Threat Modeling a Ransomware Attack on a Wallpaper Manufacturer

Carlos Colón Rivera
Department of Engineering, Leadership and Program Management
The Citadel
Charleston, USA
carlos.colonrivera2@gmail.com

Trevor Richie
Department of Computer Science
College of Charleston
Charleston, USA
ritchiets@g.cofc.edu

***Abstract*— Ransomware attacks pose a critical threat from large to small businesses, which often lack the resources to defend against sophisticated adversaries [1] [2]. This paper presents a comprehensive case study of a real-world ransomware incident perpetrated by the Akira threat actor group against a U.S.-based wallpaper distribution business in July 2025 [3]. We conducted a retrospective, data-centric threat model to deconstruct the attack vector and identify the specific security vulnerabilities that were exploited. The methodology involved mapping the adversary's tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK framework and analyzing indicators of compromise to reconstruct the intrusion timeline. The primary contribution of this research was a detailed threat analysis and a strategic risk mitigation plan that provides actionable security countermeasures. By demonstrating how proactive threat modeling could have preempted this attack, this work served as a practical framework for businesses to enhance their cybersecurity posture and build resilience against prevalent ransomware threats.**

Index Terms — Akira, Ransomware, Threat Modeling, Risk Management, Cyber Threat Emulation

I. Introduction

The manufacturing sector has emerged as a high-priority target for financially motivated cybercriminals, driven by the industry's acute sensitivity to operational downtime [4]. Unlike purely administrative environments, manufacturers rely on the continuous availability of Operational Technology (OT), where even minor disruptions result in immediate and quantifiable revenue loss [5]. This 'availability dependency' makes Small and Medium-Sized Enterprises (SMEs) in this vertical attractive targets for ransomware groups like Akira, who exploit the gap between sophisticated threat tradecraft and the limited defensive resources typical of smaller organizations [1] [2]. This vulnerability was starkly illustrated on July 1, 2025, when the operations of Roysons Corporation were paralyzed by a targeted intrusion [3]. The incident serves as a critical example of how traditional perimeter-based defenses often fail to protect the hybrid IT-OT workflows essential to modern production."

The Akira ransomware group emerged as a prolific and financially motivated adversary [6]. Since its appearance in March 2023, Akira targeted a wide range of businesses and critical infrastructure entities across North America, Europe, and Australia [2]. According to the joint CISA and FBI advisory, #StopRansomware: Akira Ransomware, the group had impacted over 250 organizations and extorted approximately $42 million in ransomware payments as of January 2024 [2] [7]. Their tactics, techniques, and procedures (TTPs) often involved exploiting common vulnerabilities in network perimeter devices, such as the Cisco VPN vulnerability identified as CVE-2023-20269, to gain initial access before deploying their ransomware payload [8].

To counter such advanced threats, organizations must shift from a reactive to a proactive security posture [2]. A cornerstone of this proactive approach is threat modeling, a structured process for identifying potential threats, vulnerabilities, and attack vectors from an attacker's perspective [9] [10]. By systematically analyzing a system's design, data flows, and trust boundaries, threat modeling allows security professionals to anticipate how an adversary might compromise a system [10]. Its importance lies in its ability to inform security decisions early in the development lifecycle, prioritize defensive resources against the most likely and impactful threats, and ultimately reduce the attack surface before an incident can occur [9].

Increasingly, simply following general "best practices" for security is insufficient for safeguarding high-value data [11]. This inadequacy is demonstrated by major incidents, such as the 2013 Target data breach, where cyber thieves stole the financial and personal information of up to 110 million customers [12]. The subsequent analysis revealed that Target missed a number of opportunities along the intrusion kill chain to stop the attackers. Specifically, Target failed to respond to multiple automated warnings from its anti-intrusion software about the installation of malware and the subsequent exfiltration of stolen data [12].

A similar failure occurred in the case of Roysons Corporation [3] [13]. The unauthorized actor successfully gained initial access on May 26, 2025, and maintained persistent access for over a month before the final impact phase on July 1, 2025. This prolonged dwell time, enabled initially by the exploitation of a Virtual Private Network (VPN) service that lacked multifactor authentication (MFA), confirmed that reliance on general vulnerability patching and checklist compliance was not robust enough to protect unique, high-value systems [6]. Both cases highlighted the need for a proactive approach that prioritized data protection over generalized host security.

Therefore, this project employed data-centric system threat modeling using NIST SP 800-154 [14]. This methodology

allowed us to shift the focus from merely preventing host compromise to protecting specific, critical data assets (such as the design files that were encrypted) by analyzing attack vectors relevant to those assets, thereby achieving demonstrably better security for data of particular importance.

This project conducted a retrospective threat model of the Akira ransomware attack on Roysons Corporation [3] [13]. The primary objective was to demonstrate how preemptive threat modeling could have identified the security gaps that were exploited and potentially prevented the attack. Uniquely, this research leverages proprietary forensic data and internal incident response logs that are not publicly available.

While general advisories regarding the Akira group exist, this study contributes a novel, granular perspective by validating specific TTPs against an actual, documented compromise. This privileged access enables a direct comparison between theoretical threat intelligence and empirical reality. The findings not only offer a roadmap for enhancing the security posture of Roysons Corporation but also serve as a valuable case study for other businesses facing similar cyber threats.

II. Literature Review

A. Technical Characterization and Cryptographic Efficiency

Recent literature has moved beyond general ransomware definitions to focus on the specific structural evolution of threats like Akira. A consensus across forensic analyses establishes Akira as a highly sophisticated "hybrid" threat that prioritizes execution speed and evasion over complex propagation mechanisms [15] [16] [7] [17].

Desai and Shingadiya provide the foundational static and dynamic analysis of the Akira binary, revealing a reliance on custom packing and high-entropy obfuscation (7.8 in .text sections) to defeat traditional signature-based detection [15]. Their forensic deconstruction identified the malware's persistence mechanisms—specifically the deletion of shadow copies via vssadmin and the use of the Global\AkiraMutex to prevent re-infection [7]. However, while Desai focuses on the binary structure, other researchers have isolated the operational drivers of its success.

The primary driver of Akira's impact is its encryption speed, achieved through a specific cryptographic implementation. Dzahabi, Hayaty, and Bettiza (2025) analyzed the implementation of the ChaCha20 stream cipher wrapped with RSA-4096 asymmetric encryption [16]. By synthesizing their findings with Desai's forensic data, it becomes clear that Akira's choice of ChaCha20 is not arbitrary; it is a strategic decision to maximize file-corruption speed before defensive automated interrupts can trigger. This confirms that the "window of opportunity" for defenders is significantly smaller against Akira than against older variants using standard AES encryption.

B. Limitation of Current Detection Frameworks

Despite the theoretical advancements in ransomware containment, a significant gap remains in real-time detection for "living-off-the-land" attacks. Recent proposals by Khaliq et al. (2024) suggest a two-phase layered framework that isolates suspicious files in a virtual machine (VM) upon signature recognition by Kaspersky-based tools [17]. While this "Isolation and Prevention" model effectively neutralizes standard malware payloads, it relies entirely on the initial signature match (Phase 1). This dependency renders the framework ineffective against the specific tradecraft employed by the Akira group, who often bypass malware scanning entirely by abusing valid VPN credentials (CVE-2023-20269) rather than deploying executable files at the perimeter [2] [18]. Consequently, purely technical detection frameworks like that of Khaliq et al. often fail to account for the logical access vulnerabilities—such as the lack of MFA—that constitute the actual attack vector in incidents like the Roysons Corporation breach.

C. From System-Centric to Data-Centric Threat Modeling

Historically, threat modeling methodologies such as STRIDE have prioritized the identification of software vulnerabilities within the application development lifecycle [10]. While effective for secure coding, these system-centric approaches often fail to account for the post-exploitation behaviors characteristic of modern ransomware.

To bridge this gap, the industry has increasingly adopted the MITRE ATT&CK framework to map adversary behaviors rather than just static signatures [19] [2] [20]. Research by Thamsongkrah emphasizes that mapping TTPs—such as the "Valid Accounts" technique (T1078) used by Akira—provides a more accurate risk picture than vulnerability scanning alone. However, behavior-based models still primarily focus on detecting the adversary on the network, rather than preventing access to critical assets.

This limitation necessitates a shift toward Data-Centric System Threat Modeling, as defined in NIST SP 800-154 [11]. Unlike system-centric models that ask, "How do we stop the hacker from entering the network?", the data-centric approach asks, "How do we stop the hacker from reading or encrypting this specific file?" [9] [11] [21]. This distinction is critical for the Roysons Corporation case; the adversary had valid network access (rendering boundary defenses moot), but a data-centric model would have flagged the lack of access controls on the specific design file servers as a critical failure point [3].

III. Methodology

The research methodology for this project was structured as a comprehensive case study, analyzing a real-world cyber incident to develop a robust security framework. The approach was systematically organized into five distinct phases: data acquisition and sanitization, data-centric threat modeling, attack vector analysis, cyber threat emulation, and the formulation of a strategic risk mitigation plan.

A. Data Acquisition and Sanitization

The initial phase of this research involved gaining access to internal company documentation related to the Akira ransomware attack on Roysons Corporation. This primary source material provided a detailed account of the incident,

including forensic timelines, affected systems, and initial response efforts [3] [13] [22]. To ensure confidentiality and adhere to ethical research standards, all identifying information pertaining to the organization's personnel and specific system identifiers was systematically redacted [14]. Although the company granted full permission to utilize its story, this sanitization process was critical for protecting the confidentiality of the affected entity while preserving the core technical data necessary for analysis.

B. Data-Centric Threat Modeling

Following data preparation, a data-centric system threat model was developed using NIST SP 800-154, Guide to Data-Centric System Threat Modeling. Unlike traditional network - centric models, this approach prioritized the identification of high-value data assets - specifically the Core Intellectual Property (Digital Art Design Files) and OT control systems. The process involved creating logical data flows diagrams to map the movement of these critical assets across trust boundaries. By adopting this perspective, the analysis focused on protecting the most valuable information, allowing for a targeted assessment of vulnerabilities relative to the specifics business impact of the Akira attack vector [11].

C. Attack Vector and IOC Analysis

To deconstruct the mechanics of the intrusion, the attack was systematically mapped to the MITRE ATT&CK framework. This process involved correlating the specific actions taken by the threat actor – such as the exploitation of the VPN (T1133) and the abuse of valid accounts (T1078) – with known TTPs cataloged in the ATT&CK knowledge base. Concurrently, a thorough analysis of the available Indicators of Compromise (IOCs), including malicious IP addresses and file hashes, was conducted. This dual analysis resulted in the creation of an "Akira Heat Map", which provided a granular understanding of the adversary's behavior and furnished the empirical data needed to develop effective detection strategies [23] [19].

D. Cyber Threat Emulation and Validated Defense Verification

To bridge the gap between theoretical analysis and operational reality, a Cyber Threat Emulation environment was constructed to mimic the Roysons Corporation network. The infrastructure was virtualized using GNS3 for network emulation and VMware Workstation Pro for host virtualization. The emulation environment included a reproduction of the firewall, domain controller, file servers, and the specific ESXi infrastructure targeted in the actual attack.

Adversary behaviors were simulated using a Kali Linux attack platform to execute the specific TTPs identified in the forensic report, including the use of netscan for discovery and WinRAR for data staging [24]. To measure defensive efficacy, a Security Onion instance was deployed as a Standalone Security Operations Center (SOC) node [25]. This allowed for the collection of PCAP data and endpoint logs (via Wazuh and Zeek) to calculate specific metrics, including Detection Rate (True Positive Rate), Mean Time to Detect (MTTD), Log/Data completeness and False Positive Rate.

To expand the scope of validation beyond the specific Akira incident and address other high-risk vectors identified in the threat model, the research utilized high-fidelity malicious packet captures (PCAPs) obtained from Malware-Traffic-Analysis.net and The Open University. These datasets allowed for the testing of complex infection chains and infrastructure attacks that were difficult to synthesize manually.

E. Risk Mitigation and Strategy Development

In the final phase, the findings from the threat model and attack analysis were synthesized to prepare a comprehensive Risk Mitigation Plan. This plan translated the analytical findings into actionable security improvements. It will identified specific vulnerabilities exploited during the incident – such as the lack of MFA and the exposure of the ESXi management interface – and proposed concrete countermeasures, procedural adjustments, and technology enhancements. The recommendations were designed to not only remediate the specific weaknesses that enabled the Akira ransomware attack but also to elevate the organization's overall security posture against future, similar threats [26].

IV. Results

This project yielded a multi-faceted security analysis to understand the events of the ransomware attack and to enhance the company's resilience against further cyber threats. The findings are detailed in the following subsections.

A. Forensic Analysis and MITRE ATT&CK Mapping

The systematic deconstruction of the Akira ransomware incident against Roysons Corp. was achieved by mapping the forensic timeline directly onto the MITRE ATT&CK for Enterprise framework. This framework is critical for structuring the adversary's actions based on Tactics (the technical objective or "why") and Techniques (the specific operational method or "how"). The analysis presented synthesizes the procedural details extracted from the MOXFIVE forensic investigation with the globally established lexicon of threat actor behaviors. By applying this model, the security gaps exploited by the threat actors are isolated and contextualized, providing an explicit roadmap of the intrusion—from the initial perimeter breach to the final impact.

The observed intrusion spanned over a month, beginning with the successful Initial Access (TA0001) on May 26, 2025, and culminating in the Impact (TA0040) phase on July 1, 2025. Forensic evidence confirmed that the unauthorized actor achieved initial entry by exploiting a VPN service that conspicuously lacked MFA, a technique categorized as External Remote Services (T1133). Following this entry, the adversary leveraged Credential Access (T1078) and employed legitimate, commonly available tools—such as the SoftPerfect Network Scanner (T1046) for Discovery (TA0007),—to move laterally and map the environment.

Prior to encryption, the actor executed a series of Defense Evasion techniques, including disabling Windows Defender via PowerShell commands (T1562.001), and used WinRAR for suspected Data Staging (T1560.001) in preparation for exfiltration under a double-extortion model. The final phase involved the execution of the Akira binary, w.exe, which utilized a sophisticated hybrid encryption scheme (T1486), and

manually or automatically deleted volume shadow copies (T1490) to Inhibit System Recovery. The following analysis maps actions to their (sub)techniques.

1) Initial Access (TA0001)

External Remote Services (T1133)

The threat actor gained initial access by logging into the Client's VPN using the account employee1@Firebox-DB from the IP address 77.247.126.239 on May 26, 2025, at 13:26 UTC. This VPN lacked MFA.

2) Credential Access (TA0006)

Valid Accounts (T1078)

Existing accounts were compromised and abused throughout the attack. Specifically, the accounts compromised were: the domain administrator account COMPANY\administrator and two Firebox user accounts (employee1@Firebox-DB and employee2@Firebox-DB). The domain administrator account was used for lateral movement and execution of malicious tools.

3) Lateral Movement (TA0008)

Remote Services: Remote Desktop Protocol (T1021.001)

The threat actor leveraged the Domain Administrator account (COMPANY\administrator) to move laterally from their VPN-connected host into the Client's environment by establishing RDP sessions.

4) Discovery (TA0007)

Network Service Scanning (T1046)

The threat actor conducted reconnaissance by executing legitimate network scanning tools: `Advanced_Port_Scanner_2.5.3869.exe` (at 07:03 UTC) and `netscan_n.exe` (SoftPerfect Network Scanner, at 07:33 UTC) on the host RC-DC-01. These tools are used to map the network, identify active hosts, and locate high-value systems.

File and Directory Discovery (T1083)

Following the execution of the port scanner, the actor accessed a file named shares.txt (located in C:\ProgramData and created shortly after the scan began), strongly suggesting the file contained the scan's output (details on discovered hosts, open ports, or shared resources).

5) Collection (TA0009)

Archive Collected Data: Archive via Utility (T1560.001)

The threat actor installed and executed the WinRAR file archiving program on the host RC-RDS-03-2016 (at 07:19 UTC). WinRAR is a common tool used by threat actors to collect and compress data for faster exfiltration [5] [6].

6) Defense Evasion (TA0005)

Impair Defenses: Disable or Modify Tools (T1562.001)

The threat actor executed a series of PowerShell commands to severely impact or disable Windows Defender's ability to detect and prevent malicious software (e.g., disabling real-time monitoring, behavior monitoring, and archive scanning) on SERVER-NX3230 (at 08:13 UTC) and SERVER-PE750xs. This ensured the successful deployment of the ransomware binary.

7) Execution (TA0002)

Command and Scripting Interpreter: PowerShell (T1059.001)

PowerShell was used to execute commands, specifically to disable Windows Defender features and to delete Volume Shadow Copies. The use of PowerShell allows malicious actions to blend with normal administrative activity.

User Execution: Malicious File (T1204.002)

The threat actor executed the Akira ransomware binary named `w.exe` at 09:00 UTC on the host RC-DC-01, initiating the final impact phase.

8) Impact (TA0040)

Data Encrypted for Impact (T1486)

The execution of the w.exe ransomware binary resulted in files being encrypted and appended with the signature extension `.akira` across multiple hosts. Akira uses a sophisticated hybrid encryption scheme combining the fast ChaCha20 stream cipher with RSA public-key encryption for key exchange.

Inhibit System Recovery (T1490)

The ransomware binary w.exe explicitly executed a PowerShell command (`Get-WmiObject Win32_Shadowcopy

9) Comparison to Established Akira TTPs

Now, we compare the Akira ransomware attack on Roysons Corp. to the published TTPs associated with the Akira threat group, including documentation from the official MITRE ATT&CK website and detailed advisories. Our analysis explicitly links Roysons' procedural facts to these external reports, demonstrating where the attack mirrored Akira's established methodology and where operational differences were observed.

10) Procedural Similarities with Known Akira TTPs

The attack demonstrated a strong adherence to the established operational blueprint utilized by the Akira ransomware group. Initial Access (T1133) was gained by exploiting a VPN service that conspicuously lacked MFA. This aligns with the primary initial access vector documented in the HC3 Sector Alert and the CISA/FBI Joint CSA, which explicitly notes that Akira uses compromised VPN accounts for initial access where MFA is not configured [6] [27]. The MITRE ATT&CK webpage for Akira confirms that the threat group utilizes External Remote Services (T1133) with compromised VPN accounts [28]. Once inside, the subsequent use of compromised Domain Administrator credentials (COMPANY\administrator) utilized the Valid Accounts technique (T1078), which the MITRE ATT&CK page lists as a core Akira technique to access critical network resources.

For reconnaissance, the adversary employed sophisticated Living Off the Land (LotL) techniques (T1018), relying on legitimate administrative tools. The threat actor utilized SoftPerfect Network Scanner (netscan_n.exe) and Advanced IP Scanner (Advanced_Port_Scanner_2.5.3869.exe). The MITRE ATT&CK page specifically links Akira to the use of both Advanced IP Scanner and MASSCAN (T1018) to identify remote hosts [28]. Similarly, the CISA/FBI Joint CSA also lists both SoftPerfect and Advanced IP Scanner as tools leveraged by Akira for network device discovery (T1016) [6]. Lateral Movement (T1021.001) was executed via RDP sessions, a technique confirmed by the MITRE ATT&CK page and an

Insurance Data Management Association (IDMA) Advisory [28] [29].

The collection phase demonstrated consistent double-extortion preparation. The installation and execution of the WinRAR file archiving program, aligns directly with the documented Archive Collected Data: Archive via Utility TTP (T1560.001), which is listed on the MITRE ATT&CK page as being used to archive data for exfiltration [28]. The CISA/FBI Joint CSA confirms Akira actors leverage WinRAR to compress files into .RAR format [6]. For Defense Evasion (T1562.001), the actor executed PowerShell commands (T1059.001) to disable Windows Defender functionality, a common technique explicitly observed by trusted third-party investigations and listed as Impair Defenses (T1562.001) in the list of techniques used by Akira [28].

The Impact phase was a definitive match for the original C++ Akira variant. The encryptor deployed was the recognized binary w.exe, appending the signature .akira extension to encrypted files. The CISA/FBI Joint CSA specifies that the encryption mechanism used is a hybrid scheme (T1486) combining the ChaCha20 stream cipher with RSA public-key encryption [6]. Crucially, the encryptor utilized the specific PowerShell command: Get-WmiObject Win32_Shadowcopy | Remove-WmiObject to delete Volume Shadow Copies (VSS) (T1490). This is listed in the CISA/FBI Joint CSA, and confirmed by Arete as the method used to inhibit system recovery [6] [7].

11) Observed Differences from Published Akira TTPs

While the high-level tactics were consistent, the specific technologies targeted for initial compromise provided a point of differentiation. The CISA/FBI Joint CSA and the HC3 Analyst Note heavily emphasize Akira actors exploiting specific vulnerabilities in Cisco Adaptive Security Appliance (ASA) VPN products to gain initial access [6] [27]. However, in the Roysons incident, the attacker exploited a WatchGuard VPN instance which lacked MFA [3]. This distinction confirms that while the goal remains exploiting weak External Remote Services (T1133), the threat group is vendor-agnostic, targeting any remote access point lacking the requisite MFA security control.

A second distinction lies in the observed sequencing of Credential Access (T1003). Akira is known to commonly leverage post-exploitation tools such as Mimikatz and LaZagne to dump Local Security Authority Subsystem Service (LSASS) process memory (T1003.001) and extract credentials [6]. In the Roysons case, the forensic report showed that lateral movement immediately relied on the use of compromised Domain Administrator account (COMPANY\administrator). Although the capability for LSASS dumping is likely present, the fast cracking of the highest-level credentials meant the attackers' strategy prioritized the direct use of Valid Accounts (T1078) to move laterally and execute commands, potentially bypassing or accelerating the typical post-exploitation credential acquisition phase detailed in the HC3 Sector Alert and CISA/FBI Joint CSA [27] [6].

Finally, the variant used in the Roysons attack, identified by the .akira extension and the binary w.exe, was the older C++ variant. This contrasts with the emergence of the Rust-based Megazord variant (which uses the .powerranges extension) [6]. However, the IMDA Advisory indicated that Akira had been observed pivoting back to the original .akira C++ tactics later in their evolution, confirming the operational flexibility of the threat group in deploying variants [29].

B. Data-Centric Threat Modeling Findings

The next objective of this research is to transition from a reactive, incident-based analysis to a proactive, generic threat model. As outlined in the methodology (Section III), this process utilizes the NIST SP 800-154 "Guide to Data-Centric System Threat Modeling." This approach mandates that the system's most valuable data and assets are identified first, and that security controls are then prioritized to protect them. This "crown jewel" analysis provides the foundation for the mitigation plan that follows.

1) Identification of High-Value Assets

Based on an analysis of the organization's business model (a wallpaper manufacturer) and its network infrastructure, three high-value asset categories were identified. These assets, listed below, are the primary targets for an adversary, as their compromise maps directly to significant business impact.

a) Core Intellectual Property (Digital Art Design Files)

This asset category, stored on the organization's file servers, represents the company's core intellectual property. The primary security objectives for this asset are Confidentiality and Integrity. A breach of confidentiality (e.g., data exfiltration for industrial espionage) would result in a severe loss of competitive advantage. A breach of integrity (e.g., unauthorized modification of design files) would result in manufacturing errors, product loss, and reputational damage.

b) Operational Technology (Production Machinery)

This asset category includes the printers, laminators, and associated control systems used in the manufacturing process. The primary security objective for this asset is Availability. As identified in the risk analysis, an adversary who gains access to these systems could halt production entirely. This DoS scenario translates to an immediate, direct, and quantifiable financial loss for every hour of downtime.

c) Virtualization Infrastructure (VMware ESXi / vCenter)

This infrastructure is a high-value asset because it serves as a "force multiplier" for an adversary. It is the platform upon which the other two assets (File Servers and OT control systems) operate. The primary security objectives for this asset are Integrity and Availability. A compromise of the hypervisor (ESXi) or the management plane (vCenter) would allow an adversary to bypass all guest-level security controls, encrypt the entire server fleet simultaneously, and inflict catastrophic, organization-wide damage.

2) Threat-Asset Mapping

By mapping adversary tactics (STRIDE, MITRE ATT&CK) to these high-value assets, a prioritized list of likely attack vectors emerges.

a) Threats to Files

An adversary will target Confidentiality and Integrity. This leads to threats like Data Exfiltration (T1560) and Data Encrypted for Impact (T1486).

b) Threats to OT

An adversary will target Availability. This leads to threats like Endpoint Denial of Service (T1499) or Impair Defenses (T1562) on the control systems.

c) Threats to VM Infrastructure

An adversary will target Integrity and Availability at a systemic level. This leads to high-impact threats like Exploitation for Privilege Escalation (T1068) via the ESXi AD bypass (CVE-2024-30078) or a Network Denial of Service (T1499) against the vCenter server (CVE-2024-37087).

The specific mitigation controls detailed in the following section are a direct response to these identified high-impact, asset-centric threats.

C. Cyber Threat Emulation and Validated Defense Verification

To bridge the gap between theoretical analysis and operational reality, the Cyber Threat Emulation phase provided quantitative evidence regarding the efficacy of the proposed sensor placement and detection rules. By replaying specific attack vectors within the virtualized environment, the project measured the system's ability to detect both the specific Akira TTPs and broader high-risk threats.

1) Metric Analysis and Log Completeness

The deployment of Security Onion provided 90% visibility into the network flows of the emulated attacks. As evidenced by the metric timelines, the sensors successfully captured high-volume event spikes corresponding to the scanning activities (endpoint.events.network) and file modifications (endpoint.events.file). This visibility established a quantifiable baseline for the "Mean Time to Detect" (MTTD), confirming that the log aggregation strategy was sufficient to reconstruct the attack chain.

2) Validation of Credential Access Detection (Emotet/Trickbot)

To validate detection capabilities against sophisticated Command-and-Control (C2) channels—a critical gap in the original incident—the research utilized a high-fidelity PCAP containing an Emotet/Trickbot infection. Upon ingestion, the Suricata NIDS successfully triggered a high-severity alert: "ET MALWARE Trickbot Checkin Response". Subsequent forensic analysis of the packet capture confirmed that the sensors correctly isolated the C2 communication to the external malicious IP 170.238.117.187 over TCP port 8082. This validated that the proposed network monitoring architecture could detect encrypted C2 traffic that bypassed endpoint controls.

3) Validation of Infrastructure Denial of Service

The emulation of the vCenter Network Denial of Service (CVE-2024-37087) demonstrated that the proposed rate-limiting rules effectively distinguished between benign administrative heartbeats and malicious service exhaustion attempts. The analysis of the "HTTP DoS" dataset confirmed that the sensors could identify the anomalous traffic volume and alert the Security Operations Center (SOC) before a complete service outage occurred.

D. Strategic Risk Mitigation Plan

The retrospective analysis of the Akira ransomware incident (Sections V and VI) highlights a reactive security posture that relied on post-incident forensics. To transition to a proactive framework, this section proposes a generic, data-centric risk mitigation plan derived from the threat model. This plan prioritizes the organization's most valuable and high-impact assets, grouping them by foundational services, core business value, and the underlying infrastructure. The goal is to build resilience against a wide spectrum of post-compromise adversaries, not just the TTPs of a single threat group.

1) Mitigating Virtualization Infrastructure Compromise

The hypervisor and its management plane are the "crown jewels" of the network. A compromise at this layer is catastrophic, as it allows an attacker to bypass all guest-level security controls (e.to, EDR, antivirus) and encrypt or destroy all virtual workloads simultaneously.

a) ESXi Authentication Bypass (CVE-2024-37085)

A critical vulnerability (CVE-2024-37085) was identified in the ESXi Active Directory (AD) integration. An attacker who has already gained Domain Administrator credentials—a common prerequisite in enterprise intrusions—can recreate a default, deleted AD group (e.g., 'ESX Admins') to gain full, root-level administrative access to the hypervisor [30].

The primary mitigation is to apply the vendor-supplied patch (e.g., ESXi 8.0 U3) immediately. However, this must be layered with a compensating control to detect the exploit attempt. A high-fidelity detection rule must be implemented in the Security Information and Event Management (SIEM) platform. This rule monitors Windows Event Logs (Event ID 4727 or 4731: "A security-enabled group was created") and triggers a critical alert if the TargetUserName field is 'ESXi Admins'.

b) vCenter Denial of Service (CVE-2024-38087)

The vCenter Server, as the central management plane, is susceptible to a network-based Denial of Service (DoS) attack (CVE-2024-38087). While this vulnerability does not exfiltrate data, its impact during an active intrusion is severe. It cripples the incident response team's ability to use vCenter for defensive actions such as isolating compromised VMs, restoring from snapshots, or migrating workloads. This effectively blinds the administration team.

Remediation requires patching the vCenter Server appliance (e.g., vCenter Server 8.0 U3). This should be augmented with network-based controls. An Intrusion Detection System (IDS) such as Suricata should be configured with rate-based rules to detect and alert on anomalous connection floods or malformed packets targeting the vCenter management interface (typically TCP/443).

2) Mitigating IoT and Legacy System Exploitation

The threat model identified legacy IoT hardware—specifically the Cisco Video Surveillance Manager—as a high-risk, low-visibility asset. These devices are often unpatched,

unmonitored, and provide an ideal "shadow" foothold for an adversary.

a) Cisco Video Surveillance Manager (CVE-2013-3429)

This legacy device is vulnerable to a directory traversal attack (CVE-2013-3429). An unauthenticated attacker with network access can exploit this input validation failure to access arbitrary system files. This would likely include configuration files containing credentials, network maps, or other sensitive data. Such a device allows an adversary to establish persistent, long-term network access that is invisible to modern EDR solutions focused on standard Windows and Linux hosts.

Given that patching legacy firmware is often unfeasible, the primary mitigation strategy is network segmentation. The surveillance devices must be isolated on a restricted "IoT" VLAN. Firewall rules must be implemented to deny all access from the general corporate LAN, permitting access only from a single, hardened management jump box. This isolation acts as a "virtual patch" and can be enforced by NIDS signatures (e.g., in Zeek or Suricata) configured to detect and block URI traversal patterns (../) targeting this device's web interface.

3) Protecting Core Business Assets

With foundational services hardened, the focus shifts to the primary targets of an attack: the core intellectual property (IP) and the operational technology (OT) required for production.

a) Protecting Core Intellectual Property (File Servers)

For a wallpaper manufacturer, the digital art design files constitute the core IP. The primary threat is data exfiltration for industrial espionage, which impacts both confidentiality (loss of IP) and integrity (unauthorized modifications causing manufacturing errors).

An attacker with compromised credentials can use legitimate tools (e.g., RDP, PowerShell) to browse file shares, aggregate data, and use common archiving utilities (e.g., WinRAR, 7-Zip) to compress the files for exfiltration. This "living off the land" technique blends malicious activity with normal administrative behavior.

Mitigation requires a layered approach. First, data loss prevention (DLP) endpoints on the file server can help classify the data and block unauthorized transfer. Second, HIDS (e.g., Wazuh) rules must be implemented to monitor for suspicious process creation events. An alert should be generated when a non-standard process (like WinRAR.exe) is executed by a service account or from a network share, or when command-line arguments consistent with mass archival (-p, .zip) are used. This provides high-fidelity detection of data staging.

4) Securing Operational Technology (Production Machinery)

The production machinery (printers, laminators) is a critical asset where the primary risk is to availability. An attacker gaining access to the manufacturing control systems can halt production, leading to immediate and significant financial loss.

The threat vector identified is lateral movement from the corporate network. An adversary, having gained RDP access via compromised administrator credentials, can pivot from the domain controller into the OT network segment. They can then use administrative tools (e.g., PowerShell) to interfere with the specialized software controlling the machinery.

The primary mitigation is robust network segmentation. The OT network must be segregated from the corporate IT network via a firewall, with strict rules that deny all traffic by default. Only specific, required protocols from a hardened management jump box should be permitted. Compensating controls should include HIDS monitoring on the OT control systems for any unexpected service stops, configuration changes, or the execution of non-standard binaries.

5) Hardening Foundational Services

An adversary's success is dependent on compromising identity and defeating recovery. Securing Active Directory (AD) and system backups is the first and most critical line of a defense-in-depth strategy.

a) Persistent Credential Theft (Active Directory)

An adversary who compromises Active Directory can dump credentials from the LSASS process (T1003.001) or create hidden domain accounts (T1136.002) to ensure long-term persistence, even after known-compromised accounts are reset.

Mitigation involves enabling Attack Surface Reduction (ASR) rules on Windows 10/11 to secure LSASS and prevent credential stealing. Furthermore, HIDS monitoring (e.g., Sysmon Event ID 10) must be configured to alert when a non-standard process (i.e., not svchost.exe) attempts to access lsass.exe memory, which is a strong indicator of a tool like Mimikatz.

b) Inhibit System Recovery (VSS Deletion)

A common ransomware technique (T1490) is to destroy local recovery points before encryption, preventing a simple rollback. This is often accomplished with a single PowerShell command: Get-WmiObject Win32_Shadowcopy | Remove-WmiObject.

This specific attack can be mitigated with a high-fidelity HIDS rule. The rule should monitor for process creation and specifically alert on the execution of vssadmin delete shadows, wbadmin delete catalog, or PowerShell processes containing the string Win32_Shadowcopy.

6) Summary of Proactive Controls

This layered mitigation plan shifts the organization's security posture from a reliance on perimeter defense to a resilient defense-in-depth model. By prioritizing controls based on asset function—first hardening foundational identity and recovery services, then protecting core business assets (IP and OT), and finally securing the underlying infrastructure (virtualization and IoT)—this strategy addresses the high-impact vulnerabilities most likely to be exploited by any post-compromise adversary. The combination of timely patching, robust network segmentation, and high-fidelity, sensor-based detection provides a durable framework for preventing a catastrophic failure, regardless of the specific TTPs employed by the attacker.

V. Conclusion

This research demonstrated that the traditional, perimeter-focused security models prevalent in SMEs are insufficient against modern, post-compromise threat actors like Akira. By conducting a retrospective analysis of the Roysons Corporation incident, this study validated that while the initial breach via a VPN vulnerability was the catalyst, the catastrophic impact was a direct result of a flat network architecture that failed to isolate critical data assets. The application of Data-Centric System Threat Modeling (NIST SP 800-154) proved to be a superior methodology for identifying these internal choke points compared to standard vulnerability scanning, which often misses logical process failures.

Furthermore, the integration of Cyber Threat Emulation provided a critical empirical validation layer often missing in theoretical risk assessments. The successful detection of the emulated Emotet and Trickbot beacons confirmed that cost-effective, open-source solutions like Security Onion can provide enterprise-grade visibility when tuned with threat-specific intelligence. This reinforces the argument that effective defense for manufacturers does not require unlimited budgets, but rather a strategic shift from passive prevention to active detection and response.

A. Future Work

While this study successfully reconstructed the attack vector and validated immediate mitigations, several avenues for future research remain. First, the current emulation environment focused on the initial access and lateral movement phases; future work should expand to Advanced Cyber Threat Emulation to test the efficacy of incident response procedures during the active encryption phase. Second, the study identified the need for a Full Implementation of a Security Operations Platform, moving beyond a standalone sensor to a fully integrated monitoring environment capable of continuous threat hunting. Finally, developing a formalized Compliance Program Implementation roadmap would help bridge the gap between the technical controls identified in this paper and the long-term governance required to maintain them.

Acknowledgment

We thank Dr. Mohamed Baza for his guidance in the course CSCI 631: Principles of Computer Security, for which this research was conducted.

We thank Roysons Corp. for giving us permission to analyze this ransomware attack and for providing valuable documentation for our analysis.

We would like to express our gratitude to Ronnie St. Clair, Ph. D., for his guidance, direction and support that is very meaningful in this research.

C References

[1] S. Scott, "3 trends set to drive cyberattacks and ransomware in 2024," 22 02 2024. [Online]. Available: https://www.weforum.org/stories/2024/02/3-trends-ransomware-2024/#:~:text=Ransomware%20activity%20alone%20was%20up,in%20the%20frequency%20of%20attacks.. [Accessed 06 10 2025].

[2] Trend Micro Research, "Ransomware Spotlight," Trend Micro, 05 10 2023. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira. [Accessed 05 10 2025].

[3] MOXFIVE, "Internal Forensic Analysis Report," MOXFIVE, Lean, 2025.

[4] M. Alvarez, C. Caridi, J. Chung, S. Cunningham, M. Epley, M. Goyal, C. Hammond, S. Hill, J. Kuo, D. McMillen, G. Muhr, G. Parham and A. Zeizel, "IBM X-Force 2025 Threat Intelligence Index," IBM, New York, 2025.

[5] DRAGOS, "OT/ICS Cybersecurity Report," Dragos, 2025.

[6] CISA, FBI, EC3 and NCSC-NL, "StopRansomware: Akira Ranswomware," CISA, Arlington, 2024.

[7] Arete, "Malware Spotlight: Akira Ransomware," 2024.

[8] H. C. Yuceel, "CVE-2023-20269: Akira Ranswomware Exploits Cisco ASA Vulnerability," Picus Security, 01 03 2024. [Online]. Available: https://www.picussecurity.com/resource/blog/cve-2023-20269-akira-ransomware-exploits-cisco-asa-vulnerability#:~:text=DATASHEET%20The%20Pioneer%20of%20Breach,Ransomware%20Exploits%20Cisco%20ASA%20Vulnerability. [Accessed 22 11 2025].

[9] V. Drake, "Threat Modeling," Open Web Application Security Project, 2025. [Online]. Available: https://owasp.org/www-community/Threat_Modeling. [Accessed 06 10 2025].

[10] V. Drake, S. Strittmatter, Z. Braiterman and A. Shostack, "Threat Modeling Process," OWASP, 2025. [Online]. Available: https://owasp.org/www-community/Threat_Modeling_Process. [Accessed 06 10 2025].

[11] M. Souppaya and K. Scarfone, "NIST SP 800-154," National Institute of Standards and Technology, 14 03 2016. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/154/ipd. [Accessed 05 10 2025].

[12] U.S. Senate Comittee on Commerce, Science, and Transportation, ""Kill Chain" Analysis of the 2013 Target Data Breach," 03, 26, 2014.

[13] Roysons Corp. IT Department, "Statement Detailing Akira Ransomware Incident," 2025.

[14] K. Stine, R. Kissel, W. C. Barker, J. Fahlsing and J. Gulick, "NIST SP 800-60 Guide for Mapping Types of Information and Systems to Security Categories," 31 01 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/60/r2/iwd. [Accessed 05 10 2025].

[15] J. M. Desai and C. J. Shingadiya, "Hybrid Malware Analysis for Threat Intelligence: Unveiling Akira Ransomware," *International Journal of Computational and Experimental Science and ENgineering,* vol. 11, no. 3, pp. 5606-5614, 2025.

[16] Z. Y. Dzahabi, N. Hayaty and M. Bettiza, "Cryptography of ChaCha20 and RSA Algorithms for Text Security," *Journal of Computer Networks, Architecture and,* vol. 7, no. 1, pp. 290-301, 2025.

[17] E. Zwick, M. Pinto, C.-E. Bettan, V. Deshmukh and D. K. Nohi, "Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption," Microsoft Threat Intelligence, 29 07 2024. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/. [Accessed 23 11 2025].

[18] K. Khaliq, K. Hamid, M. U. Ullah, M. Ibrar, N. Z. Ab Rahim and U. Ahmad, "Ransomware Attacks: Tools and Techniques for Detection," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, 2024.

[19] Cisco, "Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN Unauthorized Access Vulnerability," Cisco, 06 09 2023. [Online]. Available: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC. [Accessed 5 10 2025].

[20] CISA, "Best Practices for MITRE ATT&CK Mapping," 17 01 2023. [Online]. Available: https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping. [Accessed 05 10 2025].

[21] A. Mundo and M. Kersten, "Akira Ransomware," Trellix, 29 11 2023. [Online]. Available: https://www.trellix.com/blogs/research/akira-ransomware/. [Accessed 05 10 2025].

[22] Z. Braiterman, A. Shostack, J. Marcil, S. de Vries, I. Michlin, K. Wuyts, R. Hurlbut, B. S. Shoenfield, F. Scott, M. Coles, C. Romeo, A. Miller, I. Tarandach, A. Douglen and M. French, "Threat Modeling Manifesto," 17 11 2020. [Online]. Available: https://www.threatmodelingmanifesto.org. [Accessed 23 11 2025].

[23] Crowdstrike Falcon Complete Team, "Allowlist Created by Falcon Complete Team," 2025.

[24] J. Thamsongkrah, "Akira," MITRE Corporation, 11 03 2025. [Online]. Available: https://attack.mitre.org/software/S1129/. [Accessed 05 10 2025].

[25] MITRE Corp., "Adversary Emulation Plan, "Center for Threat-Informed Defense"," 2024. [Online]. Available: https://github.com/center-for-threat-informed-defense/adversary_emulation_library. [Accessed 23 11 2025].

[26] M. Nazar, "A Review on Security Onion Tools for Intrusion Detection," *International Journal of Scientific & Engineering Research,* vol. 12, no. 3, pp. 599-607, 03 2021.

[27] Joint Task Force Transformation Initiative, "NIST Special Publication 800-30," 09 2012. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/30/r1/final. [Accessed 05 10 2025].

[28] Health Sector Cybersecurity Coordination Center (HC3), "Akira Ransomware Sector Alert," 2023.

[29] J. Thamsongkrah, "Akira Group MITRE ATT&CK Webpage," MITRE, 11 March 2025. [Online]. Available: https://attack.mitre.org/groups/G1024/.

[30] Insurance Data Management Association (IDMA), "Akira Ransomware Pivoting Back to Double," 2024.

[31] N. Schevchenko, T. A. Chick, T. P. Scanlon and C. Woody, "Threat Modeling: A Summary of Available Methods," Software Engineering Institute, July 2018. [Online]. Available: https://www.sei.cmu.edu/documents/569/2018_019_001_524597.pdf. [Accessed 06 10 2025].

[32] National Cyber Security Centre, "Ransomware," Government of the United Kingdom , 2025. [Online]. Available: https://www.ncsc.gov.uk/ransomware/home. [Accessed 07 10 2025].

[33] VMware, "CVE-2024-37085 Detail," National Institute of Science and Technology, 30 10 2023. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2024-37085. [Accessed 23 11 2025].

[34] Broadcom, "VMSA-2024-0013:VMware ESXi and vCenter Server updates address multiple security vulnerabilities," VMware, 12 08 2024. [Online]. Available: https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505. [Accessed 23 11 2025].