Ransomware, Threat, and Detection Methods

Yusuf Tezcan
Beykent Üniversitesi

Ransomware, Threat, and Detection Methods

Summary

The rise of ransomware has fostered a distinct cybercriminal landscape. Consequently, this paper aims to offer a comprehensive insight into the threat posed by ransomware and discuss recent detection methodologies. A successful ransomware attack carries direct financial consequences, driven by several mature facilitators such as encryption technology, cyber currency, and accessibility. Encryption, nearly impregnable, remains highly effective. Anonymous cyber currency mitigates traceability risks. The ready availability of ransomware code facilitates easy entry into the cybercriminal sphere. The convergence of these factors presents an enticing avenue for cybercriminals, nurturing specialized perpetrators. Regarding detection techniques, machine learning (ML) via regression algorithms emerges as the most widely adopted method by ransomware researchers. However, none have devised a model to proactively shield against ransomware attacks. This study underscores the necessity for a solution employing ML algorithms for the detection engine.

Introduction

Ransomware has garnered significant attention from cybersecurity experts in recent years, owing to its rapid proliferation and the emergence of new variants capable of circumventing antivirus and anti-malware defenses. It constitutes a relatively novel form of malware but has garnered considerable interest from cybercriminals due to its efficacy in executing successful attacks with direct financial gains. The primary objective of ransomware is to impede victims' access to their data by either locking the operating system or encrypting specific files deemed valuable, such as images, spreadsheets, and presentations. Two primary categories of ransomware exist: locky and crypto. Locky ransomware restricts system access, typically resolvable through rebooting or safe mode. In contrast, crypto ransomware employs encryption technology to render targeted files inaccessible, posing more significant challenges for resolution and potentially irreversible damage. Scareware, a third ransomware variant, induces fear without actual system damage, prompting victims to pay the ransom. This paper focuses on locky and crypto ransomware, omitting discussion of scareware.

Methodology of Literature Review

This research adheres to specific criteria concerning ransomware, emphasizing recent studies from 2015 onwards to ensure relevance. Sources include scientific journals and conference papers for authenticity. The scope remains confined to ransomware threats and detection techniques.

Contribution of Paper

This paper furnishes a comprehensive overview of the ransomware attack lifecycle and its attributes, laying the groundwork for future research endeavors. Furthermore, it reviews existing ransomware detection techniques, delineating their merits and demerits. Based on these findings, a proposed solution in the form of a model is outlined, slated for presentation in subsequent work.

Ransomware

Ransomware constitutes a malware type that impedes victims' data access until a ransom is paid. Its direct financial repercussions have spawned a cybercriminal ecosystem, with ransomware-as-a-service (RaaS) facilitating easy acquisition of ransomware codes. Cyber currency serves as the primary payment method for ransoms, offering anonymity to recipients. Noteworthy encryption technologies include symmetrical, asymmetrical, and hybrid encryption, harnessed by ransomware for file encryption purposes.

Enablers of Ransomware Attack

Ransomware attacks have proliferated due to facilitative enablers, stemming primarily from technological advancements and shifts in lifestyle.

Encryption Technology

Encryption, initially developed for privacy protection, now serves as a double-edged sword exploited by ransomware for extortion purposes. Symmetrical encryption employs a single key for both encryption and decryption, prioritizing speed over security. Asymmetrical encryption utilizes separate public and private keys for encryption and decryption, enhancing security albeit at the expense of speed. Hybrid encryption combines both approaches, optimizing both speed and security.

Cyber Currency

Cyber currency, exemplified by Bitcoin, serves as the predominant ransom payment medium, offering anonymity and wide acceptance. Blockchain technology, employing a one-way hash function, underpins cyber currency transactions, ensuring legitimacy.

Ransomware Accessibility

The proliferation of RaaS and the availability of free development kits, such as Torlocker and Hidden Tear, have lowered the entry barrier for ransomware perpetrators, fostering a surge in ransomware incidents.

Ransomware Lifecycle

The ransomware lifecycle comprises seven stages, delineating a symbiotic relationship between creators and campaigners, fostering specialization among cybercriminals.

Creation

Creators develop ransomware code, continually enhancing it for increased potency across successive cycles.

Campaign

Campaigners disseminate ransomware, targeting individual and institutional victims through various infection vectors, including email attachments, compromised websites, and social media.

Infection

Upon reaching a victim's system, ransomware initiates setup behavior, potentially employing precautionary measures to thwart detection.

Command and Control

Ransomware may establish communication with a command and control center to obtain encryption keys or download additional files.

Search

After acquiring encryption keys, ransomware identifies valuable files for encryption, typically encompassing documents, spreadsheets, and images.

Encryption

Ransomware employs symmetrical, asymmetrical, or hybrid encryption techniques to encrypt targeted files, rendering them inaccessible.

Extortion

The final stage entails displaying a ransom demand, specifying payment modalities and deadlines, threatening irreversible deletion of encrypted files upon non-compliance.

Types of Ransomware Attacks

Locky ransomware restricts system access, often remediable through system rebooting. In contrast, crypto ransomware encrypts specific file types, posing more significant challenges for resolution and potentially irreversible damage.

Ransomware Setup Behavior

Upon successful infiltration, ransomware may employ various precautionary actions to ensure persistent infection, impede system restoration, evade detection, verify system environment, mask communication, and elevate privileges.

Types of Ransomware Analysis

Ransomware analysis aims to elucidate its functionalities, enabling the formulation of defensive measures. Static and dynamic analyses represent two primary approaches.

Static Analysis

This expedient method involves examining executable code features to identify malicious code, susceptible to obfuscation and ineffective against encrypted or multi-phase attacks.

Dynamic Analysis

Behavioral-based analysis entails executing ransomware in a controlled environment to capture and analyze all actions, less susceptible to obfuscation but necessitating costly and time-consuming setups.

Ransomware Detection Techniques

Various techniques, including machine learning, honeypots, and statistical analysis, are employed for ransomware detection, each bearing distinct advantages and limitations.

Machine Learning

ML entails discerning patterns in data to construct predictive models, offering accurate predictions but necessitating careful algorithm selection to mitigate biases and overfitting.

Honeypot

This technique involves deploying decoy files to lure ransomware, offering minimal maintenance but lacking assurance of successful ransomware attraction.

Statistic

Statistical analysis aids in understanding ransomware characteristics but presents implementation challenges as a detection mechanism.

Ref.	Purpose/ Motivation	Methodology	Result	Limitation/ Future Direction
[8]	Early detection can still be effective after the victim is infected.	Honeyfiles in Linux	Ransomware is immediately blocked, and user is notified for its removal	Not tested on other platforms such as Windows and Android Combine honeypot with tracking mechanism
[9]	Intrusion detection (ID) prevention system and antivirus as a single monitoring agent is complex and time-consuming and thus fails in ransomware detection.	Honeyfolder, a decoy folder modelled using social leopard algorithm (SoLA)	Better accuracy and precision, and recall software-defined networking improved network protection with simple rules.	Not tested on healthcare implants and other internet-connected gadget
[10]	Identify salient features of ransomware	Statistical comparison of API call between normal operation and ransomware	Eight APIs existed only in ransomware. Four APIs were found in ransomware to a statistically significant degree. Six API frequencies were more than three standard deviations away from the mean.	Cannot actually be used to detect ransomware.
[11]	Ransomware that can fingerprint environments can evade dynamic analysis.	Five ML algorithms were used for binary classification of ransomware using static analysis of opcodes transformed into n-gram using eight families of ransomware.	Both random forest and K-nearest neighbour produced the highest recall value of 99.8%.	Cannot adequately distinguish between CryptoWall, Locky and Reveton ransomwares according to accuracy metric for binary classification

Reference	Network	PC				Mobile		Cloud	Data Source		Honeypot	Statistic	Machine Learning											Outcome			Evaluation							
		Windows	Mac	Linux	Raspberry	Android	iOS		Dynamic Analysis	Static Analysis			Bayesian	Decision Tree	Dimension Reduction	Instance Based	Clustering	Deep Learning	Ensemble	Neural Network	Regularization	Rule System	Regression	Binary Classification	Multi-class Classification	Clustering	Accuracy	True Positive Rate	False Positive Rate	True Negative Rate	False Negative Rate	Precision	F-measure	Time
[8]				x							x													x										
[9]					x						x													x			x	x				x		
[10]		x							x			x																						
[11]		x								x			x	x		x								x			x	x				x	x	
[12]		x				x			x	x																								
[13]								x	x									x						x	x			x	x				x	
[14]		x							x				x		x						x		x					x	x					
[3]																																		
[15]																																		
[2]																																		
[1]																																		
[16]		x								x									x	x			x	x			x		x		x			x
[17]		x							x								x									x								
[18]		x							x															x				x				x		x
[19]		x							x												x			x			x			x		x		
[20]						x				x					x	x			x				x	x			x							
[21]	x														x								x	x			x						x	
[22]		x							x				x						x	x			x	x				x				x	x	
[23]		x							x										x	x			x	x			x	x	x					
[24]		x								x			x	x	x	x			x				x	x			x	x				x	x	
[27]						x			x			x												x										
[28]		x							x		x													x				x				x		
[30]	x	x											x	x		x			x	x				x				x	x			x	x	x
[31]						x			x	x														x			x							
[32]						x				x														x				x				x	x	x
[33]		x							x	x									x	x			x	x				x	x					
C	**2**	**14**	**0**	**1**	**1**	**5**	**0**	**1**	**13**	**8**	**3**	**2**	**5**	**3**	**4**	**4**	**1**	**1**	**7**	**5**	**2**	**0**	**8**	**18**	**1**	**1**	**9**	**12**	**6**	**1**	**1**	**9**	**7**	**4**

Results and Discussion

Recent studies predominantly focus on ML techniques for ransomware detection, leveraging regression algorithms to predict behavioral patterns. Regression algorithms yield accurate binary classifications, underpinned by metrics such as accuracy and true positive rate.

Our Proposed Technique

To enhance ransomware detection efficacy, we propose a hybrid algorithm integrating regression and rule-based approaches, leveraging insights from both static and dynamic analyses. This holistic approach aims to comprehensively understand ransomware infection and attack patterns, culminating in a robust detection model.

Conclusion

Our proposed solution encompasses developing a ransomware attack model through a synthesis of static and dynamic analyses, augmented by a hybrid algorithm. This multifaceted approach ensures a nuanced understanding of ransomware threats and facilitates proactive detection, underscoring the novelty and efficacy of our proposed methodology.