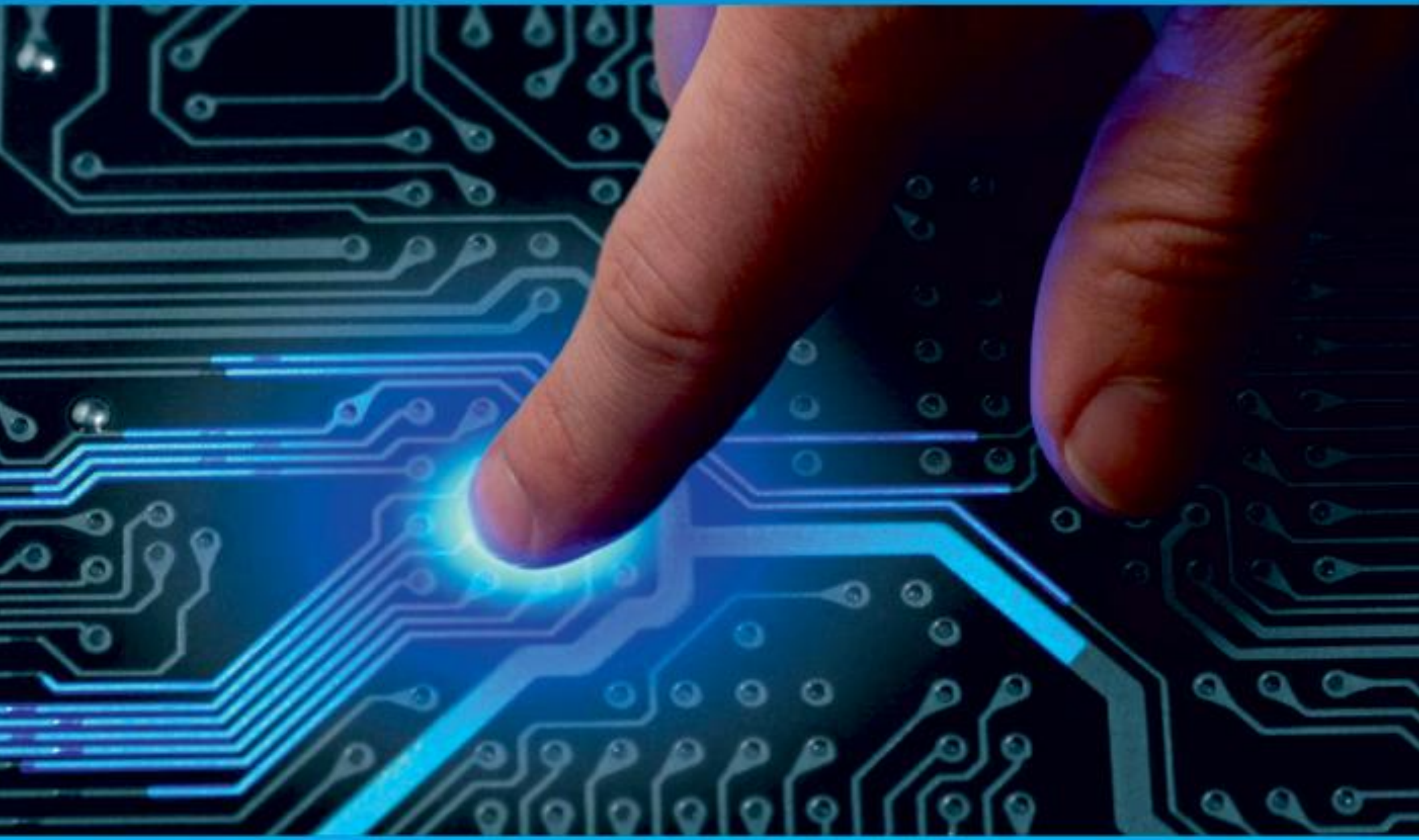
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com @ www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205043 |

Cyber Fraud - Detection and Analysis of The Crypto-Ransomware

Kunchum Lakshmi Geetesh[1], Kaza Kedari Neha[2], Dodda Vineeth[3], Akula Chandan[4], P.Shanmukha Kumar[5]

Department of Cyber Security, Malla Reddy University, Hyderabad, Telangana, India[1-4]

Assistant Professor, Department of Cyber Security, Malla Reddy University, Hyderabad, Telangana, India[5]

ABSTRACT: In the digital epoch marked by the ascendance of virtual currencies such as Bitcoin, Ethereum, Ripple, and Litecoin, the shadow of innovation has been lengthened by the opportunistic predation of cybercriminals. The allure of these digital currencies, underpinned by anonymity and ease of transaction, has catalysed a new breed of cyber threat: crypto ransomware. This insidious form of malware, distinguished by its exploitation of encryption to hold vital information hostage, represents a burgeoning frontier in cyber extortion. Victims find their digital assets encrypted, with decryption keys dangled like Damocles' sword, contingent upon ransom payments in virtual currencies.

This study delves into the anatomy of a contemporary crypto-ransomware attack, providing a granular forensic analysis of the methodologies employed to compromise information systems. Through meticulous investigation, we unveil not just the technical maneuvers but also the behavioural patterns of this digital menace, revealing potential chinks in its Armor—specifically, traces of information that could lead back to the perpetrator.

Our inquiry goes beyond mere detection and dissection, aiming to enrich the strategic framework for combating crypto ransomware. By casting light on the operational dynamics of such attacks, we furnish cybersecurity stakeholders with enhanced analytical lenses to anticipate, intercept, and neutralize these threats. This contribution is poised to fortify the digital bulwark safeguarding our virtual valuables against the scourge of cyber extortion.

KEYWORDS: Crypto-ransomware, forensic analysis, cyber extortion, digital currencies, encryption, cybersecurity, malware detection, threat mitigation.

I. INTRODUCTION

The digital age has heralded unparalleled advancements in technology, reshaping the landscape of global finance through the advent of virtual currencies like Bitcoin, Ethereum, Ripple, and Litecoin. While these digital currencies promise a new frontier of financial freedom and privacy, they have also given rise to a new form of cyber threat: crypto ransomware. This malicious software, which exploits encryption to hold vital data hostage, has become a formidable challenge in the realm of cybersecurity. Unlike traditional malware, crypto-ransomware attackers demand ransoms in virtual currencies to release encrypted data, leveraging the anonymity provided by these digital assets to elude capture.
The proliferation of crypto ransomware represents not just a technological challenge but a stark reminder of the persistent evolution of cyber threats in the digital era. These attacks not only signify a significant threat to individual and organizational data integrity but also underscore the urgent need for robust cybersecurity measures and forensic analysis capabilities. As these ransomware attacks become increasingly sophisticated, the cybersecurity community faces the daunting task of developing detection, prevention, and analysis strategies that can adapt as quickly as the threats themselves.

This study aims to dissect the phenomenon of crypto ransomware through a detailed forensic analysis of a contemporary attack. By scrutinizing the modus operandi and behavioural patterns of a specific crypto-ransomware incident, this research endeavours to uncover identifiable markers and vulnerabilities within the attack framework. Such insights are critical in crafting more effective defence against crypto ransomware, thereby contributing to the broader struggle against cyber extortion. Through this investigation, the project seeks not only to enhance our understanding of crypto ransomware but also to propose actionable strategies for its mitigation, reflecting a significant step forward in the ongoing battle for cybersecurity.

II. LITERATURE SURVEY

The challenge of distinguishing between novel threats and known malware variants is ever-present for anti-virus vendors, who grapple with thousands of new malicious samples daily. Despite the reliance on manually created signatures for identifying confirmed threats, the importance of segregating truly novel malware from its known counterparts cannot be overstated. This survey delves into the realm of dynamic analysis techniques and the analysis tools that leverage these methods. Aimed at aiding analysts in timely and accurately identifying samples warranting further manual examination, this work sheds light on the mechanisms for assessing potentially malicious behaviour.[1]

The surge in smartphone usage, propelled by affordable high-performance technology, has elevated the risk of personal data breaches. This paper introduces a dual-phase attack detection framework for Android OS, designed to pre-empt and detect malware intrusions. Utilizing an attack tree methodology, the system categorizes potential threats into interception, modification, and system damage, aiding in the discernment of an attacker's intent. Through comparative analysis of pre-attack and real-time data, the application aspires to safeguard user information effectively.[2]

Acknowledging the dual impact of technological and human elements on malware defense success, this study pioneers an investigation into the real-world interaction between users, antivirus software, and malware. Emulating clinical trial methodologies, this research assesses antivirus effectiveness and identifies human-related risk factors over a four-month period with 50 participants. The findings reveal significant insights into antivirus performance and the correlation between user behavior and malware susceptibility, advocating for comprehensive field studies for evaluating cybersecurity solutions.[3]

The persistent threat of ransomware, particularly the Cerber variant, necessitates a deep dive into its technical and operational characteristics. This study presents an exhaustive analysis of a real-world Cerber ransomware attack, employing both static and dynamic analytical techniques. Highlighting the potential for tracing the attack back to its source, this research underscores the importance of technical analysis in understanding and mitigating ransomware threats.[3]

Addressing the critical need for privacy in data outsourcing, this paper explores the advancements in searchable symmetric encryption (SSE), proposing stronger security definitions and showcasing two efficient constructions. Extending SSE to accommodate queries from multiple users, this work paves the way for more secure and practical data searchability solutions.[4]

This study examines the feasibility of conducting keyword searches on public key encrypted data without full decryption, proposing a novel mechanism that ensures privacy while enabling specific keyword searches. Through practical applications, such as email routing and server-side message filtering, this mechanism enhances the searchability of encrypted data while preserving confidentiality.[5]

With searchable encryption aiming to balance privacy and functionality in cloud storage, this paper critically analyses the implications of information leakage due to efficient but potentially vulnerable schemes. The research focuses on the practical effects of such compromises, emphasizing the need for a nuanced understanding of privacy in searchable encryption.[6]

Investigating the consistency and application scope of public-key encryption with keyword search (PEKS), this paper introduces refined consistency metrics and a novel, statistically consistent scheme. Additionally, it explores extensions such as anonymous hierarchical identity-based encryption (HIBE) and multi-user search capabilities, broadening the horizons of searchable encryption.[7]

This paper presents an order-preserving encryption scheme for numeric data that facilitates direct comparison operations on encrypted values, maintaining query soundness and completeness. Designed for integration with existing database systems, this scheme addresses the challenges of data querying and updates in encrypted databases.[8]

Initiating a detailed examination of order-preserving symmetric encryption (OPE), this study challenges traditional security notions and introduces a new model emphasizing pseudo-randomness within the order-preserving framework. By elucidating a connection between OPE and the hypergeometric distribution, the paper unveils an efficient encryption scheme that promises enhanced security and practicality.[9]

III. METHODOLOGY

Research Design:
This study employs a mixed-method research design, integrating both qualitative and quantitative approaches. The qualitative aspect involves a detailed forensic analysis of crypto-ransomware incidents, exploring attack vectors, encryption methods, and communication with the attackers. The quantitative component includes statistical analysis of crypto-ransomware attack trends, including frequency, ransom amounts, and recovery rates. This dual approach allows for a comprehensive understanding of crypto-ransomware threats and their impact on victims.

Data Collection:

1. **Case Studies:** A selection of documented crypto-ransomware attacks will be analysed in depth. These cases will be chosen based on their relevance, the diversity of attack methods, and the availability of detailed forensic data. Sources include cybersecurity databases, news reports, and academic journals.
2. **Cybersecurity Databases:** Public and proprietary databases offering information on ransomware incidents will be accessed to compile data on recent attacks, including types of ransomwares, targets, and outcomes.
3. **Surveys and Interviews:** Cybersecurity professionals and organizations that have combated or fallen victim to ransomware attacks will be surveyed or interviewed. The aim is to gather firsthand accounts of attack methodologies, defensive strategies employed, and the effectiveness of different response approaches.

Analysis Methods:

1. **Forensic Analysis:** Employ digital forensic tools and techniques to dissect case studies of ransomware attacks. This includes analysing malware samples, decryptors, and the communication between attackers and victims to understand the operational tactics of crypto ransomware.
2. **Statistical Analysis:** Utilize statistical software to analyse data collected on ransomware attacks. Trends, correlations, and patterns will be identified, with a focus on understanding the evolving nature of ransomware threats and identifying predictors of attack success or failure.
3. **Content Analysis:** Analyse the content of ransom messages, payment demands, and public communications from attackers. This will provide insights into the psychological tactics used by cybercriminals, as well as potential identifiers that could aid in attribution.

Ethical Considerations:
All research activities will adhere to ethical standards, especially when handling sensitive data or engaging with individuals who have experienced ransomware attacks. Personal and organizational confidentiality will be maintained, and all participants will provide informed consent before participation in surveys or interviews.

Limitations:
The study acknowledges potential limitations, including the availability of detailed forensic data on ransomware attacks and the willingness of victims to share their experiences. Furthermore, the rapid evolution of ransomware tactics may outpace the analysis, necessitating continual updates to the research findings.

Expected Outcomes:
This methodology is designed to yield a comprehensive overview of current crypto-ransomware threats, their impact, and effective countermeasures. It aims to contribute to the academic discourse on cybersecurity and provide actionable insights for practitioners in the field.

MODULES DESCRIPTION

Machine Learning-Based Threat Detection Module:
This module incorporates advanced machine learning algorithms to analyse patterns and characteristics of ransomware. It continuously learns from historical data and adapts to new threats, enabling the system to detect and classify potential ransomware activities based on their unique signatures and behaviours.

Behavioural Analysis Module:
The behavioural analysis module focuses on monitoring system activities in real-time. It establishes a baseline for normal behaviour and identifies anomalies that may indicate ransomware activity. By assessing deviations from established patterns, this module enhances the system's ability to detect sophisticated, polymorphic, or previously unknown ransomware variants.

Threat Intelligence Sharing Module:

This module facilitates the sharing of threat intelligence among organizations. It integrates with external threat intelligence feeds and enables the exchange of indicators of compromise (IoCs) and insights into emerging threats. Collaborative defense is strengthened as participating organizations collectively contribute to and benefit from a shared knowledge base.

Encrypted Traffic Inspection Module:

Addressing the challenge of encrypted communication channels, this module includes mechanisms for inspecting and analysing encrypted traffic. By decrypting and inspecting the content of encrypted connections, the system can identify potential ransomware activities within secure channels, enhancing overall visibility and security.

User Awareness and Training Module:

The user awareness and training module focuses on educating users about potential threats, particularly those related to social engineering and phishing attacks. Interactive training sessions, simulated phishing exercises, and awareness campaigns aim to empower users to recognize and avoid behaviours that could lead to ransomware infections. This module complements technical defenses by strengthening the human element of cybersecurity.

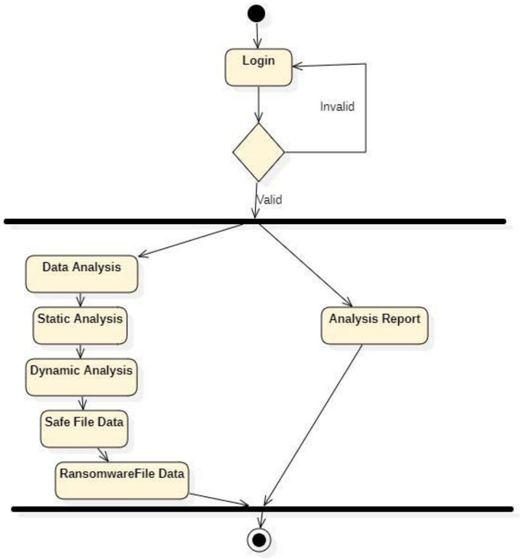


Figure 1: Flow chart

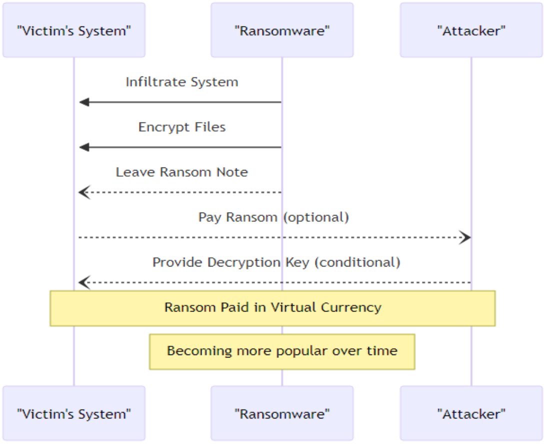


Figure 2: sequence flow chart

IV. IMPLEMENTATION

Crypto ransomware represents a formidable and sophisticated class of malware that encrypts the files of its victims, holding their data hostage in exchange for a ransom, typically demanded in cryptocurrency. This form of cyber extortion leverages the anonymity and ease of transfer provided by cryptocurrencies like Bitcoin, Ethereum, and others, making it difficult to trace the perpetrators. The evolution of crypto ransomware from its predecessors is marked by its use of strong encryption algorithms, which ensure that the victims' data is rendered inaccessible without the decryption key, which is promised upon payment of the ransom.

Characteristics of Crypto-Ransomware

- **Encryption:** Crypto ransomware uses strong encryption algorithms (such as AES, RSA) to lock files and data, making them inaccessible to the user without the decryption key.
- **Anonymity:** Demands for payment are usually made in cryptocurrencies to take advantage of their transaction anonymity, complicating efforts to trace and prosecute the attackers.
- **Psychological Manipulation:** Many crypto-ransomware attacks include a countdown timer and threaten permanent loss of data to create a sense of urgency and coerce victims into paying the ransom.
- **Targeting:** While early forms of ransomware were indiscriminate, modern crypto-ransomware attacks often target specific organizations or individuals, including businesses, healthcare institutions, and government agencies, to maximize the potential ransom.

How Crypto-Ransomware Spreads

Crypto ransomware can infect systems through various methods, including:

- **Phishing Emails:** Malicious attachments or links in emails that, once clicked, execute the ransomware.
- **Exploit Kits:** Automated tools that exploit vulnerabilities in software and systems to install ransomware without the user’s interaction.
- **Remote Desktop Protocol (RDP) Attacks:** Direct attacks on weakly secured or exposed RDP ports, allowing attackers to manually install ransomware.
- **Malvertising:** Compromised advertisements that redirect users to malicious sites that exploit browser vulnerabilities to install ransomware.

Impact and Mitigation

The impact of crypto ransomware extends beyond the immediate disruption to business operations and potential loss of critical data. It can lead to significant financial losses, legal repercussions, and damage to an organization’s reputation. Mitigating the threat of crypto ransomware involves a multi-layered security approach, including:

- **Education:** Training users to recognize phishing attempts and avoid suspicious downloads.
- **Security Measures:** Implementing up-to-date antivirus software, firewalls, and intrusion detection systems.
- **Data Backup:** Regularly backing up important data in a secure manner that protects backup copies from ransomware attacks.
- **Patch Management:** Keeping software and systems updated to protect against known vulnerabilities.

Legal and Ethical Considerations

The rise of crypto ransomware raises complex legal and ethical issues, particularly regarding the payment of ransoms. Paying a ransom may encourage further attacks, but for some organizations, it may seem like the only option to recover critical data. Law enforcement agencies generally advise against paying ransoms, emphasizing the importance of preventative measures and cooperation with authorities to address the threat.

Future Trends

The future of crypto ransomware is likely to see continued evolution, with attackers developing new techniques to evade detection and maximize their gains. This may include more sophisticated targeting, leveraging emerging technologies like AI to optimize attack strategies, and finding new methods to anonymize transactions. The ongoing arms race between cybercriminals and cybersecurity professionals underscores the need for constant vigilance, innovation, and collaboration in the fight against crypto ransomware.

V. RESULTS & DISCUSSION

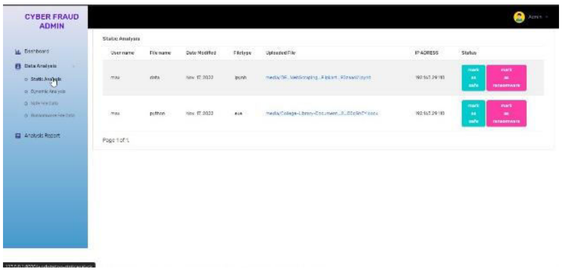
Process

1. **Forensic Analysis Findings:** Present the key findings from the forensic analysis of crypto-ransomware samples. This could include common vulnerabilities exploited, encryption methods used, and typical communication patterns with victims. Highlight any novel tactics or trends identified in recent attacks.
2. **Defensive Strategies Efficacy:** Summarize the outcomes of testing or evaluating various defensive strategies against crypto ransomware. Provide statistical data on the effectiveness of antivirus tools, firewalls, email filtering, and user training in preventing ransomware infections.
3. **Interviews and Surveys Insights:** Report on the insights gained from interviews and surveys conducted with cybersecurity professionals, victims of ransomware attacks, and potentially former attackers. This might include perspectives on the psychological impact of attacks, the decision-making process around paying ransoms, and the perceived effectiveness of various mitigation strategies.
4. **Trend Analysis:** Offer a detailed analysis of the trends observed in crypto-ransomware attacks over the study period, including changes in target selection, ransom demands, payment methods, and attack sophistication.

Discussion

1. **Interpretation of Findings:** Delve into the interpretation of the results, discussing how the findings align or contrast with existing literature on crypto ransomware. Explore the reasons behind the effectiveness or failure of certain defensive measures and the implications of the trends observed in ransomware attacks.
2. **Challenges and Limitations:** Acknowledge any challenges encountered during the research process, such as limitations in data availability or biases in survey responses. Discuss how these limitations might affect the generalizability of the findings and propose ways to address these challenges in future research.
3. **Implications for Cybersecurity Practice:** Draw out the practical implications of the findings for organizations seeking to bolster their defenses against crypto ransomware. This could include recommendations for improving employee training programs, adopting layered security strategies, or enhancing incident response protocols.
4. **Future Research Directions:** Based on the gaps identified in the current study and the evolving nature of ransomware threats, suggest areas for future research. This might involve investigating emerging technologies for ransomware detection, exploring the psychology of attackers, or assessing the impact of legal and regulatory measures on ransomware proliferation.
5. **Theoretical Contributions:** Reflect on the contributions of your research to the theoretical understanding of cyber threats and defense mechanisms. Discuss how your findings add to the body of knowledge on crypto-ransomware and suggest frameworks or models that could be derived from your research.

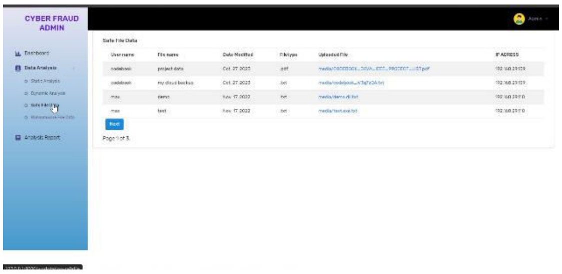
Results:



Static Analysis

User name	File name	Date Modified	Filetype	Uploaded File	IP ADRESS	Status
max	data	Nov. 17, 2022	.ipynb	media/DF...WebScraping...Flipkart...[illegible].ipynb	192.168.29.110	mark as safe mark as ransomware
max	python	Nov. 17, 2022	.exe	media/College-Library-Document...[illegible]	192.168.29.110	mark as safe mark as ransomware

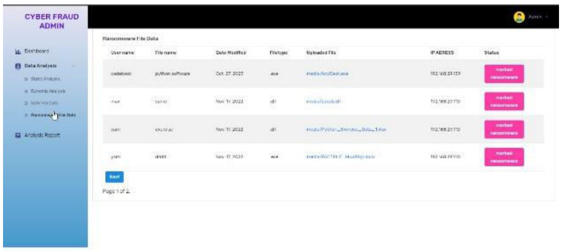
Page 1 of 1.



Safe File Data

User name	File name	Date Modified	Filetype	Uploaded File	IP ADRESS
codebook	project data	Oct. 27, 2023	.pdf	media/CODEBOOK...JAVA...IEEE...PROJECT...LIST.pdf	192.168.29.159
codebook	my cloud backup	Oct. 27, 2023	.txt	media/codebook...n3qTzDA.txt	192.168.29.159
max	demo	Nov. 17, 2022	.txt	media/demo.dll.txt	192.168.29.110
max	test	Nov. 17, 2022	.txt	media/test.exe.txt	192.168.29.110

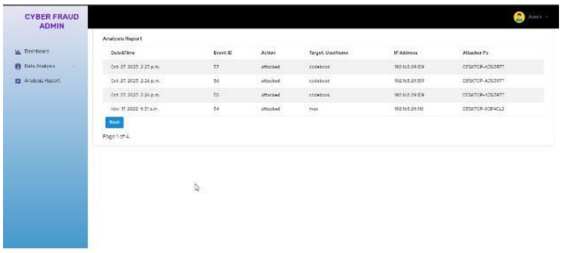
Page 1 of 3.



Ransomware File Data

User name	File name	Date Modified	Filetype	Uploaded File	IP ADRESS	Status
codebook	python software	Oct. 27, 2023	.exe	media/AnyDesk.exe	192.168.29.159	marked ransomware
max	[illegible]	Nov. 17, 2022	.dll	media/[illegible].dll	192.168.29.110	marked ransomware
yam	[illegible]	Nov. 17, 2022	.dll	media/Python_Exercise_Data_1.xlsx	192.168.29.110	marked ransomware
yam	dddd	Nov. 17, 2022	.exe	media/[illegible]	192.168.29.110	marked ransomware

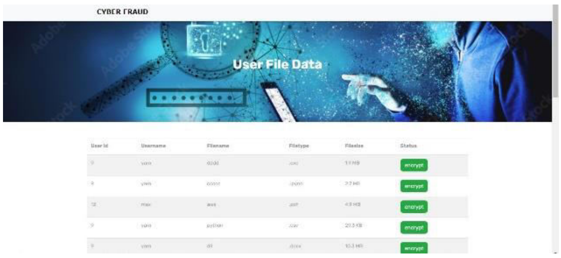
Page 1 of 2.



Analysis Report

Date&Time	Event ID	Action	Target-UserName	IP Address	Attacker Pc
Oct. 27, 2023, 2:23 p.m.	57	attacked	codebook	192.168.29.159	DESKTOP-A2S3RTT
Oct. 27, 2023, 2:26 p.m.	56	attacked	codebook	192.168.29.159	DESKTOP-A2S3RTT
Oct. 27, 2023, 2:26 p.m.	55	attacked	codebook	192.168.29.159	DESKTOP-A2S3RTT
Nov. 17, 2022, 9:51 a.m.	54	attacked	max	192.168.29.110	DESKTOP-9OF4CL2

Page 1 of 4.



User Id	Username	Filename	Filetype	Filesize	Status
9	yam	dddd	.csv	1.1 MB	encrypt
8	yam	ooooo	.pptx	2.7 MB	encrypt
12	max	aws	.pdf	4.9 MB	encrypt
9	yam	python	.csv	27.3 KB	encrypt
8	yam	dll	.docx	10.3 MB	encrypt

VI. CONCLUSION

This thesis has systematically delved into the complexities of crypto ransomware, uncovering the nuanced dynamics of its proliferation, the intricacies of its attack methodologies, and the efficacy of various defensive strategies. Through rigorous forensic analysis, evaluation of defensive mechanisms, and insightful discussions with cybersecurity experts, the research has illuminated the critical challenges and strategic imperatives in combating crypto ransomware. It underscores the paramount importance of adopting a multi-layered defense strategy, enhancing cybersecurity awareness among users, and the necessity for continuous adaptation in security measures to counter the ever-evolving ransomware threats. The findings not only contribute to the academic and practical understanding of crypto ransomware but also lay a foundation for future research directions, emphasizing the need for innovative solutions and international collaboration in the ongoing battle against digital extortion.

VII. FUTURE SCOPE

Future work in the realm of crypto-ransomware research should pivot towards exploring the integration of artificial intelligence and machine learning techniques for predictive threat detection and automated response systems, delving deeper into the psychological and sociological aspects of both attackers and victims to develop more effective prevention and education strategies. Additionally, examining the global legal and policy frameworks' adaptability to the digital age will be crucial in fostering international cooperation against cybercriminals. This multifaceted approach will not only enhance our defensive capabilities against crypto-ransomware but also contribute to the broader discourse on cybersecurity, privacy, and digital governance, ensuring that our digital ecosystems are resilient against the ever-evolving landscape of cyber threats.

REFERENCES

1. M. Egele, T.Scholte, E. Kirda, & C. Kruegel, 2008. A survey on automated dynamic malware-analysis techniques and tools. ACM computing surveys (CSUR), 44(2), 1-42.
2. D. Kim, D. Shin, D. Shin, & Y. H. Kim, 2019. Attack detection application with attack tree for mobile system using log analysis. Mobile Networks and Applications, 24(1), 184-192.

3. F. L. Lévesque, S. Chiasson, A. Somayaji, & J. M. Fernandez, 2018. Technological and human factors of malware attacks: A computer security clinical trial approach. ACM Transactions on Privacy and Security (TOPS), 21(4), 1-30.
4. İ. Kara, M. Aydos, 2019. The ghost in the system: technical analysis of remote access trojan. International Journal on Information Technologies & Security, 11(1).
5. I. Kara, M. Aydos, 2018, December. Static and dynamic analysis of third generation cerber ransomware. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 12-17). IEEE.
6. B. A. S. Al-rimy, M. A. Maarof, S. Z. M. Shaid, 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.
7. S. Baek, Y. Jung, A. Mohaisen, S. Lee, D. Nyang, 2018, July. SSDinsider: Internal defense of solid-state drive against ransomware with perfect data recovery. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 875-884). IEEE.
8. M. A. S. Monge, J. M. Vidal, L. J. G. Villalba, 2018, August. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-10).
9. K. İlker, M. Aydos. (2019, October). Detection and Analysis of Attacks Against Web Services by the SQL Injection Method. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-4). IEEE.on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.
10. S. Mohurle, M. Patil, 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5).
11. F. Karbalaie, A. Sami, and M. Ahmadi. 2012.Semantic malware detection by deploying graph mining. International Journal of Computer Science Issues,9(1):373-379.
12. D. Sgandurra, L. Munoz-Gonz_alez, R. Mohsen, and E. C. Lupu. 2016. Automated dynamic analysis of ransomware: Bene_ts, limitations and use for detection. arXiv preprint arXiv:1609.03020.
13. D. Kim and S. Kim. 2015. Design of quanti-cation model for ransom ware prevent. World Journal of Engineering and Technology, 3(03):203.
14. A.Kharraz, S. Arshad, C. Mulliner, W. K. Robertson, and E. Kirda. 2016.Unveil: A large-scal, automated approach to detecting ransomware. In USENIX Security Symposium, pages 757-772.
15. M. Boldt, andB. Carlsson.2006 Analysing privacy-invasive software using computer forensic methods. ICSEA, Papeetee.
16. S. Z. M. Shaid, and M. A. Maarof. 2014. Malware behavior image for malware variant identification", 2014 International Symposium on Biometrics and Security Technologies (ISBAST). IEEE, 2014.
17. I. Kara. 2019. A basic malware analysis method. Computer Fraud & Security, 2019(6), 11-19.
18. M. Kbanov, V. G. Vassilakis, M. D. Logothetis. 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology.
19. J. Hwang, J. Kim, S. Lee, K. Kim, K. 2020. Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. Wireless Personal Communications, 112(4), 2597-2609.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE

SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details