Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

AN IN-DEPTH ANALYSIS OF RANSOMWARE ATTACK TREND: EMERGING PATTERNS AND EFFECTIVE COUNTER MEASURES FOR CYBER SECURITY

[1]Samra Aslam, [2]Dr. Abdul Rauf, [3]Prof. Dr, Majid Hussain
[1]MS Scholar, Department of Computer Science, Faculty of Information Technology, The University of Faisalabad.
[2]Associate Professor, Department of Computer Science, Faculty of Information Technology, The University of Faisalabad.
[3]Dean, Faculty of Computer Science & Information Technology, The University of Faisalabad.
[1]samraaslam4549@gmail.com, [2]abdulrauf2000.pk@gmail.com, [3]majidhussain1976@gmail.com

DOI:- https://doi.org/10.5281/zenodo.20525169

Keywords
Ransomware, Cybersecurity, Effective countermeasures, Attack Lifecycle, Tactics techniques procedures (TTPs), Threat intelligence

Article History
Received: 06 May, 2026
Accepted: 25 May, 2026
Published: 30 May, 2026

Corresponding Author: *

Abstract
Ransomware has become one of the most costly global cyber threats to businesses, infrastructure, and individuals. The rapid evolution of ransomware has become more dangerous with the introduction of Ransomware-as-a-Service. Even with advancements in security, most organizations are left vulnerable to cyber attacks due to lack of knowledge regarding evolving trends, inadequate and insufficient defensive measures, and poorly integrated defense mechanisms. This research examines the lifecycle, trends, and techniques of contemporary ransomware and analyzes both defensive and response mechanisms. This study utilizes a mixed method approach whereby the public reporting of ransomware incidents is quantitatively analyzed, and the remaining portions of the analysis are qualitatively aided by the expertise of the security professionals. The investigation focuses on the range, sophistication, and aggressiveness of the techniques employed by ransomware actors during the phases of initial access, lateral movement, the theft and encryption of data, and demand for payment. This study also seeks to understand the range, sophistication, and aggressiveness of countermeasures to ransomware attacks in addition to identifying the most critical barriers concerning the preparedness of organizations. The most frequently identified barriers were unpatched systems, inadequate access controls, susceptibility to phishing, and a weak incidents response. PhD candidate posits a deterrence and response model to ransomware that combines threat intelligence and tiered ransom assessments integrated with behavioral analysis of ransomware and methodical gaps identified through a critical and cooperative threat analysis. This study combines technical, malware and ransomware, and organizational defense analysis. Additionally, this study offers new insights into cybersecurity and ransomware policies and provides additional protective measures to better strengthen organizations against ransomware attacks.

Introduction

Ransomware represents one of the most devastating forms of cyber extortion that causes considerable damage to the global economy and has emerged as a greater threat to people and businesses. In cyber extortion, attackers encrypt sensitive data and demand a ransom in return for the decryption key, typically in the form of a cryptocurrency. Supply chain integrity, reputation, and ciphertext-sensitive information are affected by this form of attack. The already vulnerable and critical healthcare sector may witness loss of life as a direct consequence of a ransomware attack. (Scaife et al., 2016; Kshetri, 2021)

The improvement of ransomware can be credited to organized criminal cartels that enhanced their systems, including "double extortion," but mostly the development of Ransomware-as-a-Service (RaaS). This has caused a rise in ransomware attacks. (Kharraz et al., 2015) Ransomware extorts the financial resources of a cartel and forces businesses to adapt newer and more anticipatory and intelligence-based cyber defense systems. This implies that businesses may no longer depend on older traditional systems of safeguarding, like firewalls and anti-virus systems. The focus of my research is to understand the entire ransomware extortion process (from infiltrating the victim organization and its systems, to the actual monetization of the attack) and analyze the existing countermeasure tools and defense systems set by the victim organizations. My research also aims to design a model that is flexible to the defense systems used by organizations to counter malware and allow for threat identification in advance and minimize attack-related costs and impact as much as possible.

Ransomware attacks became more advanced in the 2010s with the introduction of Bitcoin and the first attacks like CryptoLocker, as well as improvements in public key cryptography (Chen et al., 2021). This marked the emergence of ransomware as a mainstream cyber and public security threat.

Take for example the attack on the information systems of 150 countries caused by the EternalBlue security vulnerability in the 2017 WannaCry case (Mohurle & Patil, 2017). After the WannaCry case, the NotPetya case exploited the same vulnerability and attacked the information systems of Ukraine. This case shows that ransomware can be even more dangerous (Nakashima, 2017).

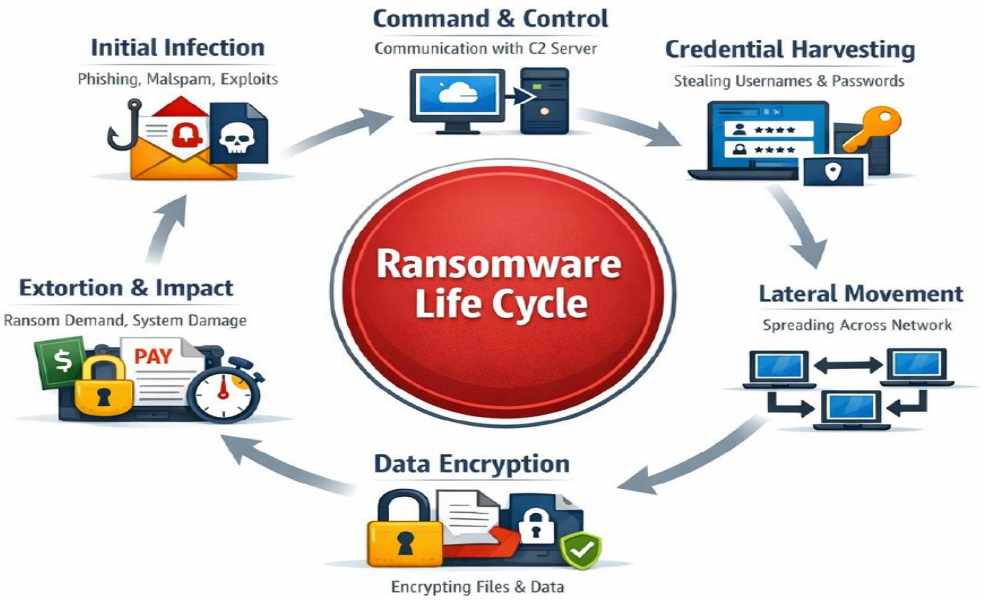
The evolution of ransomware has made it harder for businesses to protect themselves. The "Big Game Hunting" scheme is executed by sophisticated gangs of criminals who target organizations with critical data (Covie, 2021). Another trend called "double extortion" adds complexity to protective schemes. In this scheme, the attackers exfiltrate sensitive data and extort their target with the threat of data release (Zimba & Wang, 2019). In addition, the Ransomware as a Service (RaaS) model has created a more equitable environment in the world of cybercrime. While systems such as REvil and Darkside execute highly sophisticated cyber attacks, they can be easily replicated by criminal groups with little to no technical skills (Europol, 2020).

Ransomware crime is extensive and predicted losses will reach $265 billion by 2031, which includes the ransom amount, losses from business disruption, and expenses to recover (Cybersecurity Ventures, 2021). Adding to the evolution of ransomware, the modern-day coronavirus pandemic has disrupted the defenses and increased the global wave of criminal ransomware.

Many companies shifting to an online focus has opened up new threats for security vulnerabilities such as unprotected VPNs and additional ways to criminally access systems through RDP (Chen et al., 2021). Outdated systems and inadequate security training, as well as poor password policies and a lack of multi-factor authentication, leave organizations open to attack, particularly in the wake of a rushed acknowledgment of ransomware.

Life - Cycle of Ransomware Attacks:

Ransomware has six phases of the life cycle: initial infection, command and control establishment, credential harvesting, lateral movement, data encryption, and extortion (Anderson & Moore, 2021). This life cycle, combined with trends of attacks, needs to be understood to improve defense strategies against the eminent threat.



Research Objectives

This research aims to achieve the following objectives:

- Studying tendencies and procedures of novel ransomware strikes.
- Recognizing repetitive offender procedures with MITRE ATT&CK.
- Evaluating gaps in organizations ransomware strikes target.
- Evaluating adequacy of existing cybersecurity measures.
- Designing an enhanced ransomware defense framework to increase organizational resilience against attack.

Novelty of the Study

This review, in contrast to other studies on ransomware, contains a quantitative attack pattern analysis, a behavioral analysis based on the MITRE ATT&CK framework, and a practitioner perspective in the cyber resilience framework. This research considers the readiness of an organization and the constant adjustments an organization makes in response to various threats. This research incorporates the contemporary knowledge of ransomware and alleviates some challenges practitioners encounter. With the knowledge of contemporary ransomware, this framework can alleviate practitioner threats.

Research Methodology

This study uses a mixed-method framework to examine the trends in ransomware attacks and analyze possible defenses. For the quantitative dimension, ransomware related incidents published between 2020 and 2025 will be documented. These incidents will be aligned with the MITRE ATT&CK framework to isolate Tactics, Techniques, and Procedures used in the attacks. Patterns and vulnerabilities will be examined using statistical methods. In the meantime, to gain a deeper understanding of the organizational defenses against ransomware, semi-structured interviews will be conducted with cybersecurity incident responders and threat analysts as well as Chief Information Security Officers (CISOs). The qualitative data helps position human and organizational factors in the context of preparedness. The findings from the qualitative and quantitative analyses will be combined to identify trends related to ransomware, discourage threat actors, and present viable cyber defensive countermeasures. The answer will speak to the mixed-method framework used with a focus on the quantitative dimension. The qualitative dimension will focus on threats posed by ransomware.

Result & Discussion

Qualitative Findings

The Landscape of Modern Ransomware Attacks

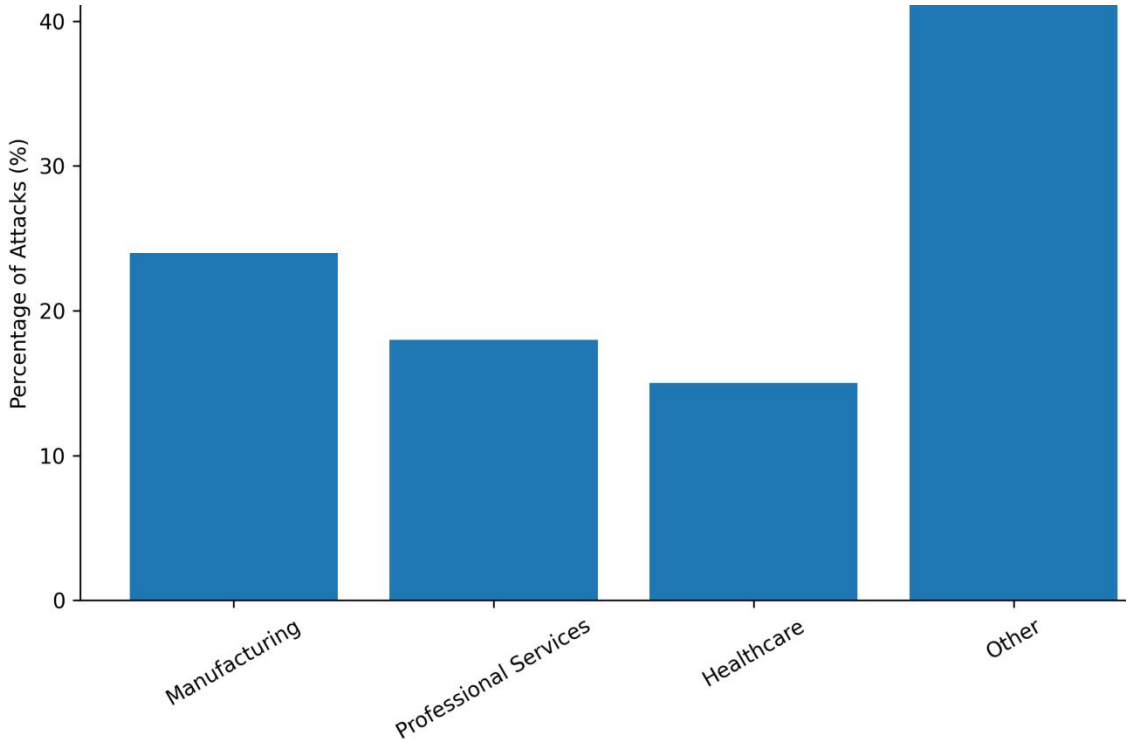
The quantitative analysis data set contains 350 public reports of ransomware attacks that occurred between January 2020 and September 2025. Examining these incidents sheds light on some of the most important factors in these scenarios including adversary actions, which were plotted against the MITRE ATT&CK framework. The

results describe the contemporary threat landscape in an objective, evidence-based manner.

Threat Actor Analysis and Victimology

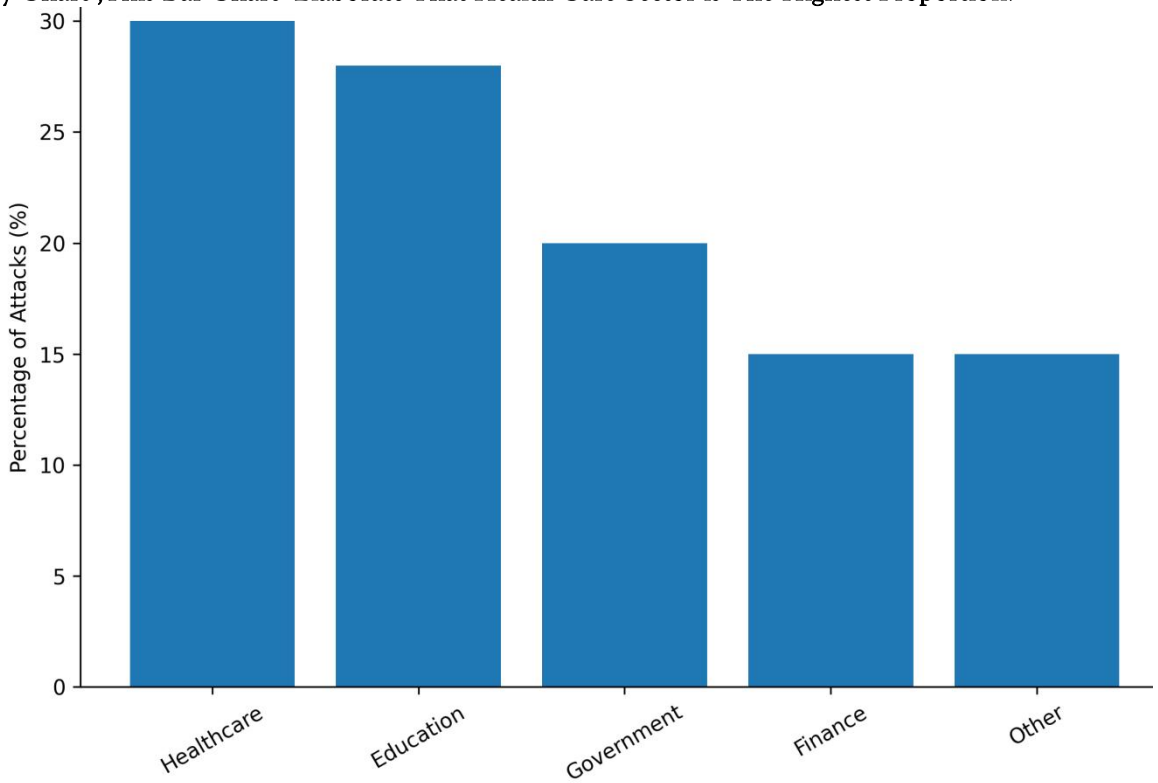
The most prevalent victim when grouped by industry was the Manufacturing industry with 24% of the incidents that occurred in the data set. Professional, Scientific and Technical Services (18%), and Healthcare (15%) came right behind. The rationale behind targeting these sectors is that they will have low tolerance of downtime, complicated and under-invested IT infrastructure and due to the valuable nature of data. The North American organizations were most attacked (55 percent) and Europe (30 percent) created high-value targets and threat reporting concentration in the areas. The threat actors involved in the market were analyzed and it was highly concentrated. The number of attacks attributed to three RaaS groups (LockBit (28%), Conti (17%), and BlackCat/ALPHV (11%)) in the dataset exceeded half of the total number of attacks. It points to the prevalence of the brand in the RaaS ecosystem of which there are few and highly professional and effective sets of people acquiring many of the talented affiliates. It was also proven that there existed a certain tendency of splintering and rebranding in which methods and even infrastructural support of the failed Conti group was found in the subsequent operations which strengthened the notion that these criminal syndicates were fluid and resilient. The figure-2 illustrate that healthcare sector is the highest proportion at slightly above 30% and then education sector with slightly less at just under 30% both are under "High Risk" category. The government and finance sectors are classified as the "Moderate Category", with a percentage of about 20 and 15 of attacks respectively. The other category is the lowest share, about 15, and is named "Low Risk". According to data, the most susceptible to ransomware attacks are the healthcare and education sectors. (CISA, 2022).

Sector Wise Distribution of Ransomware Attacks



This Bar chart show the total ransomware damaged of each sector. The sector with the most damage is the other sectors, which is above 40%. The second total goes to the Manufacturing sector with 20%. Total damages to the Professional Services and Healthcare sectors are appreciably lower. Some sectors such as Manufacturing and Healthcare are primarily targeted. However, other sectors are also being attacked more.

Risk Category Chart ,This Bar Chart Elaborate That Health Care Sector is The Highest Proportion.



The bar chart indicates that the Healthcare and Education sectors are the most affected by ransomware, with over 30% and almost 30% impact, respectively. Government and Finance sectors are at moderate and low risk, with ransomware threat levels of over 15%. It can be concluded that the most susceptible to ransomware are the Healthcare and Education sectors.

Proactive Ransomware Defense

In the face of growing ransomware threats, this framework employs proactive cybersecurity, automated defenses, behavioral control, and a defense-in-depth approach to formulate an improved defense system.

Threat Intelligence

The formulation of threat intelligence enables the forecasting of future ransomware campaigns. This type of active surveillance will improve an organization's preparedness and real-time threat intelligence by mapping the malicious infrastructure and attacks along with published indicators.

Behavioral Control

With the increasing sophistication of threats, especially with the use of administrative tools to bypass detection, continuous threat monitoring will be implemented to behavioral control systems for the abnormal activities of file encryption, PowerShell execution, privilege escalation, and lateral movement.

Defense-in-Depth: Zero Trust

The detection of sophisticated threats will be dependent upon the application of Zero Trust and the continuous verification security posture, where threats will be contained by multifactor authentication and limiting the least-privilege access.

Backup Isolation and Recovery Planning

Ransomware recovery requires that isolated and immutable backups be maintained. The protection of recovery data from ransomware ensuring backups remain isolated from the primary organizational networks.

Employee Awareness and Security Training

Human error remains the principal cause of most ransomware attacks.

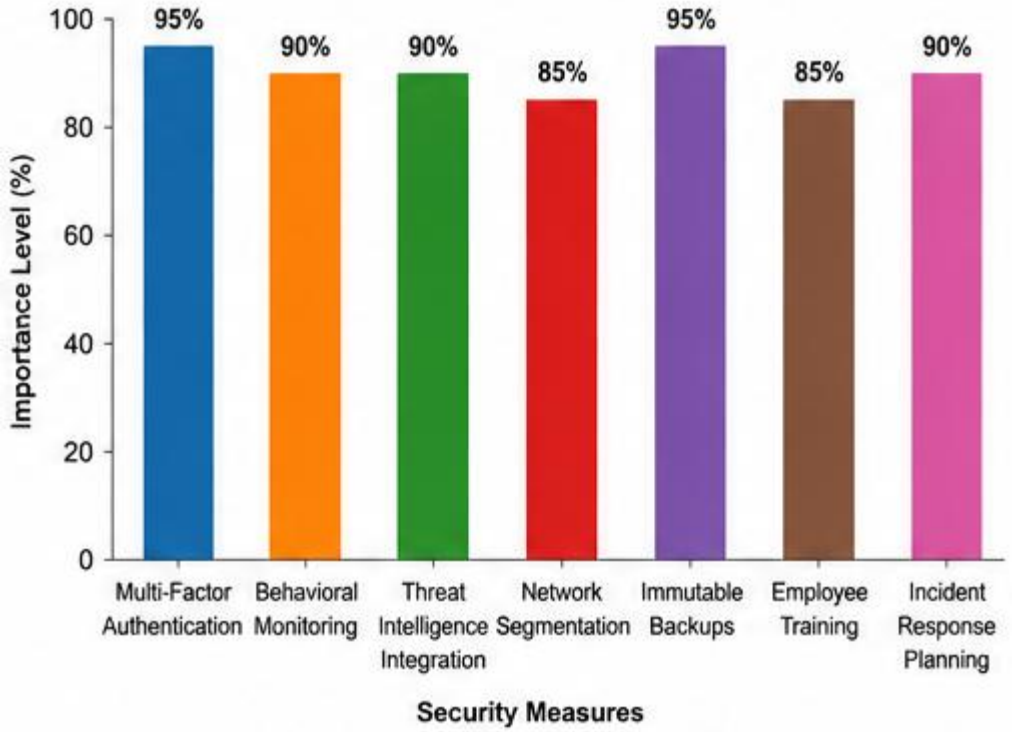
Improving employee security awareness training provides them with the skills to recognize the different attack vectors, including phishing, malicious attachments, and social engineering.

Response to Incidents and Continuous Improvement

Organizations should possess the capability to respond promptly to incidents in order to contain the effects of a ransomware attack and recover from it. Analyzing incidents

to recognize the vulnerable points in security assists in creating a more effective security posture in the future.

Recommended Security Measures



Haley proposed bolstering organizational resilience against ransomware attacks through behavioral monitoring, threat intelligence integration, and employee awareness programs. This image illustrates how each would be implemented.

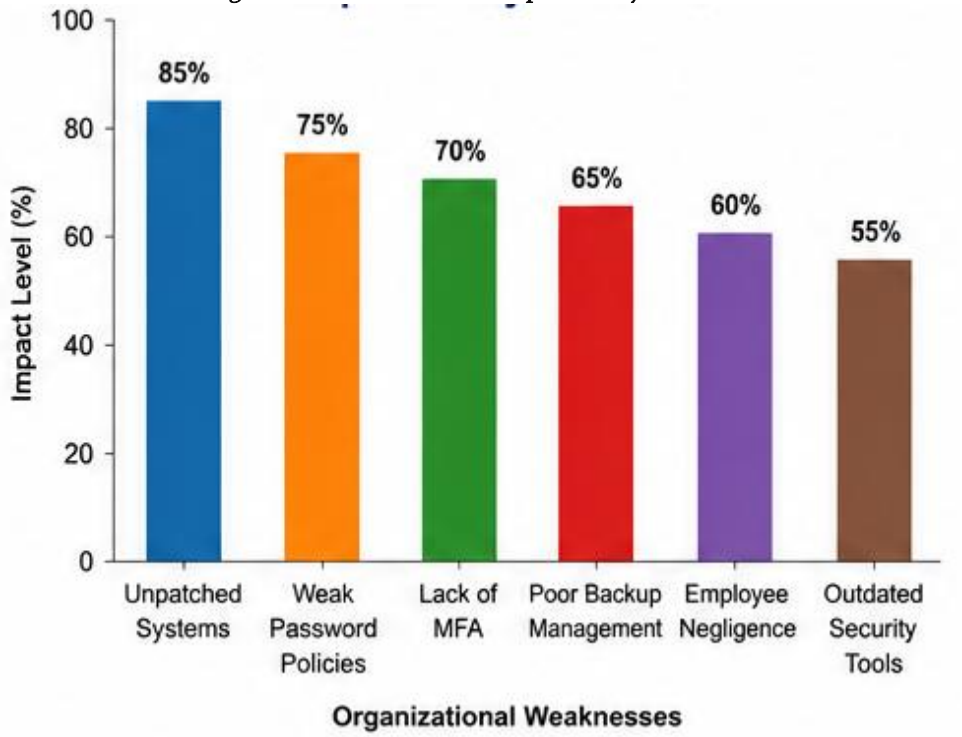
Organizational Weaknesses Exploited by Attackers

The analysis identified several common organizational weaknesses frequently exploited during ransomware attacks. Unpatched systems, weak authentication mechanisms, poor backup management, and limited employee awareness remain major contributors to successful intrusions. Attackers often exploit exposed remote access services and compromised credentials to gain unauthorized access to internal systems.

These findings indicate that ransomware defense requires not only technical security controls but also stronger organizational cybersecurity governance and continuous security awareness-

Initiatives

Organizational Weakness Exploited by Attackers



This **Figure illustrates the major organizational weaknesses exploited during ransomware incidents , including weak authentication controls , unpatched systems , and poor backup manangement practices.**

The Analysis of Adversary Tactics, Procedures and Techniques

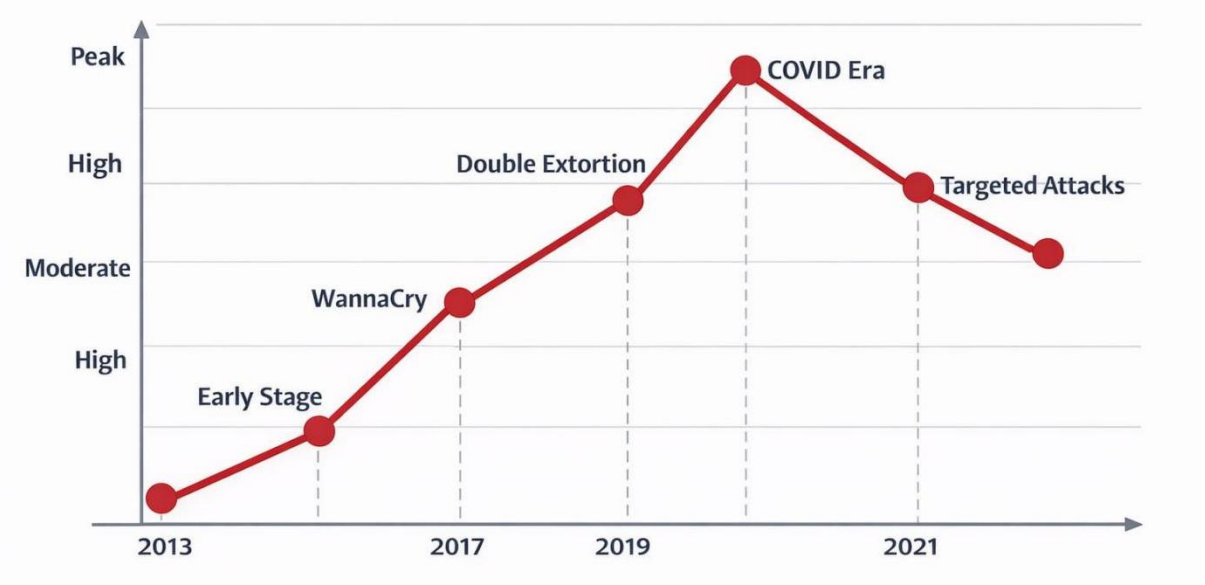
The essence of the quantitative analysis was to map observed TTPs of the 350 incidences to the MITRE ATT&CK framework. It led to a frequency analysis of the most common methods that are used by ransomware perpetrators during the attack lifecycle. Initial Access (TA0001): The statistics indicated that three channels dominated as the leading channels to victim networks. Exploit Public-Facing Application (T1190), which was the most prevalent, was found in 41% of cases where the initial vector could be found. The exploitation of the unpatched vulnerabilities in VPN appliances, remote access software, and web server applications such as Microsoft exchange server were overwhelmingly seen in this category. The second most common method was Valid Accounts (T1078) which were applied in 32% of them. This was mainly through hacked credentials of Remote Desktop Protocol (RDP) or VPNs that are sold by Initial Access Brokers. Finally, the Phishing (T1566) rate was 22 percent of first-time intrusions that is typically a malicious file or link to run a loader payload. Post-Compromise Execution and Persistence: Attackers developed an unreasonable affection with living off the land after gaining access to a network. The most prevalent method used was the use of PowerShell (T1059.001) which was found in 65 percent of all analyzed incidents. This was succeeded by Windows Management Instrumentation (WMI) (T1047) at 48% percent. In the case of Persistence, the most commonly (52) used package was Scheduled Task/Job (T1053) to have their tools persist even after rebooting the system. Credential Access and Discovery: Attackers with a presence will target privileged credentials. The most prevalent method at this stage was OS Credential Dumping (T1003) that happened in 71% of cases. Specifically, it was mentioned that most of these cases involved the use of Mimikatz tool. After gaining credentials, attackers took up much time in discovery. Identification of the network structure was most commonly used and Network Share Discovery (T1135) and querying of Active directory (T1069.002) were almost universal in detailed incident descriptions.

Lateral Movement and Impact

Attackers moved to systems of high value in lateral movement with privileged credentials and network map. The most common lateral movement, namely the RDP (T1021.001) and Windows Admin Shares (T1021.002) was

done using Remote Services. The last stage of impact was extremely similar among incidents. Exfiltration Over C2 Channel (T1041) was seen in 85 percent of instances of double extortion before encryption happened. Service Stop (T1489), to reach files of high importance, and Data Encrypted for Impact (T1486) were the last devastating measures. An important facilitating method on this stage was Impair Defenses (T1562), as in more than three-quarters of the instances, attackers tried to put out EDR and antivirus software. The compilation of this information shows that there is a typical chain of attacks: A human attacker gets his first access by exploiting an unpatched internet facing server. They then run PowerShell so as to run reconnaissance scripts and Mimikatz to dump credentials. They then laterally access the domain controller and backup servers, with domain administrator credentials, disabling security tools on their way. Lastly, they steal confidential information and install the ransomware on the whole network via Group Policy. Figure-3 shows the ransomware attacks growth trend between 2013 and 2024. The trend starts with a low level in 2013, designated as the "Early Stage" and is constantly rising in 2017, with the incident of WannaCry. It is growing in 2019 whereby a new form of extortion known as "Double Extortion" is being implemented at a "High Level". The curve reaches its peak in the COVID Era around 2020, meaning that the most frequent attacks occur. The trend then starts to decrease until 2021, which is related to "Targeted Attacks" and further into 2024 and returns to a "Moderate level". Overall, the statistics indicate that ransomware attacks have increased significantly between the years 2013 and COVID period, followed by a slow increase in the following years.

Growth Trend Of Ransomware Attacks Between (2013 - 2024)



This graph illustrates the increase in ransomware crime from 2013 to 2024. For much of the timeframe, crime was largely unreported/low, but spikes around 2017 due to the exponentially large incidents of WannaCry. The trend worsened and reached its zenith during the COVID crisis, and was characterized by a rapid increase in perpetrators enacting increasingly violent and/or severe criminal exploits and new criminal variants using the "Double Extortion" method. The graph shows declining incidents after 2021, and later depicts victims of preference. "Targeted Attacks" were the new focus of crime after this timeframe.

Qualitative Findings

The Practitioner's Perspectives

Six semi-structured interviews with respondents in cybersecurity (two incident responders, two Chief Information Security Officers, and two threat analysts) were conducted. These interviews led to qualitative analysis and identification of four themes. These themes build upon the quantitative data and describe the human and organizational aspects of vulnerability and defensive measures toward ransomware.

Theme 1: The Unavoidability of Compromise and the Preeminence of Resiliency

A common trend across the participants was the wholesale transformation in strategic thinking where it no longer

applied solely to the preventive model. They all agreed that once human forces initiate the first wave of aggressive attacks, a compromise will almost certainly take place. One resilient shift was rapid detection, response, and recovery. Regarding an incident, one of the interviewees (IR1) indicated that:

My discussion with boards is different now. 5 years ago, it was, How do we stop this? At this point, it is all about getting back up when it occurs at the quickest rate. We have to assume they will get in. The real battle is the dwell time."

It is a motif of the mentality which values the ability to endure and recover following an assault than the more pointless attempt at creating an impractical, impregnable line. The respondents all emphasized the necessity of not only having backups, but also having verified, segmented and immutable backups. One manufacturing industry CISO (CISO1) grumbled:

Everyone says they have backups, the first question I put after a breach is, When was the last time you completed a full restore test?. The silence is usually deafening. The attackers know this; they go for the backups first."

Theme 2: Gap in Implementation of Best Practice

Despite the fact that the knowledge of best practices in cybersecurity were evenly distributed among the respondents, the overwhelming impression was that it is so impossible to apply the best practices in the real world in a holistic manner. Cases of such an implementation gap were perceived as a mere elimination of organizational and technical and financial bottlenecks. Patch management was referred to as one of the most popular. According to one incident responder:

"The conversation I have with boards has changed. Five years ago, it was 'How do we stop this?' Now, it's 'How fast can we get back up when it happens?' We have to assume they will get in. The real battle is the dwell time."

The reason behind this discrepancy in his manufacturing environment. According to one manufacturing industry CISO that complained:

"Everyone says they have backups. The first question I ask after a breach is, 'When was the last time you did a full restore test?' The silence is usually deafening. The attackers know this; they go for the backups first."

Theme 3: The Human Element as the Perennial Wildcard

Though the quantitative evidence was striking on the fact that there was a certain inclination to turn to external weaknesses, all the participants reiterated the anthropological aspect as one of the most powerful and even unpredictable ones. This was more than what the phishing phishing was about to assume a wider sense of a security culture. CISO2 was a medical facility and witnessed:

"We can have the best EDR in the world, but even one overworking doctor clicking a link in a persuasive email that appears to have been issued by a partner hospital can take it all away. It is not that our users are dumb, it is that the attackers are extremely strong in using trust and urgency to their advantage."

Traditional compliance-focused security awareness training was also subject to criticism by the participants. It has been described by IR2 as a necessary evil that only ticks a box to a large extent, and recommends a more integrated, culturally-grounded approach. The same theme was that technology is not enough because the attackers will always look and exploit the least resistance and in most instances it will be the exploitation of a trusted party.

Theme 4: The Strategic Blind Spot: Not Understanding the Adversary

The final theme was the ultimate source of misconception by the majority of victim organizations in the nature of threat. They tend to plan an attack by a malware, rather than a lasting, non-robot, individual attacker who is on the network. IR1 explained:

"Many clients detect the ransomware as it's deploying. That's not detecting the attack; that's detecting the last five minutes of a two-week-long attack. They've been living in your network, learning your systems, finding your crown jewels. The ransomware is just them blowing up the bridge on their way out."

To this strategic blind spot owes the erroneous reliance on preventative and signature-based preventative mechanisms like antivirus of the traditional variety that cannot be effective against the so-called living off the land techniques that are adopted at the stealthy phases of an assault. TA1 added:

"If an organization's security posture is entirely focused on stopping malware at the perimeter, they are completely blind to the 99% of the attack that happens post-compromise. They're waiting for an alarm that will only go off after they've already lost."

Integrating Quantitative and Qualitative Findings

The quantitative and the qualitative themes were combined to give a more in-depth and practical view on the problem of ransomware. The two sets of data are then combined to provide some substantial validation to some of the big inferences.

Convergence 1: Porous Perimeter and Foundational Failures

Based on the quantitative data, it can be seen that the highest number of entry points are in unpatched external service (T1190) and compromised access remote credentials (T1078). This is eloquently articulated on qualitative theme of the Best Practice Implementation Gap. The statistics confirm what the attackers are up to and the interviews tell why it is so effective. The real explanation of why vulnerabilities take a lengthy period to be fixed is the technical mortgage mentioned by CISO1. There is a systemic vulnerability which is exerted by the pressure experienced by keeping the systems operational and the complexity of the legacy environment, which attackers have now learned to take advantage of at scale. Therefore, the discussion should be on how to reach the heart of the organizational and operational barriers that contribute to the absence of systematic application of the basic security hygiene, not on some new and magic-bullet technology.

Convergence 2: Living off the Land: The Reality

The quantitative analysis revealed that the official, inbuilt tools were widely used in the form of PowerShell, WMI and RDP to execute the post-compromise operations. This would be in line with the qualitative theme of, Misunderstanding the Adversary. The input shows that most of the tools that are not malicious in nature are used to carry out an attack. The interviews substantiate the fact that it is one of the key blind spots of organizations that continue to think in terms of malware-centric concept of security. The fact that the results overlap is a good point that there is a necessity of behavioral-based detection tools (including EDR and XDR) and necessity to create a baseline of normal activity within the network. Unless they can tell the difference between malicious and legitimate use of PowerShell, defenders are left virtually blind to the most important stages of an intrusion.

Convergence 3: The Importance of Dwell Time

The quantitative data depicts an attack chain spanning several stages. There is no direct payoff for the attacker during the initial access. Here, dwell time (and the associated loss) corresponds to the qualitative themes of the Inevitability of Compromise and the Primacy of Resilience. For practitioners, the quantitative data describing the lengthy attack chain demonstrates that the attacker is changing their approach. Since compromise is a reality, the best opportunity to defend the attack may be during the multiple stages of the attack. During the quantitative analysis of credential dumping, network discovery, and subsequent lateral movement, each identified TTP was viewed in isolation as a sign that the process could be defended from the threat actor before the most damaging and the final attack was executed. This analysis breaks the ransomware problem. The goal should be to disrupt the chain, but ideally, multiple steps should be taken to disrupt the chain prior to the final.

Limitations of the Study

There are a number of important limitations. The quantitative analysis was limited to publicly available ransomware cases and therefore likely represents only a small fraction of the overall ransomware cases since many go unreported. Another limitation is that the qualitative findings were based on a handful of cyber security professionals, which may not reflect a broad range of views. Finally, due to the rapidly evolving nature of the ransomware threat, the techniques and methods employed by the attackers may alter.

Future Work

The continued evolution of malware may include the development of systems that detect ransomware in real time. In the future, research might look at automated incident responses to ransomware, ransomware protection systems in the cloud, and sector-wide comparisons on resilience to ransomware. Improvements in behavioral analytics, enhanced threat intelligence and integration of the two will yield more proactive measures to counter the ransomware threat in today's business environments.

Conclusion

This study seeks to analyze the patterns, lifecycle, and countermeasures of ransomware; in particular, it focuses on the countermeasures of organizations and the different segments of ransomware attacks. The aim of the study was to not only understand the segments of ransomware attacks, but also understand the countermeasures employed by organizations to defend against them. The study used a mixed method where quantitative data of 350 ransomware attacks documented in public domains were used, along with qualitative data collected through personal interviews with cybersecurity experts. The results suggest the presence of incomplete and worthless systems, unpatched systems, and unprotected authentication systems. Based on behavioral and anomaly detection, a method of proactive detection was proposed. The results of the findings demanded a shift of focus toward the attack prediction and detection methods and the organizations that have been targeted by the attacks to strengthen their systems and employ active countermeasures to attack and remove the unpatched ransomware from their systems.

References

Anderson R and Moore T (2021) Cybercrime: The economics behind ransomware. Journal of Cybersecurity 7: 1–12.

Chen Y, Zhang X and Lin Z (2021) Understanding ransomware attacks: A data-driven analysis. Computers & Security 105: 102258.

Covie B (2021) Double extortion ransomware: The new norm. Journal of Cyber Policy 6: 239–255.

Europol (2020) Internet Organised Crime Threat Assessment (IOCTA) 2020. The Hague: Europol.

Farooq, A., Javed, F., Hussain, M., Abbas, T., & Hussain, A. (2012). Open source content management systems: a canvass. International Journal of Multidisciplinary Science and Engineering, 3(10), 38-43.

Hussain, M., Kim, K. H., Akbar, A. H., Khalid, S., Bang, S. J., Javed, M., & Amjad, M. (2016). A gateway deployment heuristic for enhancing the availability of sensor grids. International Journal of Distributed Sensor Networks, 12(8), 7595038.

Hussain, M., Shafeeq, M. F., Jabbar, S., Akbar, A. H., & Khalid, S. (2016). CRAM: a conditioned reflex action inspired adaptive model for context addition in wireless sensor networks. Journal of Sensors, 2016(1), 6319830.

Kharraz A, Arshad S, Mulliner C, Robertson W and Kirda E (2015) Cutting the Gordian knot: A look under the hood of ransomware attacks. Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment 3–24. Berlin: Springer.

Kshetri N (2021) The global cybersecurity policy landscape and the role of institutions. Telecommunications Policy 45: 102128.

Mohurle S and Patil M (2017) A brief study of WannaCry ransomware attack. International Journal of Advanced Research in Computer Science 8: 1938–1940.

Richardson R and North MM (2017) Ransomware: Evolution, mitigation and prevention. International Management Review 13: 10–21.

Scaife N, Carter H, Traynor P and Butler KRB (2016) Cryptolock (and drop it): Stopping ransomware attacks on user data. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS) 303–312.

Ubaid, S., Shafeeq, M. F., Hussain, M., Akbar, A. H., Abuarqoub, A., Zia, M. S., & Abbas, B. (2018). SCOUT: a sink camouflage and concealed data delivery paradigm for circumvention of sink-targeted cyber threats in wireless sensor networks. The Journal of Supercomputing, 74(10), 5022-5040.

Young A and Yung M (1996) Cryptovirology: Extortion-based security threats and countermeasures. Proceedings of the 1996 IEEE Symposium on Security and Privacy 129–140.

Zimba A and Wang Z (2019) Modeling and analyzing ransomware attacks using kill chain and diamond models. IEEE Access 7: 153384–153395.