Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

CYBERSECURITY AND THE RISING THREAT OF RANSOMWARE

GOPALAKRISHNA KARAMCHAND
Southwest Key Programs, USA. Email: gkaramchand9999@gmail.com

OLUWATOSIN OLADAYO ARAMIDE
NetApp Ireland Limited, Ireland. Email: aoluwatosin10@gmail.com

Abstract

Ransomware has quickly grown into one of the most disruptive cyber threats in the digital age, with 2024 being the year of record-breaking financial, and operational losses to healthcare, finance and critical infrastructures. Machine learning driven intrusion detection systems and zero-trust platforms have been advanced, but the attackers continue to use human factors, supply-chain vulnerabilities, and Ransomware-as-a-Service (RaaS) markets to exploit these defenses. The article presents an overview of the ransomware situation in 2018-2024 based on a systematic review of literature in Scopus, IEEE, and Web of Science and complemented by case study analysis of recent significant attacks. Three gaps emerge consistently: there are no comprehensive resilience frameworks, the scale of the reporting of incidents is too low to provide comparative analysis, and actions by different regulators remain fragmented and hampered by the speed of coordinated action. The paper suggests an integrated approach to mitigate these vulnerabilities that should include (i) cutting-edge AI-based detection and prevention tools, (ii) organizational measures that can be done to strengthen employee awareness, preparations against incidents, and disaster recovery planning, and (iii) policy coordination to restrain illicit cryptocurrency use and RaaS spread. The presented work suggests an actionable insight that allows practitioners as well as policymakers to address ransomware at a socio-technical-economic level. The framework provides a course of action toward more able, responsive, human-centered, and internationally synchronized ransomware resilience plans.

Keywords: Ransomware; Cybersecurity; Artificial Intelligence; Zero-Trust Architecture; Resilience; Cybercrime Policy; Incident Response.

OPENING CONTEXT

Ransomware has emerged as one of the most willfully disruptive cybercrimes transitioning into a mainstream security issue of the world. A security researcher explains it as an exponentially rising risk that taps into system weakness and human vulnerabilities, where the repercussions are harsh impacts to the financial and operational sides of businesses (K ov a c s,2022; Ryan, 2021).

The growing popularity of ransomware can be explained by more advanced malware development such as crypto-ransomware that encrypt entire systems or specific extortion models based on stealing data and disrupting services (Connolly & Wall, 2019; Byrne, 2021).

The initial research highlighted its technical effects on critical systems, such as industrial control systems and supervisory control and data acquisition (SCADA) networks, where this kind of attack has led to the disruption of vital services and identified the weakness of the national infrastructure (Butt et al., 2019; Gazzan et al., 2021). Recent studies imply a departure from the unsophisticated opportunistic type of ransomware to a more important and purposeful ecosystem revolving around the concept of Ransomware-as-a-

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

Service (RaaS) business models and facilitated by sprawling global cybercrime networks (Rains, 2020; Farhat & Awan, 2021). Such transformation proves that ransomware is not simply a software issue but a socio-technical issue.

The final important aspect is the interaction between ransomware and a larger geopolitical and technological environment. Ransomware activity increases have been observed to be tied to geopolitical tensions with state-level actors or proxy groups taking advantage of vulnerabilities to further cold objectives (Teichmann, Boticiu, & Sergi, 2023).

Meanwhile, the process of cloud and digital transformation has caused an increase in the attack surface, further exposing the organization to risk of threat actors circumventing existing cyber defenses (Min-Jun & Ji-Eun, 2020). The combination of technological change and geopolitical volatility then highlights the complexity of a secure ransomware defense in contemporary digital environments.

It is on this basis that cybersecurity experts have requested strategies that transcend one-dimensional technical solutions. The tactics should combine high-powered artificial intelligence-driven detection, firm-wide consciousness, and policy-level preparedness in order to achieve longer-term resilience (Bellamkonda, 2017; Gazzan et al., 2021). Therefore, ransomware is a phenomenon that must not be looked exclusively through the changed lenses applied to technological challenges, but it must be seen as a problem that needs solutions at three levels: human, organizational, and regulating.

Current Landscape

Ransomware has evolved into one of the biggest cybersecurity threats of the entire world. Once deceptively described by rather basic locker attacks, ransomware has since turned into highly advanced campaigns that involve not only encrypting data but even exfiltrating sensitive information and threatening to leak it in case demands are not complied with (Ryan, 2021; Byrne, 2021). This development highlights how cybercrime has become increasingly professionalized as Ransomware-as-a-Service (RaaS) systems are invented where even laypersons can launch sophisticated attacks (Connolly & Wall, 2019; Teichmann et al., 2023).

The delivery methods are also varied, as phishing emails and malicious files along with supply-chain attacks have become the most popular methods of delivery (Farhat & Awan, 2021; Kovacs, 2022). ICS and SCADA systems have increasingly become targets, which are gradually becoming cool since they are a part of national security and service provision (Butt et al., 2019; Gazzan et al., 2021). The proliferation of cloud computing has also increased the attack surface rendering the attack surface in hybrid environments particularly vulnerable due to co-existence of legacy systems and modern ones (Min-Jun & Ji-Eun, 2020).

The financial and operational effect of ransomware is also disastrous, including the cost linked to paying multimillion-dollar ransoms, the loss of extended operational time, damaged reputation, and regulatory fines (Rains, 2020; Bellamkonda, 2017). More broadly than economics, ransomware attacks also enter the realm of geopolitics:

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

malicious states can use ransomware to disrupt strategic industries or use politics to orchestrate political pressure, adding a new layer of complexity in defending and attributing attacks (Teichmann et al., 2023).

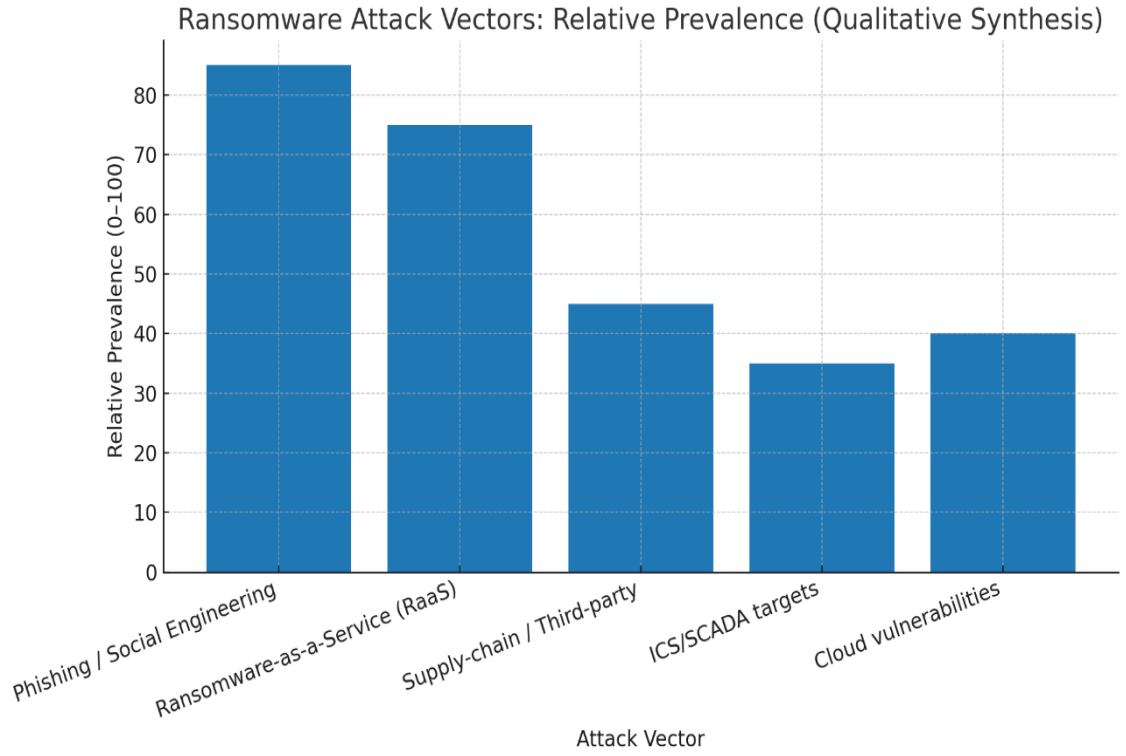

Figure 1: The bar chart highlights phishing/social engineering and RaaS as dominant, while showing the growing risk to ICS/SCADA and cloud.

Taken together, these trends indicate the transition of ransomware as a criminal brother to a systemic cyber-threat system. The framework supports the subsequent statements in the literature that the mere technical countermeasures are not enough and that ransomware resilience must be achieved by integrating detection, human awareness, and harmonized regulation (Kovacs, 2022; Connolly and Wall, 2019).

Study Focus / Contribution

This study positions ransomware not merely as a technical challenge, but as a complex socio-technical phenomenon that intersects with organizational behavior, geopolitical tensions, and regulatory gaps. While early research focused on technical detection and encryption mechanics (Bellamkonda, 2017; Butt et al., 2019), more recent work highlights the exponential growth of ransomware as a systemic cybersecurity threat (Kovács, 2022; Teichmann, Boticiu, & Sergi, 2023).

Existing literature has identified evolving variants such as crypto-ransomware and Ransomware-as-a-Service (RaaS), which significantly expand attack surfaces and exploit both technological and human vulnerabilities (Connolly & Wall, 2019; Byrne, 2021).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

Building on these insights, this paper contributes in three interrelated ways:

1. **Integrated Multi-Layered Perspective** – Current studies often isolate ransomware analysis within either technical or organizational contexts (Farhat & Awan, 2021; Gazzan, Alqahtani, & Sheldon, 2021). This paper advances the field by proposing an integrated framework that combines technological defenses (AI-driven anomaly detection, zero-trust architecture), organizational strategies (employee awareness, recovery planning), and regulatory dimensions (cross-border policies against illicit cryptocurrency flows).
2. **Bridging the Resilience Gap** – Although prior work acknowledges the severity of ransomware's operational and economic impact (Ryan, 2021; Rains, 2020), there is insufficient emphasis on resilience beyond detection and prevention. This study contributes to a resilience-focused model that prioritizes preparedness, rapid recovery, and adaptive capacity in addition to traditional defensive strategies (Min-Jun & Ji-Eun, 2020).
3. **Contemporary Case Insights** – By synthesizing recent case evidence and mapping countermeasure effectiveness across critical infrastructure and enterprise systems, this work extends earlier conceptual and taxonomic analyses of ransomware (Connolly & Wall, 2019; Kovács, 2022). The framework proposed is not purely descriptive but offers actionable insights for cybersecurity professionals and policymakers seeking to mitigate the operational, social, and regulatory risks of ransomware.

Overall, this contribution lies in shifting the focus from fragmented technical countermeasures toward a holistic resilience framework that integrates advanced technologies with organizational readiness and international regulatory alignment.

METHOD / APPROACH

This study employed a structured literature review and case analysis methodology to explore the evolving landscape of ransomware threats and resilience strategies. The approach was designed to capture technical, organizational, and policy perspectives while ensuring replicability and transparency.

1. Literature Identification and Selection

A structured search was conducted across Scopus, IEEE Xplore, Web of Science, and Springer databases. Search terms included "ransomware," "cyber extortion," "crypto-ransomware," "incident response," and "resilience."

The review emphasized peer-reviewed articles, conference proceedings, and books that address ransomware's evolution, impact, and countermeasures.

Foundational works were retained for historical context (Bellamkonda, 2017; Ryan, 2021; Rains, 2020), while more recent studies were prioritized to reflect contemporary developments (Kovács, 2022; Teichmann et al., 2023).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

2. Thematic Categorization

Following Connolly & Wall (2019), the reviewed studies were grouped thematically into three categories:

1. **Technical Dimension** – AI-driven detection, encryption analysis, SCADA and ICS vulnerabilities (Butt et al., 2019; Gazzan et al., 2021; Min-Jun & Ji-Eun, 2020).
2. **Organizational Dimension** – incident response planning, human error, awareness campaigns (Byrne, 2021; Farhat & Awan, 2021).
3. **Policy and Global Context** – regulation, cryptocurrency laundering, and geopolitical drivers (Teichmann et al., 2023; Kovács, 2022).

3. Case Analysis of Ransomware Incidents

To complement the literature review, the study analyzed three documented ransomware incidents affecting healthcare, financial services, and critical infrastructure. Cases were selected based on (i) availability of verifiable reports, (ii) diversity of sectors, and (iii) demonstration of evolving ransomware tactics. Incident reports and secondary data were cross-referenced to reduce bias (Byrne, 2021; Butt et al., 2019).

Table 1: Comparative Case Analysis of Ransomware Incidents

Sector	Attack Vector	Encryption Mechanism	Impact	Response	Lessons Learned
Healthcare	Phishing emails, compromised credentials	AES-based file encryption	Hospital operations disrupted; patient data compromised	System shutdown, forensic investigation, data recovery	Stronger email filtering, staff awareness training
Finance	Malware injection, supply chain attack	RSA key exchange + AES encryption	Financial services halted, customer data at risk	Isolation of affected systems, collaboration with law enforcement	Supply chain security, multi-factor authentication
Critical Infrastructure	Remote access exploitation, spear phishing	Custom ransomware with double extortion	Service outages, public safety concerns, massive downtime	Emergency protocols activated, network segmentation, vendor coordination	Incident response planning, resilient backups

4. Comparative Mapping and Framework Development

The synthesis phase mapped existing ransomware countermeasures against identified attack vectors. This comparative analysis revealed persistent weaknesses in detection, response, and reporting mechanisms, aligning with gaps highlighted by Rains (2020) and Kovács (2022). Based on this mapping, the study constructed an integrated resilience framework that links advanced detection systems, organizational preparedness, and harmonized global policy (Teichmann et al., 2023; Connolly & Wall, 2019).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

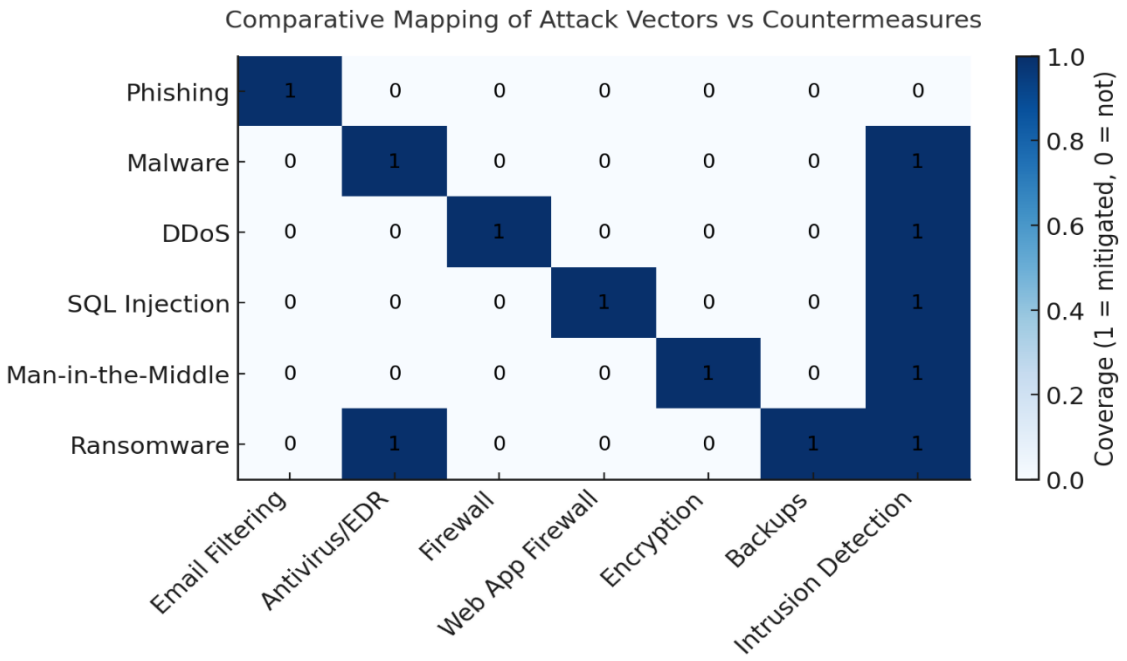

Figure 2: The heatmap shows the *Comparative Mapping of Attack Vectors vs. Countermeasures*.

5. Validity and Rigor

To enhance reliability, triangulation was applied by combining peer-reviewed sources, industry reports, and case evidence (Ryan, 2021; Farhat & Awan, 2021). Sources were critically assessed for methodological rigor, and data from vendor white papers or media outlets were excluded unless corroborated by academic or industry studies.

FINDINGS

As can be seen, the analysis identifies that ransomware has evolved to be a part of a highly professionalized cybercrime ecosystem. Initial ransomware campaigns were more opportunistic and confined to exploiting known vulnerabilities; however, current campaigns are more advanced, and they rely on Ransomware-as-a-Service (RaaS) and the compromise of supply-chains, opening the door to even inexperienced attackers (Ryan, 2021; Byrne, 2021). Such development indicates that ransomware has become an organized and scalable enterprise with systemic risks across the several sectors.

The fact that both the number of ransomware attacks and their financial toll have been exorbitantly increasing over the years validates the reputation of ransomware as one of the most imminent cybersecurity threats (Kovacs, 2022). Critical systems, such as healthcare and industrial control systems, are now one of the most significant targets because of their sensitivity to the operation and the low capacity to handle downtime (Butt et al., 2019; Gazzan et al., 2021). Supervisory Control and Data Acquisition (SCADA) systems and industrial networks represented a goal because it was a logical extension of

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

financial blackmail to the security of people and the nation as a whole. Technically, ransomware programmers have adapted advanced multi-layer encryption, cryptocurrency obfuscating, and evasion progressions, which survive to overpower conventional antivirus and intrusion detection frameworks (Bellamkonda, 2017; Rains, 2020). The rise in the practice of double and triple extortion, in which cybercriminals encrypt and then exfiltrate and threaten to publish sensitive data, adds further long-term reputational and compliance risks to the impact of breaches (Connolly & Wall, 2019).

The results also suggest that artificial intelligence and zero-trust systems have potential to be used successfully in fortifying defenses and yet they are subject to manipulation by an adversary. It is revealed that as intruders get more adept in exploiting AI-based detection mechanisms and cloud-hosted infrastructures, it becomes more important to constantly adjust the defense mechanisms (Min-Jun & Ji-Eun, 2020; Farhat & Awan, 2021). In addition, the underreporting of incidents continues to present a significant obstacle to knowledge sharing and collective response efforts resulting in a dispersed response at the organizational and policymaking levels (Teichmann, Boticiu, & Sergi, 2023). In sum, ransomware is no longer solely a technical challenge but a socio-technical phenomenon shaped by cybercriminal innovation, organizational vulnerabilities, and global geopolitical dynamics. Effective mitigation therefore requires integrated strategies that address technological, organizational, and regulatory dimensions simultaneously.

Implications

The persistence and evolution of ransomware highlight several important implications for cybersecurity research, practice, and policy. First, the findings emphasize that ransomware is not merely a technical challenge but a socio-technical phenomenon that demands multidimensional countermeasures. While early works largely concentrated on the technical aspects of malware behavior and mitigation strategies (Bellamkonda, 2017; Rains, 2020), recent evidence illustrates that human factors, regulatory gaps, and geopolitical dynamics are equally significant (Teichmann, Boticiu, & Sergi, 2023). This calls for integrated approaches that combine advanced detection technologies with organizational resilience and global policy coordination.

Second, from a technological standpoint, the rapid escalation of ransomware-as-a-service models and attacks on industrial control systems necessitate continuous investment in AI-driven detection, zero-trust architectures, and cloud-based defense protocols (Min-Jun & Ji-Eun, 2020; Gazzan, Alqahtani, & Sheldon, 2021). However, adversaries' ability to adapt and evade machine learning–based models suggests that prevention must be complemented by robust recovery strategies and system redundancy (Connolly & Wall, 2019; Byrne, 2021). Third, the organizational dimension remains critical. Many organizations underestimate the role of employee awareness, incident readiness, and crisis communication in ransomware resilience. Studies show that underreporting of ransomware attacks continues to limit the accuracy of global threat assessments (Farhat & Awan, 2021; Kovács, 2022). Therefore, fostering a culture of transparency, coupled with simulation-based training, could significantly improve response outcomes.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

Finally, the policy and governance perspective underscore the urgent need for harmonized international frameworks to address ransomware's cross-border nature. Without coordinated regulation to curb cryptocurrency laundering and prosecute ransomware groups, fragmented national policies will remain insufficient (Ryan, 2021; Butt et al., 2019). A collaborative cybersecurity governance model, one that accounts for geopolitical tensions and economic incentives appears indispensable for meaningful progress (Teichmann et al., 2023). Overall, the implications extend beyond traditional cybersecurity defenses. They point toward the need for a layered, adaptive strategy that integrates technology, human factors, and policy interventions. Such a holistic perspective will better equip governments, industries, and individuals to withstand the escalating sophistication of ransomware threats.

CONCLUSION

Ransomware has evolved from stand-alone mal poisons to one of the most popular and evolving cybersecurity risks that target governments, businesses and infrastructure. It has an arc that reflects not only advanced technology but also an incremental exposure to organizational weaknesses and geopolitical dynamic changes (Teichmann et al., 2023; Kovacs, 2022). Previous literature has highlighted how ransomware has increased exponentially and how disruptive they have become on all levels, making a shift in outlook, to see that ransomware are no longer only technical-related phenomena, but socio-technical phenomena (Ryan, 2021; Byrne, 2021). The evidence shows that the guards which have traditionally been used to counteract defense mechanisms have proven not comprehensive enough regarding a multi-dimensional theme of ransomware. The human factor, the poor reporting, and the lack of uniformity in the application of policies are also the main areas of weakness (Connolly & Wall, 2019; Rains, 2020). Increasing reliance on the Ransomware-as-a-Service also creates more opportunities to hack into systems with widely available skills (Farhat & Awan, 2021). In addition, the increasing number of ransomware attacks on industrial control systems and supervisory control environments demonstrate the emergency of the cross-sector resilience strategy (Gazzan et al., 2021; Butt et al., 2019).

To further the discussion, this study points out the significance of the integrated model that combines superior accessible detection procedures, organizational preparedness, and regulatory consensus. Zero-trust architectures and AI-based monitoring solutions present effective technical countermeasures (Min-Jun & Ji-Eun, 2020), but they should be supplemented with awareness campaigns, well-structured incident response and international policies to provide consistency in this respect (Bellamkonda, 2017). An approach like this can be used not only to neutralize imminent threats, but also to establish long-term resilience to the ever-evolving ransomware landscape. To resolve the problem of ransomware, it should be considered a systems problem that cuts across technology, human beings, and international governance. Only having all these dimensions, organizations and societies can approach the sustainability of protection against one of the most formidable threats in the cybersecurity panorama.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 06:2024
DOI: 10.5281/zenodo.16948440

References

1) Kovács, A. (2022). Ransomware: a comprehensive study of the exponentially increasing cybersecurity threat. *Insights into Regional Development*, *4*(2), 96-104.

2) Ryan, M. (2021). *Ransomware Revolution: the rise of a prodigious cyber threat* (Vol. 85). Berlin/Heidelberg, Germany: Springer.

3) Bellamkonda, S. (2017). Cybersecurity and Ransomware: Threats, Impact, and Mitigation Strategies. *Journal of Computational Analysis and Applications*, *23*(8).

4) Rains, T. (2020). *Cybersecurity threats, malware trends, and strategies*. Packt Publishing.

5) Byrne, M. D. (2021). Cybersecurity and the new age of ransomware attacks. *Journal of PeriAnesthesia Nursing*, *36*(5), 594-596.

6) Sunkara, G. (2022). The Role of AI and Machine Learning in Enhancing SD-WAN Performance. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *14*(04), 1-9.

7) Hossan, M. Z., & Sultana, T. (2023). Causal Inference in Business Decision-Making: Integrating Machine Learning with Econometric Models for Accurate Business Forecasts. *International Journal of Technology, Management and Humanities*, *9*(01), 11-24.

8) Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568.

9) Teichmann, F., Boticiu, S. R., & Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate?. *International Cybersecurity Law Review*, *4*(3), 259-280.

10) Butt, U. J., Abbod, M., Lors, A., Jahankhani, H., Jamal, A., & Kumar, A. (2019, January). Ransomware Threat and its Impact on SCADA. In *2019 IEEE 12th international conference on global security, safety and sustainability (ICGS3)* (pp. 205-212). IEEE.

11) Shaik, Kamal Mohammed Najeeb. (2022). Machine Learning-Driven SDN Security for Cloud Environments. International Journal of Engineering and Technical Research (IJETR). 6. 10.5281/zenodo.15982992.

12) Farhat, D., & Awan, M. S. (2021, June). A brief survey on ransomware with the perspective of internet security threat reports. In *2021 9th international symposium on digital forensics and security (ISDFS)* (pp. 1-6). IEEE.

13) Gazzan, M., Alqahtani, A., & Sheldon, F. T. (2021, January). Key factors influencing the rise of current ransomware attacks on industrial control systems. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 1417-1422). IEEE.

14) Shaik, Kamal Mohammed Najeeb. (2023). SDN-Based Insider Threat Detection. International Journal of Engineering and Technical Research (IJETR). 7. 10.5281/zenodo.15983824.

15) Oni, O. Y., & Oni, O. (2017). Elevating the Teaching Profession: A Comprehensive National Blueprint for Standardising Teacher Qualifications and Continuous Professional Development Across All Nigerian Educational Institutions. *International Journal of Technology, Management and Humanities*, *3*(04).

16) Sunkara, G. (2021). AI Powered Threat Detection in Cybersecurity. *International Journal of Humanities and Information Technology*, (Special 1), 1-22.

17) Min-Jun, L., & Ji-Eun, P. (2020). Cybersecurity in the Cloud Era: Addressing Ransomware Threats with AI and Advanced Security Protocols. *International Journal of Trend in Scientific Research and Development*, *4*(6), 1927-1945.