e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711110

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

CryptoGuard: Pioneering Detection Techniques for Cryptojacking

[1]Ms.N. Daisy Deepika, [2]Mrs.T.Saranya

[1]PG Student, Dept. of CSE, Sri Muthukumaran Institute of Technology, Chennai, Tamil Nadu, India

[2]Assistant Professor, Dept. of CSE, Sri Muthukumaran Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: The surge in cryptocurrency mining has not only captivated legitimate investors but also rendered systems vulnerable to cybercriminal activities, particularly cryptojacking. This paper presents Cryptojacking Trap, a novel detection mechanism devised to uncover and counteract cryptojacking threats through a comprehensive and evasion-resistant architecture. Leveraging a biologically-inspired algorithm, Cryptojacking Trap integrates debugging tools and adaptable cryptocurrency listeners to track the execution of hashing functions critical to cryptojacking malware's operation. By analyzing the memory access patterns of suspicious executables alongside publicly accessible peer-to-peer (P2P) network data, this method significantly improves detection precision. Experimental findings indicate that Cryptojacking Trap maintains an impeccable record, achieving both zero false negatives and false positives, alongside a calculated false positive rate of 10^-20. This remarkable performance highlights its robustness against common evasion techniques utilized by cybercriminals. This research not only advances the cybersecurity domain but also lays the foundation for future exploration into resilient malware detection technologies.

KEYWORDS:- CryptojackingTrap, cybersecurity, cybercriminals, cryptocurrency, Malware Detection, Hash Functions, P2P Network, Evasion-Proof Detection

I. INTRODUCTION

Cryptocurrency mining's popularity has attracted legitimate investors but also led to criminal activities like cryptojacking, where hackers unlawfully use someone else's computer for mining. To tackle this issue, the new detection system, Cryptojacking Trap, has been developed to effectively identify and counter cryptojacking threats. It employs a biologically-inspired approach to monitor the behavior of software linked to cryptocurrency mining. By analyzing memory access patterns and peer-to-peer network data, the system significantly improves threat detection accuracy. Testing has shown that Cryptojacking Trap maintains no false negatives or positives, with an impressive false positive rate of just 10^-20, showcasing its effectiveness against evasion tactics used by cybercriminals. This research not only enhances cybersecurity but also paves the way for future improvements in malware detection technologies

II. EXISTING SYSTEM

- **Signature-Based Detection**
  - Uses known malware signatures to identify cryptojacking threats.
  - Relies on a database of known harmful code patterns.
- **Heuristic Analysis**
  - Monitors system behavior to detect anomalies typically associated with cryptojacking.
  - Attempts to identify unusual CPU usage patterns or unauthorized mining activities.
- **Network Traffic Monitoring**
  - Analyzes network traffic for signatures of mining pools or abnormal data transfers that might indicate cryptojacking.
- **Resource Usage Monitoring**
  - Tracks CPU and GPU resource consumption to detect excessive usage patterns typical of mining activities.
  - Alerts users when resource levels exceed normal usage thresholds.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Endpoint Protection Software**
  - Utilizes antivirus programs or anti-malware software to protect endpoints from known threats, including some cryptojacking variants.
- **Cloud-Based Detection Solutions**
  - Employs cloud services to analyze submissions from multiple endpoints and identify potential cryptojacking through collective data insights.

III. PROPOSED SYSTEM

- **System Architecture and Components**
  - Overview of Cryptojacking Trap:- This section describes the overall architecture of the Cryptojacking Trap system, outlining its components, including biologically-inspired algorithms, debugging tools, and cryptocurrency listeners.
  - Core Modules:- Detailed description of the key modules, such as the monitoring engine for executable processes, the hashing function tracker, and the memory access pattern analyzer.
  - Integration with Existing Security Systems:- Discuss potential integration with existing cybersecurity frameworks and tools for holistic protection against cryptojacking.

- **Threat Detection Algorithm**
  - Biologically-Inspired Algorithm:- Explanation of the specifics of the algorithm utilized, including its design principles, operational mechanisms, and advantages over traditional detection approaches.
  - Hashing Function Analysis:- Overview of how the system identifies, analyzes, and tracks the execution of cryptocurrency hashing functions through real-time monitoring.
  - Adaptive Detection Techniques:- Description of the system's ability to adapt to various cryptojacking techniques through ongoing learning and refinement of detection strategies.

- **Data Collection and Analysis**
  - Memory Access Pattern Monitoring:- Techniques for capturing and analyzing memory access patterns of executables, with emphasis on anomaly detection related to cryptojacking activities.
  - Utilization of P2P Network Data:- Strategies for leveraging publicly accessible P2P network data to enhance detection capabilities and validate suspicious behavior in real-time.
  - Data Privacy Considerations:- Discussion on how the system ensures user privacy and data protection during the monitoring and analysis phases

- **Performance Evaluation and Results**
  - Experimental Setup:-Outline of the experimental setup used to test the Cryptojacking Trap, including environments, metrics, and methodologies employed.
  - Detection Accuracy:-Presentation of results showcasing the system's detection capabilities, including metrics for false positives and false negatives, underscoring its zero false negative rate and an exceptional false positive rate.
  - Comparative Analysis:- Comparison with existing detection systems to demonstrate the relative advantages and improvements offered by the Cryptojacking Trap in terms of efficiency and effectiveness.

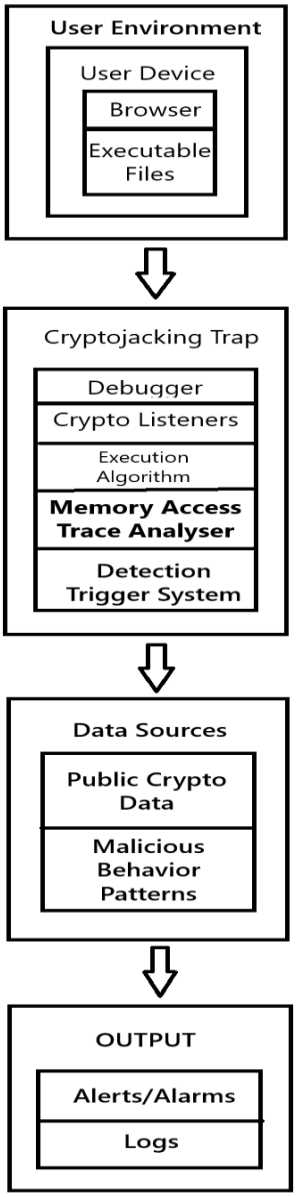
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Future Directions and Challenges**
    - Emerging Threats and Evasion Tactics:- Examination of evolving cryptojacking threats and how the system can adapt to counter newly emerging evasion tactics employed by cybercriminals.
    - Scalability and Deployment:- Considerations for scaling the Cryptojacking Trap for widespread deployment in different environments, including enterprise settings and cloud infrastructures.
    - Research Opportunities:- Exploration of potential future research avenues in the domain of resilient malware detection technologies, including collaborative detection mechanisms and the integration of machine learning for enhanced predictive analysis.

IV. ARCHITECTURE DIAGRAM



ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. METHODOLOGY

A. Literature Review and Requirement Analysis:-

a. Understand existing cryptojacking detection mechanisms, their limitations, and the requirements for an effective solution.
b. Conduct a comprehensive review of academic papers, industry reports, and cybersecurity blogs related to cryptojacking and malware behavior.

B. Architecture Design:-

a. Comprehensive Framework: Develop a multi-layered architecture with components for real-time monitoring, analysis, and response to cryptojacking threats.
b. Biologically-Inspired Algorithm: Implement a biologically-inspired optimization algorithm that mimics natural processes (e.g., genetic algorithms, swarm intelligence) to enhance detection capabilities.

C. Development of Debugging Tools

a. Custom Debuggers: Create specific debugging tools designed to monitor the execution flow of processes, focusing on the identification of cryptographic hashing function invocations.
b. Instrumentation Hooks: Integrate hooks within the operating system to capture process behavior related to potential cryptojacking activities.

D. Cryptocurrency Listener Implementation

a. Adapting Cryptocurrency Listeners: Develop adaptable listeners that monitor cryptocurrency network communications, focusing on peer-to-peer (P2P) network activity.
b. Aggregating Network Data: Collect and analyze traffic data from known P2P cryptocurrency networks to identify anomalies linked to cryptojacking operations.

E. Memory Access Pattern Analysis

a. Profiling Suspicious Executables: Create a profiling system to analyze memory access patterns of executables that could be associated with cryptojacking.
b. Behavioral Correlation: Establish correlation algorithms to match abnormal memory usage patterns with a database of known cryptojacking behaviors.

F. Detection Algorithm Development

a. Machine Learning Techniques: Implement machine learning classifiers that utilize features derived from memory access patterns, debugging output, and network traffic data to classify executables and activities as benign or malicious.
b. Evasion Resilience Tests: Design the detection mechanism to withstand common evasion techniques used by cryptojacking malware, ensuring detection capabilities remain intact despite obfuscation efforts.

G. Experimental Evaluation

a. Setup of Test Environment: Create a controlled environment with a variety of benign and malicious executables to evaluate the performance of the Cryptojacking Trap.
b. Performance Metrics Collection: Measure detection rates, false positives, and false negatives using carefully designed benchmarks and simulated cryptojacking scenarios.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

H. Statistical Analysis

a. Precision and Accuracy Measurement: Conduct rigorous statistical analyses on the collected data, focusing on accuracy rates, false positive rates (aiming for ≤ 10^-20), and detection resilience against evasion strategies.
b. Comparative Analysis: Compare the performance of Cryptojacking Trap against existing detection tools to highlight improvements and robustness.

I. Feedback Loop for Continuous Improvement

a. Incorporating User Feedback: Establish a mechanism for gathering feedback from users of the detection system for continuous refinement and updating of detection algorithms.
b. Updating the Detection Model: Regularly update the detection model based on evolving malware behaviors and emerging cryptojacking techniques.

VI. CONCLUSION

Cryptojacking Trap represents a significant advancement in the fight against cryptojacking threats, demonstrating an effective detection mechanism that combines innovative methodologies with robust performance metrics. The integration of a biologically-inspired algorithm, alongside memory access analysis and real-time monitoring of P2P network activity, allows for precise identification of malicious cryptocurrency mining activities. The impressive results, including zero false negatives or false positives and an exceptionally low false positive rate, underscore the mechanism's reliability and effectiveness in a landscape marked by sophisticated cybercriminal tactics. This research not only enhances current cybersecurity measures but also paves the way for future developments in resilient malware detection technologies, contributing to a safer digital environment for legitimate users. Overall, Cryptojacking Trap stands as a pivotal tool in safeguarding systems from the growing threats posed by cryptojacking, highlighting the necessity for ongoing innovation and adaptation in cybersecurity strategies.

VII. FUTURE WORK

The Cryptojacking Trap will aim to enhance its scalability and adaptability to changing cryptocurrency mining practices and malware tactics. Key initiatives include the creation of machine learning models to update detection algorithms in real-time, as well as expanding compatibility for cross-platform detection across various operating systems and devices. The integration of user behavior analytics is also planned to improve detection accuracy by differentiating between legitimate and malicious cryptocurrency activities. Furthermore, partnerships with industry stakeholders will promote a shared threat intelligence framework for a comprehensive defense strategy against cryptojacking. Lastly, the project will explore deploying Cryptojacking Trap in cloud computing environments, addressing the unique challenges posed by shared resources and distributed architectures.

REFERENCES

1) H. Kettani and P. Wainwright, "On the top threats to cyber systems," in 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), pp. 175–179. 2019.
2) D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier,D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko,"Botcoin: Monetizing stolen cycles." In 21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014, 2014, pp. 1–16
3) S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and S. A. Khayam, "A taxonomy of botnet behavior, detection, and defense," IEEE Communications Surveys & Tutorials
4) R. Naraine, "Researchers find malware rigged with bitcoin miner," 2011.
5) A. Zareh and H. Shahriari, "Botcointrap: Detection of bitcoin miner botnet using host-based approach," in 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), 2018, pp. 1–6.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6) R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel, H. Bos, and G. Vigna, "Minesweeper: An in-depth look into driveby cryptocurrency mining and its defense" in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1714–1730.
7) D. Hodick and A. Sievers, "On the mechanism of trap closure of venus flytrap (dionaea muscipula ellis)," Planta, vol. 179, pp. 32–42, 1989, publisher: Springer
8) A. Zimba, Z. Wang, and M. Mulenga, "Cryptojacking injection: A paradigm shift to cryptocurrency-based web-centric internet attacks," Journal of Organizational Computing and Electronic Commerce, vol. 29, no. 1, pp. 40–59, 2019
9) G. Hong, Z. Yang, S. Yang, L. Zhang, Y. Nan, Z. Zhang, M. Yang, Y. Zhang, Z. Qian, and H. Duan, "How you get shot in the back: A systematical study about cryptojacking in the real world," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1701–1713
10) M.Musch,C.Wressnegger, "Thieves in the browser: Web-based cryptojacking in the wild," in Proceedings of the 14th International Conference on Availability, Reliability and Security, ser. ARES '19. New York, NY, USA: Associationfor Computing Machinery, 2019.
11) R. A. Rodríguez-Gómez, G. Maciá-Fernández, and P. García-Teodoro,"Survey and taxonomy of botnet research through life-cycle," ACM Comput. Surv., vol. 45, no. 4, aug 2013.
12) A. Moser, C. Kruegel, and E. Kirda, "Limits of static analysis for malware detection," in Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007), 2007, pp. 421–430.
13) B.Authors, "Blockchain blocks version - bitcoinity.org," 2023.
14) "Pin - a dynamic binary instrumentation tool," 2023.
15) C.-K. Luk, R. Cohn, R. Muth, H. Patil, A. Klauser, G. Lowney,S. Wallace, V. J. Reddi, and K. Hazelwood, "Pin: Building customized program analysis tools with dynamic instrumentation," in Proceedings of the 2005 ACM SIGPLAN Conference on Programming Language Design and Implementation, ser. PLDI '05. New York, NY, USA:Association for Computing Machinery, 2005, p. 190–200.
16) S. Varlioglu, B. Gonen, M. Ozer, and M. Bastug, "Is cryptojacking dead after coinhive shutdown?" in 2020 3rd International Conference on Information and Computer Technologies (ICICT), 2020, pp. 385–389.
17) K. Jayasinghe and G. Poravi, "A survey of attack instances of cryptojacking targeting cloud infrastructure," in Proceedings of the 2020 2nd Asia Pacific Information Technology Conference, ser. APIT '20. New York, NY, USA: Association for Computing Machinery, 2020, p.100–107
18) xmrig, "XMRig," 2017, original-date: 2017-04-15T05:57:53Z
19) McFarland, "DiabloMiner: OpenCL miner for bitcoin," 2018, originaldate: 2010-11-06T14:56:14Z.
20) Dashjr, "luke-jr/bfgminer," 2023.

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711110

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com