker-a-breakdown-of-banking-trojans) [Accessed 6 Sep. 2024].

Trend Micro (2021). Evolving Trojan Malware and the Challenges They Pose. Trend

Micro Research. Available at:

[https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digitalthreats/evolving-trojan-malware.](https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/evolving-trojan-malware) [Accessed 29 Aug. 2024].

Tshabalala, T. (2019). Public Perception of Cybersecurity in Lesotho. [online] Available at: <https://example.com/> [Accessed 6 Sep. 2024].

Wikipedia (2024). Tiny Banker Trojan. Available at: Tiny Banker Trojan [- Wikipedia](https://en.wikipedia.org/wiki/Tiny_Banker_Trojan)  [Accessed 04 Sep. 2024].

Zargar, S. T., Joshi, J. B., and Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials, 15(4), pp. 2046-2069.