Reconnaissance to Ransom - A Kill Chain-Based Approach to Ransomware Analysis

Alexander Lawall
IU International University of App. Sc.
Erfurt, Thüringen, Germany
e-mail: alexander.lawall@iu.org

Petra Beenken
IU International University of App. Sc.
Erfurt, Thüringen, Germany
e-mail: petra.beenken@iu.org

Alexandra Blia
Threat Intelligence Services, Rapid7
Prague, Czech Republic
e-mail: alexandra_blia@rapid7.com

***Abstract*—The current ransomware ecosystem is analyzed, focusing on the Tactics, Techniques, and Procedures (TTPs) adopted by ransomware groups. The last two years are considered and compared. The purpose of the research is to enhance the understanding of ransomware operations and to improve defense strategies. The paper investigates the research questions: (1) How has the ransomware ecosystem evolved over the past two years? and (2) What is the impact of these changes on the TTPs adopted by ransomware groups? Using Open Source Intelligence and Dark Web Intelligence, the methodology follows a three-step approach: (1) Identifying active ransomware groups, (2) Profiling threat actors and mapping their TTPs to the MITRE ATT&CK framework, and (3) Prioritizing mitigation strategies based on a heatmap analysis. The research outcomes reveal a shift in top ransomware techniques with an increasing focus on data exfiltration, vulnerability exploitation, and cloud-based exfiltration. This contributes to empirical insights and data-driven mitigation recommendations, supporting cybersecurity professionals, policymakers, and researchers in strengthening resilience against ransomware attacks.**

***Keywords*-Ransomware, Cybercrime, Ransomware-as-a-Service (RaaS), Tactics Techniques and, Procedures (TTPs), Dark Web Intelligence, Artificial Intelligence.**

I. Introduction

A. Background and Motivation

Investing in effective and efficient cybersecurity measures is essential for companies to protect their systems against the increasing threat of cyberattacks [1]–[3]. Among these threats, ransomware attacks pose a particularly serious risk, capable of inflicting substantial financial and operational damage on organizations in various sectors [4]. The dynamic and adaptive nature of ransomware groups requires companies to adopt proactive defense strategies that are tailored to the modus operandi of current threat actors. In [5], the contribution presented the ransomware landscape from the first half of 2023, analyzing the Tactics, Techniques, and Procedures (TTPs) characterizing the groups that were active at that time. This article adopts this methodology to capture the current ransomware threat landscape, focusing on ransomware groups active in the second half of 2024. The application of the same methodology enables a direct comparison between the results obtained, reflecting changes in the adopted TTPs over the reporting periods in scope.

A fundamental prerequisite for developing such defense strategies is a comprehensive understanding of the TTPs adopted by ransomware groups. By systematically analyzing the TTPs of the most active groups, organizations can improve their detection and mitigation capabilities while identifying intervention points along the attack chain. This knowledge empowers security teams to align defensive measures with adversary behaviors, increasing the overall resilience of enterprise environments.

This paper provides an overview of the current TTPs of the most active ransomware groups, classified according to their victim counts and operational impact. Identified TTPs are systematically mapped to the MITRE ATT&CK framework [6], offering a structured model to understand ransomware attack patterns and to derive targeted defense strategies. Specifically, MITRE ATT&CK Matrix for Enterprise version 16.1 is used to model the behavior of the ransomware groups in scope. As the framework is updated regularly, with a new version being released twice a year, recent updates that influence the results are also discussed.

As part of this process, recently emerged ransomware groups were identified, with their behavior mapped to relevant TTPs. This evolution of the ransomware landscape, with the introduction of new players and the rebranding of older ones, alters the TTPs that are commonly adopted by ransomware groups. These changes are highlighted in this paper, along with the recommended reprioritization of mitigations and defense strategies in response to changing threat actor behavior. Furthermore, the paper mentions the enhancements of the MITRE ATT&CK framework.

B. Research Questions and Objectives

The ransomware ecosystem is in constant flux, with new groups emerging and existing actors continuously adapting their TTPs to evade detection and maximize impact. As ransomware operations become increasingly dynamic, understanding the current landscape and identifying the prevailing attack patterns are critical for developing effective defense strategies. This paper aims to provide an up-to-date overview of the most active ransomware groups and their associated TTPs.

The analysis leverages Open Source Intelligence (OSINT) and Dark Web Intelligence to systematically observe ransomware groups and gather insights into their operational

methods. The following research questions guide the investigation:

RQ1 *"How has the ransomware ecosystem evolved over the past two years, and what key trends currently characterize its structure and operations?"*

RQ2 *"What is the impact of these changes on the TTPs adopted by ransomware groups?"*

By addressing these questions, the study contributes to a deeper understanding of ransomware group dynamics and supports the development of TTP-based defense models.

C. Contribution and Paper Structure

Beyond providing an updated overview of ransomware activity, this paper makes three specific contributions. First, it offers a longitudinal empirical comparison of ransomware TTPs across two observation periods, enabling the identification of shifts in attacker behavior between 2023 and 2024. Second, it maps the observed TTPs to the MITRE ATT&CK framework and derives a mitigation prioritization based on technique prevalence, thereby translating threat intelligence observations into actionable defensive guidance. Third, it interprets the observed shifts from a socio-technical perspective by relating them to changes in attacker incentives, defender adoption of security controls, and the increasing availability of cloud services and Artificial Intelligence (AI)-enabled tooling. In this way, the paper aims not only to describe recent ransomware developments, but also to explain why these developments matter for organizational defense.

The remainder of this paper is structured as follows. Section II reviews the theoretical background on ransomware, its evolution, and related defense frameworks. Section III presents the research methodology, including data collection, profiling, ATT&CK mapping, and mitigation prioritization. Section IV reports the empirical findings and analyzes the evolution of the ransomware ecosystem, prevalent TTPs, and recommended mitigations. Finally, Section V concludes the paper and outlines directions for future research.

II. Theoretical Background

A. Definition and Characteristics of Ransomware

The National Institute of Standards and Technology (NIST) defines ransomware as "a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access" [7]. Beyond data encryption, ransomware attacks may also involve extortion tactics, where attackers threaten to publicly disclose stolen data unless an additional ransom payment is made [8]. These attacks represent a form of computer fraud with significant legal and economic implications [9].

Ransomware can be broadly categorized into two primary types: file-encrypting ransomware and locker ransomware [10]–[12].

- File-encrypting ransomware is the most prevalent type, where attackers encrypt files on the victim's system and demand payment for the decryption key [13].
- Locker ransomware, on the other hand, locks users out of their entire system without encrypting individual files, preventing access to the device until a ransom is paid.

Ransomware attacks are not only defined by the type of ransomware deployed but also by the techniques used during the attack vector [14]. For example, threat actors use social engineering techniques, such as phishing emails, to trick victims into downloading malicious payloads that execute ransomware on the targeted system [15]. These techniques are part of the initial access phase of ransomware campaigns, showing the need for both technical defenses and user awareness measures [16].

B. Ransomware's Paradigm Shift

Ransomware has evolved from opportunistic attacks to sophisticated, orchestrated operations, becoming a major cybersecurity threat [17]. The rise of Ransomware-as-a-Service (RaaS) models and double extortion techniques has increased the scale and impact of attacks [18]. Ransomware groups have complex relationships with states, particularly Russia, leading to the concept of "cyber privateers" engaged in state crime [19]. The evolution of ransomware has seen paradigm shifts in attack structures, with impacts on both technical and economic fronts [17]. Research has primarily focused on detection techniques, with 72.8% of studies addressing this area and 70% of those utilizing machine learning methods [20]. However, there is a lack of focus on predicting ransomware and addressing issues, such as adversarial machine learning exploitation and concept drift [20].

C. Ransomware Defense and Prevention Frameworks

Mitigating ransomware attacks requires a multifaceted approach that combines technical, organizational, and human-centric measures to strengthen overall resilience [21]–[23]. Key mitigation strategies include the implementation of robust backup and recovery systems, network segmentation, access control policies, patch management practices, threat intelligence integration, and incident response plans [24]. These mitigations collectively strengthen defenses across different stages of the attack vector.

The NIST Cybersecurity Framework provides a comprehensive model for ransomware mitigation, structured around five core functions: Identify, Protect, Detect, Respond, and Recover [25]. This framework enables organizations to take a holistic approach to ransomware defense by aligning technical and procedural measures with risk management principles.

Additionally, incident response methodologies, such as the SANS and NIST Incident Response frameworks, emphasize the importance of pre-incident preparation, threat detection, containment, eradication, and recovery [26]–[28]. These approaches show the need for continuous readiness and post-incident learning to mitigate the impact of ransomware attacks.

Furthermore, adherence to international standards like ISO/IEC 27001 for information security management and

ISO/IEC 22301 for business continuity enhances an organization's ability to resist and recover from ransomware incidents [29].

By integrating these strategies and frameworks, organizations can establish a layered defense posture that not only prevents ransomware attacks but also ensures rapid recovery and operational continuity in the event of an incident [30].

III. Methodology

The methodology applied in this research is adapted from the approach presented by [5]. It follows a three-step process, illustrated in Figure 1, to systematically analyze the ransomware threat landscape. In the first step, a quantitative

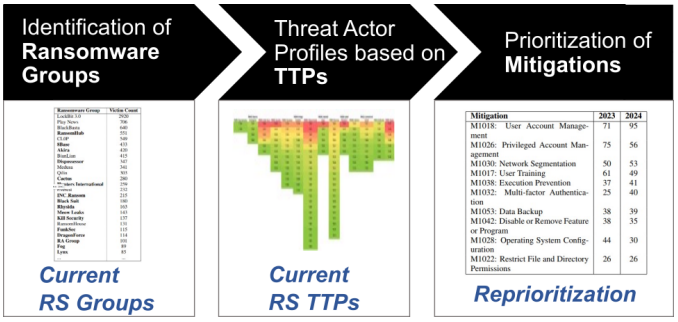

Figure 1. Three-step Methodology adapted from [5]

foundation is established to support the subsequent analysis. This involves identifying the most active ransomware groups based on their victim count within a defined observation period.

The second step focuses on the qualitative analysis of the identified groups. This includes the creation of threat actor profiles and the examination of the TTPs each group employs.

The final step consists of mapping the identified TTPs to corresponding mitigation strategies, providing actionable insights for enhancing organizational defense measures.

A. Data Collection and Coding Procedure

The data collection process followed a structured multi-source workflow to improve methodological transparency and reproducibility. First, ransomware groups active in the second half of 2024 were identified using publicly available incident-tracking sources, primarily the Ransomware Database, complemented by vendor reporting and open-source reporting. Second, groups were ranked according to publicly attributed victim counts observed during the study period. Third, for each selected group, qualitative threat-intelligence material was collected from academic publications, vendor reports, OSINT sources, and dark-web-related reporting in order to identify described attacker behaviors. Fourth, these behaviors were manually coded into MITRE ATT&CK techniques and sub-techniques, using ATT&CK for Enterprise version 16.1 as the reference taxonomy.

Only techniques supported by explicit behavioral evidence in the consulted sources were included to reduce ambiguity during ATT&CK mapping. When multiple sources described the same behavior differently, the most specific ATT&CK-compatible interpretation was selected. If the evidence was too vague to support a reliable mapping, the behavior was excluded from the technique set. This conservative coding approach was chosen to reduce over-attribution and improve interpretability.

The study focuses on the top ransomware groups identified during the observation period to capture the most operationally relevant actors. This choice improves the practical relevance of the findings for defenders, although it also introduces a bias toward more visible and more heavily reported groups. The resulting dataset should therefore be interpreted as a structured view of prominent ransomware activity rather than an exhaustive census of all ransomware operations.

B. Identification of Ransomware Groups

This research was carried out in January 2025, focusing on ransomware groups active during the second half of 2024. To identify the most active groups, data was gathered from publicly available sources, including the Ransomware Database, which provides real-time updates on ransomware incidents.

Table I presents an overview of the identified ransomware groups, ranked by their victim count. Newly emerging groups are highlighted in bold font to emphasize their entry into the ransomware ecosystem. By highlighting newly emerging groups in bold, we draw attention to the dynamic nature of the ransomware threat. We specifically define "emerging" as groups that have reached a victim count of 84 or more since the second half of 2024, providing a clear and objective criterion. This allows us to track not only the established threat actors but also the rising threats that may pose significant future risks. The analysis of their TTPs, combined with their victim count and emergence status, allows for a comprehensive understanding of the current ransomware landscape and its evolution.

This research has conducted a comprehensive analysis of the top 24 ransomware groups (ranked in Table I) to understand the evolving landscape of ransomware attacks. This approach allows for a direct comparison of changes in their TTPs over time.

C. Threat Actor Profiles based on TTPs

The profiling of threat actors and the analysis of their TTPs are based on the methodology outlined by Lawall et al. [5]. Detailed profiles are created for ransomware groups active in recent months, with each profile incorporating a dedicated MITRE ATT&CK matrix that maps the observed TTPs.

Different data sources were used to achieve a comprehensive understanding of the ransomware landscape. This includes academic literature, cybersecurity reports from companies, such as Trend Micro and CrowdStrike, as well as information from databases like the Ransomware Database and SOCRadar. Additionally, intelligence gathered from Dark Web research and OSINT platforms, including BleepingComputer and Reddit cybersecurity forums, provided valuable insights into the

activities, TTPs, and impact of ransomware groups across various sectors.

Threat actor profiling involves examining the motivations, capabilities, and attack patterns of ransomware groups to develop detailed behavioral profiles. These profiles support the identification of vulnerabilities and the formulation of targeted mitigation strategies [31]. Since ransomware actors continuously adapt their tactics, ongoing monitoring is essential to maintain up-to-date threat intelligence. This paper presents an updated assessment of the ransomware landscape as of January 2025, reflecting the latest developments in threat actor behavior and their operational methods.

D. Identification and Prioritization of Mitigations

The prioritization of mitigations is based on a comprehensive heatmap analysis that visualizes the TTPs employed by various ransomware groups. This heatmap provides an overview of the frequency and prominence of specific TTPs across the analyzed threat actor profiles (cf. Figure 2).

By identifying TTPs that are commonly used and have a significant impact, the analysis aligns them with established mitigation strategies from cybersecurity frameworks. The frequency of TTP occurrence serves as a key criterion for prioritization, enabling the targeted allocation of resources toward the most critical threats.

The resulting prioritized mitigations are systematically documented, offering cybersecurity teams a strategic roadmap for their implementation (cf. Table IV). The methodology for scoring and ranking mitigations is outlined in detail in Section IV-C.

This tailored approach helps organizations strengthen their defenses against the most widespread and impactful ransomware techniques, significantly improving their resilience against ransomware attacks.

IV. Results and Analysis

A. The Ransomware Ecosystem

The ransomware ecosystem has experienced a significant transformation in 2024, characterized by an expansion in the number of active groups and a noticeable shift towards professionalization. In the second half of 2024, the number of active ransomware groups increased to 77, compared to just 26 in the first half of 2023. As such, the number of ransomware groups nearly tripled during this period. This substantial increase indicates a thriving and rapidly evolving threat landscape that has embraced new organizational models and strategies.

The dynamics of this ecosystem reveal an interplay between established and emerging groups. Among the top 24 ransomware groups (cf. Table I) whose TTPs were analyzed, 10 were identified in previous research, while 14 had ascended the ranks. This development and success of "new" groups may be attributed to alliances, or shared knowledge with "older" groups, suggesting an underlying network of connections and collaborations that facilitate their rise to prominence.

Table I
Ransomware Groups in Scope

Ransomware Group	Victim Count
LockBit 3.0	2920
Play News	706
BlackBasta	640
RansomHub	551
CL0P	549
8Base	433
Akira	420
BianLian	415
Dispossessor	347
Medusa	341
Qilin	303
Cactus	280
Hunters International	259
Everest	232
INC_Ransom	215
Black Suit	180
Rhysida	163
Meow Leaks	143
Kill Security	137
RansomHouse	131
FunkSec	115
DragonForce	114
RA Group	101
Fog	89
Lynx	85
...	...

The leading ransomware groups, such as LockBit, Play News, and BlackBasta, continue to maintain a foothold, with their operations dating back to at least 2022. The persistence and dominance of these groups underscore their adaptability and the relevance of their operational models. In contrast, newly emerged groups like Lynx and RansomHub have embraced the RaaS business model, typifying a prevalent trend in the ransomware domain that enhances the scale and reach of attacks through affiliate networks.

The distinction between conventional cybercrime and hacktivism is increasingly dissolving, as evidenced by the activities of emergent threat actors, such as FunkSec and Kill Security. While these groups are broadly categorized as ransomware operators due to their proclaimed capabilities, their operations are profoundly shaped by politically motivated agendas, blending financial extortion with ideological objectives. This convergence of motives reflects the hybrid nature of modern threat actors, who navigate the intersection of cybercrime, hacktivism, and state interests, challenging traditional classifications of cyber threats.

A particularly notable development is the reported use of AI tools, including large language model assistants, to support malware development and operational preparation. From a research perspective, the technical significance of this trend lies less in the novelty of the final malware artifacts and more in the democratization of attacker capability. AI-assisted tooling can accelerate code generation, scripting, documentation, and adaptation, thereby lowering the expertise threshold required to participate in ransomware operations. In socio-technical terms, this development may help explain the rapid expansion

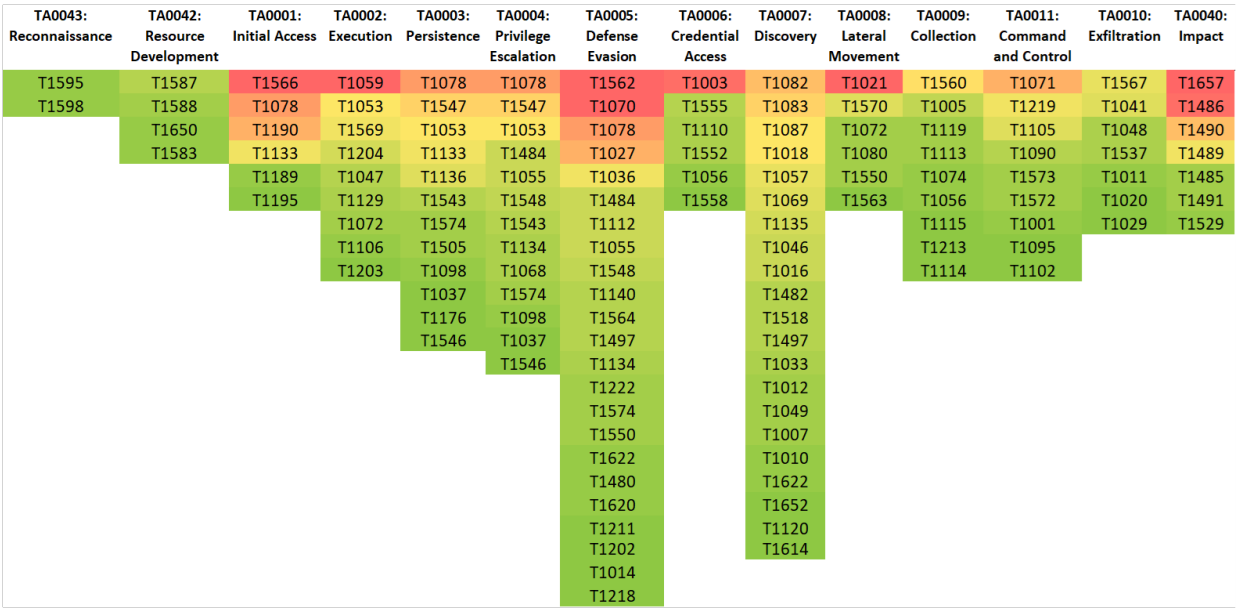

Figure 2. Heatmap of the Tactics and Techniques of the analyzed Ransomware Groups

Table II
INTERPRETATION OF KEY TECHNIQUES USED IN THIS STUDY

Technique	Interpretation in Ransomware Context
T1190: Exploit Public-Facing Applications	Attackers exploit vulnerabilities in internet-exposed services such as VPNs, web applications, or edge devices to obtain initial access.
T1078: Valid Accounts	Attackers use legitimate credentials, whether stolen, purchased, or reused, to access systems while blending in with normal user activity.
T1486: Data Encrypted for Impact	Attackers encrypt victim data to disrupt business operations and force ransom payment.
T1490: Inhibit System Recovery	Attackers delete backups, shadow copies, or recovery mechanisms to make restoration more difficult.
T1021.001: Remote Desktop Protocol	Attackers use RDP for remote access, lateral movement, or direct control of compromised systems.
T1566: Phishing	Attackers use malicious emails, links, or attachments to deceive users into enabling compromise.
T1219: Remote Access Software	Attackers abuse legitimate remote administration software for persistence, control, or evasion.
T1657: Financial Theft	Attackers pursue direct financial gain through extortion or financially motivated theft, including operations where data theft and coercion take precedence over encryption.

of the ransomware ecosystem by enabling more decentralized and opportunistic actors to approximate capabilities that previously required stronger technical specialization.

The ransomware landscape in 2024 is characterized by a dynamic interplay between continuity and disruption. While long-standing ransomware groups continue to exert significant influence, the entrance of novel actors leveraging emerging technologies and hybrid motivations introduces unprecedented complexity into the threat ecosystem. This evolution underscores the adaptive nature of ransomware groups and presents persistent challenges for cybersecurity defenses, requiring both technological innovation and intelligence-driven strategies to effectively mitigate the shifting threat landscape.

B. TTPs used by current Ransomware Groups

For readability, each MITRE ATT&CK identifier in Figure 2 corresponds to a concrete attacker behavior, cf. Table II. For example, T1190 refers to the exploitation of public-facing applications, T1078 refers to the abuse of valid accounts, T1486 denotes data encryption for impact, and T1657 captures financially motivated theft or extortion-oriented actions that do not rely solely on file encryption. Accordingly, the ATT&CK identifiers should be interpreted as compact references to operational behaviors rather than abstract labels. This is important because the heatmap is intended to summarize how ransomware groups move across the attack chain, from reconnaissance to impact.

Therefore, Figure 2 presents a MITRE ATT&CK heatmap, where each technique is represented by its unique identifier. The heatmap visualizes the TTPs adopted by the ransomware groups under analysis, offering a structured overview of their operational methods.

The heatmap was generated based on the methodological approach using aggregated layers that consolidate the TTPs observed across the analyzed ransomware groups. The heatmap presents relevant techniques, aggregating the scores of the associated sub-techniques using the sum function. The color intensity indicates the relative prevalence of each technique across the observed groups:

- Green represents techniques with low adoption rates.
- Red highlights techniques that are frequently employed.
- Yellow and orange shades form a gradient between green and red, automatically calculated based on the underlying frequency scores.

This visualization provides insights into the most commonly adopted techniques and the emergence of novel attack methods within the ransomware ecosystem.

1) Most used Techniques by Ransomware Groups: The analysis of ransomware groups reveals a substantial shift in operational tactics, with ∼40% of the top ten techniques changing between 2023 and 2024, cf. Table III. This degree of change indicates a significant adaptation and diversification in the methods employed by ransomware groups, reflecting their ability to rapidly evolve in response to technological advancements and defensive measures. From an analytical perspective, this result indicates only partial continuity between the two periods and suggests that a static view of ransomware behavior is insufficient for defensive planning. Even when some core techniques remain stable, the reordering of their prevalence materially changes which controls should be prioritized.

A particularly noteworthy development in 2024 is the introduction of the technique T1657: Financial Theft, which extends the scope of ransomware operations to include extortion attempts independent of encryption-based attacks. This technique applies to all ransomware groups and marks a critical expansion of the ransomware threat model. Its absence in prior evaluations highlights the dynamic evolution of threat actor strategies, where data theft and financial extortion increasingly serve as primary attack objectives alongside traditional file encryption.

This observation reinforces the need for continuous reassessment of ransomware TTPs, but it also points to a broader socio-technical shift in ransomware operations. In particular, the rise of techniques, such as T1190 and T1082, suggests that ransomware groups are adapting to a defensive environment in which phishing awareness, stronger password policies, and Multi-Factor Authentication (MFA) increasingly constrain traditional intrusion paths. At the same time, data theft, direct extortion, and cloud-supported exfiltration create alternative revenue models that reduce dependence on encryption alone. Thus, the observed TTP changes should not be interpreted merely as technical variation, but as evidence of adversarial adaptation to both defensive pressure and changing economic opportunities.

The next sections focus on each phase of the attack vector, highlighting the main developments in terms of tactics adopted by ransomware groups.

2) TA0001 Initial Access: The findings from our study underscore an evolution in ransomware groups' techniques leveraged for initial access, particularly a heightened focus on exploiting known vulnerabilities in 2024. This is reflected in increased adoption of the technique T1190: Exploit Public-Facing Applications by the ransomware groups in scope. While groups like Cl0p are adept at exploiting zero-days, it is the prevalent targeting of existing vulnerabilities that drives this current trend. This shift could be attributed to improved password policies and the adoption of MFA, making legitimate credentials a less favored route for intrusion. Furthermore, there has been a noticeable decline in reliance on phishing techniques compared to 2023, with a move towards malicious links over spearphishing attachments. The targeting of external remote services, such as VPNs, a technique that surged during the COVID-19 pandemic, has decreased, potentially due to the transition to hybrid work models and enhanced security management. It is notable that the techniques T1078: Valid Accounts and T1133: External Remote Services frequently intersect, explaining their reduced utilization. Another notable development is the use of T1195: Supply Chain Compromise for initial access. This indicates the growing sophistication of modern ransomware groups, given that only threat actors with high capabilities can successfully deploy this technique. Historically, this technique has been associated with the activity of nation-state and state-sponsored threat actors, primarily of Russian and Chinese origin.

Table III
COMPARISON OF THE TOP 10 TECHNIQUES

Technique	2023	2024
T1657: Financial Theft	-	100%
T1486: Data Encrypted for Impact	96%	96%
T1190: Exploit Public-Facing Applications	54%	71%
T1490: Inhibit System Recovery	63%	67%
T1082: System Information Discovery	33%	67%
T1078: Valid Accounts	83%	63%
T1562.001: Disable or Modify Tools	58%	63%
T1083: File and Directory Discovery	58%	58%
T1021.001: Remote Desktop Protocol	42%	58%
T1070.004: File Deletion	29%	50%
T1133: External Remote Services	63%	46%
T1489: Service Stop	50%	46%
T1059.001: PowerShell	54%	42%
T1566: Phishing	50%	42%

3) TA0002 Execution: In terms of execution, ransomware groups predominantly use scripts and command-line interfaces, with a decline in PowerShell use attributable to restrictive policies. There is a marked increase in the abuse of the Windows command shell and the service control manager, signaling a concentrated shift towards the exploitation of Windows systems.

4) TA0003: Persistence & TA0004 Privilege Escalation: In 2024, ransomware groups continue relying on T1078: Valid Accounts and T1053: Scheduled Task/Job to maintain their foothold and escalate their privileges within the compromised environments. Although the results under this tactic are similar to the ones obtained in 2023, ransomware groups have started executing automatically scripts, either at boot, or logon to establish persistence, or escalate their privileges. Thus, the technique T1037: Boot or Logon Initialization Scripts is of relevance, since such initialization scripts often run with higher privileges.

5) TA0005 Defense Evasion: Ransomware groups persist in using legitimate credentials while employing sophisticated

obfuscation techniques, such as encryption, to minimize the likelihood of detection. Additionally, these threat actors have increasingly adopted T1211: Exploitation for Defense Evasion, underscoring a strategic shift towards vulnerability exploitation across multiple stages of the attack vector. Furthermore, forensic analysis has identified the use of T1014: Rootkit, enabling ransomware groups to conceal the presence of malicious payloads and maintain persistence within compromised systems.

6) TA0006 Credential Access: In 2024, ransomware groups were observed executing T1003: OS Credential Dumping, a widely utilized technique, along with its associated sub-techniques, to extract authentication credentials and account login data. A notable advancement in their tactics was the adoption of T1056: Input Capture, which facilitates credential harvesting and information collection through keylogging and other input monitoring mechanisms.

7) TA0007 Discovery: Ransomware groups actively employ discovery techniques to gain a comprehensive understanding of compromised environments and internal systems. The use of T1082: System Information Discovery has become increasingly prevalent, as adversaries seek detailed insights into the operating system and hardware to tailor subsequent attack phases. This trend highlights the growing precision and targeted nature of ransomware operations.

Additionally, T1083: File and Directory Discovery remains a standard tactic, enabling ransomware operators to systematically enumerate files and directories within infiltrated environments. This activity is strongly correlated with the widespread adoption of double-extortion strategies, as it facilitates both data collection and exfiltration.

Furthermore, adversaries have expanded their reconnaissance methodologies by using T1010: Application Window Discovery, which provides visibility into active application windows, and T1652: Device Driver Discovery, which enables enumeration of local device drivers. These advancements suggest an increasing emphasis on environmental awareness, allowing ransomware groups to refine their attack execution based on real-time system insights.

8) TA0008 Lateral Movement: In 2024, Remote Desktop Protocol (RDP) remains the predominant vector for compromising networked systems, underscoring its continued prevalence due to its capability to grant direct access to targeted environments. This sustained reliance on RDP highlights its effectiveness in facilitating unauthorized system entry and operational control.

Simultaneously, there has been a significant increase in the adoption of lateral tool transfer by ransomware groups, a technique involving the movement of tools or files across systems within the same network. This tactic not only enhances the propagation of malicious activity but also enables deeper infiltration into critical infrastructure by circumventing conventional security mechanisms.

9) TA0009 Collection: Ransomware groups continue to employ a range of techniques to systematically extract data from compromised systems, with T1560.001: Archive via Utility being a prominent sub-technique used for data compression and exfiltration. Additionally, the recently observed use of T1056: Input Capture further reinforces this tactic, enabling adversaries to harvest sensitive information by keystroke logging and other input monitoring mechanisms. These developments highlight the increasing sophistication of ransomware operations in data collection and exfiltration strategies.

10) TA0011 Command and Control: In 2024, ransomware groups have increasingly used T1219: Remote Access Software and T1071.001: Web Protocols as primary techniques for command and control (C2) operations, reinforcing their reliance on covert communication channels.

To further evade detection, these threat actors have expanded their arsenal by employing T1001: Data Obfuscation, along with its sub-technique T1001.001: Junk Data, to obscure C2 traffic and bypass security monitoring mechanisms. Additionally, ransomware operators have begun exploiting T1102: Web Service by utilizing legitimate external web services, such as Amazon S3 and Google Drive, to exfiltrate and relay data from compromised systems. This trend highlights the persistent abuse of cloud-based platforms to facilitate ransomware operations while evading traditional network security defenses.

11) TA0010 Exfiltration: Recent findings indicate a growing trend among ransomware groups to exfiltrate data through their C2 channels, likely as a strategy to avoid detection during exfiltration efforts. This tactic allows malicious actors to maintain a low profile by concealing their data theft activities within regular communication channels. Furthermore, there is a noticeable increase in the use of cloud environments by ransomware groups, which facilitates the efficient storage and distribution of illicitly obtained information. Emerging ransomware groups, such as Lynx, have been observed utilizing cloud storage services, like Mega, to store and share their stolen data, demonstrating an evolution in their operational methods to leverage accessible and often less scrutinized cloud resources. This shift underscores the critical need for enhanced monitoring and security measures tailored to cloud-based environments to effectively counteract these evolving threats.

12) TA0040 Impact: The widespread adoption of double extortion tactics by ransomware groups has become increasingly prevalent, with nearly all active groups operating a ransomware variant, Kill Security being a notable exception. This evolution reflects a strategic shift, wherein adversaries not only encrypt and restrict access to critical data but also leverage the threat of sensitive data exfiltration to coerce victims into compliance.

This dual-pronged approach significantly amplifies the coercive leverage of ransomware operators, demonstrating their adaptability and reinforcing the global cybersecurity threat they pose. While some groups intermittently engage in pure extortion without deploying ransomware, double extortion remains the dominant strategy, as it maximizes psychological and financial pressure on victims, thereby increasing the likelihood of ransom payments.

Table IV
COMPARISON OF THE TOP 10 MITIGATIONS

Mitigation	2023	2024
M1018: User Account Management	71	95
M1026: Privileged Account Management	75	56
M1030: Network Segmentation	50	53
M1017: User Training	61	49
M1038: Execution Prevention	37	41
M1032: Multi-factor Authentication	25	40
M1053: Data Backup	38	39
M1042: Disable or Remove Feature or Program	38	35
M1028: Operating System Configuration	44	30
M1022: Restrict File and Directory Permissions	26	26

C. Mitigation Measures and Effectiveness

These evolving cyber threat patterns emphasize the need for organizations to fortify their security frameworks and implement adaptive defense strategies to counteract the growing sophistication of ransomware operations.

An analysis of the current TTPs employed by ransomware groups reveals a subtle shift in prioritizing corresponding mitigations.

Methodology for Scores: The mitigation scoring approach follows a systematic methodology to quantify the effectiveness of defense strategies against ransomware attacks. The process consists of four sequential steps. First, ransomware techniques and their prevalence scores were collected and structured into individual layers. Next, these layers were aggregated into a master layer, providing a comprehensive view of the ransomware techniques observed across all analyzed groups.

Based on this consolidated view, mitigation strategies were identified by mapping each technique to its corresponding mitigations. Finally, the prevalence scores of all techniques mapped to each mitigation were summed, resulting in a representative score that reflects the importance of each mitigation strategy in countering the most commonly adopted ransomware techniques.

This approach provides empirical, data-driven insights into the significance of mitigation measures, enabling organizations to prioritize defenses against the most prevalent ransomware methods.

Mitigations: Table IV lists the top mitigation strategies associated with the most prevalent ransomware techniques observed in 2024. Although the set of leading mitigations is broadly similar to that of 2023, their relative prioritization has changed in response to shifts in attacker behavior. This finding does not imply that lower-ranked mitigations have become unimportant. It indicates that the defensive emphasis should be adjusted to reflect the changing prevalence of exploitation, remote access abuse, defense evasion, and extortion-oriented behaviors.

In more detail, User Account Management (M1018) is currently the top mitigation, mainly because it offers protection against impact techniques, including Financial Theft (T1657) and Inhibit System Recovery (T1490). Thus, the recent introduction of Financial Theft (T1657) as a new technique further raised the importance of this mitigation. Even though Privileged Account Management (M1028) and User Training (M1017) remain high-priority mitigations, their importance has slightly declined. This observation does not imply these mitigations are obsolete but rather reflects shifts in threat actor behavior, specifically the reduced adoption of T1078: Valid Accounts and Phishing (T1566) respectively.

Instead, as the threat actors have shifted towards vulnerability exploitation, Network Segmentation (M1030) should be prioritized further. Similarly, the results suggest that Software Updates (M1051) should also be prioritized, aligning with the rising exploitation of software vulnerabilities and network-based attack techniques. Similarly, a significant increase in the importance of Multi-factor Authentication (M1032) as well as Execution Prevention (M1038) was also observed due to the enhanced adoption of the techniques Remote Desktop Protocol (T1021.001) and Disable or Modify Tools (T1562.001), as well as Inhibit System Recovery (T1490), respectively.

D. Socio-Technical Interpretation of TTP Evolution

The observed changes in ransomware TTPs between 2023 and 2024 can be interpreted as the result of an ongoing adaptation process at the interface of attacker incentives, defender controls, and technological opportunity structures. First, the increased use of vulnerability exploitation, particularly against public-facing applications, suggests a rational response to improved defensive controls, such as stronger password policies and wider adoption of MFA. When credential abuse becomes more difficult or more detectable, attackers are incentivized to shift toward exploitable exposed systems.

Second, the growing relevance of exfiltration, financial theft, and cloud-based channels indicates that ransomware groups are optimizing for flexible monetization. In this sense, ransomware is no longer reducible to encryption-centric disruption. Instead, it increasingly reflects a broader extortion economy in which data theft, coercion, and reputational pressure can be monetized independently or in combination. Third, the use of legitimate cloud services and remote administration software illustrates a continued strategic preference for blending malicious behavior into normal enterprise activity, thereby complicating detection and attribution.

Finally, the emergence of AI-assisted workflows may lower the barrier to entry for less mature actors and accelerate the operational learning cycle of new groups. Taken together, these developments suggest that ransomware evolution should be understood not only as a sequence of changing techniques, but as a socio-technical process shaped by attacker business models, defender adaptation, and the availability of widely accessible digital infrastructure.

E. Limitations

This study has several limitations that should be considered when interpreting the results. First, the analysis relies heavily

on publicly available reporting, including OSINT, vendor reports, and incident-tracking platforms. As a result, the dataset is affected by visibility bias: groups that are more publicly reported or more active in naming victims are more likely to be represented than stealthier actors. Second, the ranking of ransomware groups by victim count provides an operationally useful approximation of ecosystem relevance, but it does not directly measure technical sophistication, or actual financial impact.

Third, the mapping of observed behaviors to MITRE ATT&CK techniques requires interpretive judgment. Although a conservative coding strategy was applied, some ATT&CK mappings remain inherently approximate because source reports vary in specificity and quality. Fourth, because the analysis focuses on the top groups in the observation period, the results emphasize prominent ransomware behavior rather than the full diversity of the ecosystem. Finally, the comparison across periods may also be influenced by changes in ATT&CK itself, as newly introduced or revised techniques affect how behaviors can be categorized. Consequently, the findings should be interpreted as a structured and practically relevant representation of current ransomware trends, rather than as a complete or exhaustive model of all ransomware activity.

V. Conclusion

The analysis of the evolving ransomware landscape provides key insights into the structural and operational transformations of ransomware groups over the past two years.

Regarding RQ1: "How has the ransomware ecosystem evolved over the past two years, and what key trends currently characterize its structure and operations?", the study reveals a significant expansion in the number of active ransomware groups, nearly tripling from early 2023 to late 2024. This surge indicates the increasing professionalization of ransomware operations, largely driven by the RaaS model. Additionally, the ecosystem has seen a convergence between financially motivated cybercrime and politically driven hacktivism, further complicating threat intelligence efforts. Notably, new ransomware actors have increasingly leveraged AI tools to facilitate malware development, lowering the technical entry barriers for emerging groups and accelerating attack innovation.

With respect to RQ2: "What is the impact of these changes on the TTPs adopted by ransomware groups?", the study highlights a 40% shift in the top ransomware techniques between 2023 and 2024, illustrating the rapid evolution of adversary tactics. The introduction of T1657: Financial Theft signifies a broader shift toward data exfiltration and extortion strategies, reducing reliance on traditional encryption-based attacks. Additionally, ransomware groups have expanded their initial access techniques, demonstrating a preference for exploiting public-facing vulnerabilities (T1190) over credential-based intrusions. Defense evasion techniques have also grown more sophisticated, with rootkits (T1014) and encryption-based obfuscation (T1211) playing a central role. Meanwhile, double extortion remains the predominant impact strategy, reinforcing the growing emphasis on leveraging stolen data as a coercive mechanism.

In conclusion, the findings underscore the dynamic and adaptive nature of ransomware groups and show that recent changes in the ecosystem are not merely incremental variations in tooling, but reflect broader shifts in attacker economics, operational models, and technology use. By combining a longitudinal comparison of ransomware TTPs with ATT&CK-based mitigation prioritization, this paper contributes a structured view of how ransomware behavior evolved between 2023 and 2024 and why these changes matter for defense. The results further suggest that ransomware analysis should move beyond purely descriptive reporting toward explanatory models that link technical behavior to socio-technical drivers. For practitioners, this means that mitigation strategies should be continuously re-prioritized in response to changing attacker behavior. For researchers, it highlights the value of studying ransomware as an evolving ecosystem rather than as a fixed malware category.

References

[1] J. W. Han, O. J. Hoe, J. S. Wing, and S. N. Brohi, "A conceptual security approach with awareness strategy and implementation policy to eliminate ransomware," in *Proceedings of the 2017 international conference on computer science and artificial intelligence*, 2017, pp. 222–226.

[2] N. Ariffin, A. Zainal, M. A. Maarof, and M. N. Kassim, "A conceptual scheme for ransomware background knowledge construction," in *2018 Cyber Resilience Conference (CRC)*. IEEE, 2018, pp. 1–4.

[3] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention," *Information Systems Security*, vol. 16, no. 4, pp. 195–202, 2007.

[4] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, 2019.

[5] A. Lawall and P. Beenken, "A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem," in *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, ser. EICC '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 210–216. [Online]. Available: https://doi.org/10.1145/3655693.3661321

[6] MITRE, "MITRE ATT&CK™: Adversarial Tactics, Techniques, and Common Knowledge," 2023, retrieved from https://attack.mitre.org/.

[7] National Institute of Standards and Technology (NIST), "Small business cybersecurity corner," NIST Cybersecurity Framework, Version 2.0, 2023, retrieved from https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware.

[8] B. Fisher, M. Souppaya, W. Barker, and K. Scarfone, "Ransomware risk management: A cybersecurity framework profile," 02 2022. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934219

[9] D.-K. Kipker and M. Barudi, *Cybersecurity - Rechtshandbuch*. München: C.H. Beck, 2020.

[10] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," *International Management Review*, vol. 13, no. 1, p. 10, 2017.

[11] F. Maymi and S. Harris, *CISSP All-in-One Exam Guide, Ninth Edition* -. Madison: McGraw Hill Professional, 2021.

[12] H. A. Shakir and A. N. Jaber, "A short review for ransomware: pros and cons," in *Advances on P2P, Parallel, Grid, Cloud and Internet Computing: Proceedings of the 12th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2017)*. Springer, 2018, pp. 401–411.

[13] R. Moussaileb, N. Cuppens, J.-L. Lanet, and H. L. Bouder, "A survey on windows-based ransomware taxonomy and detection mechanisms," *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–36, 2021.

[14] S. Jimada, T. D. L. Nguyen, J. Sanda, and S. K. Vududala, "Analysis of ransomware, methodologies used by attackers and mitigation techniques," in *Research in Intelligent and Computing in Engineering: Select Proceedings of RICE 2020*. Springer, 2021, pp. 379–387.
[15] A. Kovács, "Ransomware: a comprehensive study of the exponentially increasing cybersecurity threat," *Insights into Regional Development*, vol. 4, no. 2, pp. 96–104, 2022.
[16] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys (CSUR)*, vol. 48, no. 3, pp. 1–39, 2015.
[17] A. Zimba and M. Chishimba, "Understanding the evolution of ransomware: paradigm shifts in attack structures," *International Journal of computer network and information security*, vol. 11, no. 1, p. 26, 2019.
[18] V. Malik, A. Khanna, N. Sharma *et al.*, "Trends in ransomware attacks: Analysis and future predictions," *International Journal of Global Innovations and Solutions (IJGIS)*, 2024.
[19] J. Martin and C. Whelan, "Ransomware through the lens of state crime: Conceptualizing ransomware groups as cyber proxies, pirates, and privateers," *State Crime J.*, vol. 12, p. 4, 2023.
[20] S. Razaulla, C. Fachkha, C. Markarian, A. Gawanmeh, W. Mansoor, B. C. Fung, and C. Assi, "The age of ransomware: A survey on the evolution, taxonomy, and research directions," *IEEE Access*, vol. 11, pp. 40 698–40 723, 2023.
[21] A. Bello and A. Maurushat, "Technical and behavioural training and awareness solutions for mitigating ransomware attacks," in *Applied Informatics and Cybernetics in Intelligent Systems: Proceedings of the 9th Computer Science On-line Conference 2020, Volume 3 9*. Springer, 2020, pp. 164–176.
[22] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks," *Applied clinical informatics*, vol. 7, no. 02, pp. 624–632, 2016.
[23] J. Thomas and G. Galligher, "Improving backup system evaluations in information security risk assessments to combat ransomware," *Computer and Information Science*, vol. 11, no. 1, 2018.
[24] A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, "Ransomware detection, avoidance, and mitigation scheme: a review and future directions," *Sustainability*, vol. 14, no. 1, p. 8, 2021.
[25] National Institute of Standards and Technology (NIST), "The nist cybersecurity framework 2.0," NIST Cybersecurity Framework, Version 2.0, 2023, retrieved from https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd.
[26] A. Kharraz and E. Kirda, "Redemption: Real-time protection against ransomware at end-hosts," in *Research in Attacks, Intrusions, and Defenses: 20th International Symposium, RAID 2017, Atlanta, GA, USA, September 18–20, 2017, Proceedings*. Springer, 2017, pp. 98–119.
[27] P. Kral, "The incident handlers handbook," *Sans Institute*, 2011.
[28] P. Cichonski, T. Millar, T. Grance, K. Scarfone *et al.*, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, no. 61, pp. 1–147, 2012.
[29] Z. A. Collier, D. DiMase, S. Walters, M. M. Tehranipoor, J. H. Lambert, and I. Linkov, "Cybersecurity standards: Managing risk and creating resilience," *Computer*, vol. 47, no. 9, pp. 70–76, 2014.
[30] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of cybersecurity standard and framework components," *International Journal of Communication Networks and Information Security*, vol. 12, no. 3, pp. 417–432, 2020.
[31] R. Dantu, P. Kolan, and J. Cangussu, "Network risk management using attacker profiling," *Security and Communication Networks*, vol. 2, no. 1, pp. 83–96, 2009.