# THREAT REPORT: Analysis of the SafePay Ransomware Attack on Ingram Micro and its Implications for Global IT Supply Chain Integrity

* **Classification:** TLP:WHITE (For Public Distribution)
* **Date of Publication:** October 26, 2025
* **Authored By:** Senior Cybersecurity Analyst

### Table of Contents

1. **Cover & Navigation**
2. **Executive Summary**
3. **Mission Context: Systemic Risk in Data-Intensive Ecosystems**
   * The Ingram Micro Incident as a Supply Chain Bellwether
   * Analyzing Third-Party Risk: Lessons for 'Project Nightingale'
   * Vulnerabilities in Centralized Distribution and Data Aggregation Models
4. **Attack Overview: A Chronological Reconstruction**
5. **Affected Organizations Analysis**
   * Direct Impact on Ingram Micro
   * The Partner Ecosystem Under Duress: MSPs and Resellers
   * End-Customer and Vendor Impact
6. **Cross-Sector Impact: The IT Supply Chain as Critical Infrastructure**
   * Quantifying the Disruption: A Node Failure Analysis
   * Erosion of Trust and Reputational Damage
   * The Strategic Targeting of Digital Linchpins
7. **Attack Path Analysis: Deconstructing the Intrusion**
   * Phase 1: Initial Access
   * Phase 2: Discovery & Lateral Movement
   * Phase 3: Defense Evasion
   * Phase 4: Exfiltration
   * Phase 5: Impact
8. **Forensic Evidence & Indicators of Compromise (IOCs)**
9. **MITRE ATT&CK® Mapping**
10. **Detection, Response, and Hardening**
    * Detection Rules
    * Incident Response Procedures
    * Long-Term Strategic Hardening
11. **Conclusion**

## Executive Summary

In early July 2025, Ingram Micro, a foundational component of the global information technology (IT) supply chain, sustained a debilitating ransomware attack that paralyzed its core business operations for several days.1 The incident, attributed to the SafePay ransomware group, disrupted the company's ability to process orders, manage cloud licenses, and ship products, causing widespread financial and operational damage that cascaded through its extensive network of partners, vendors, and end-customers.3 This report provides an exhaustive analysis of the attack, its multifaceted impact, the threat actor's tactics, and critical recommendations for mitigating similar systemic risks in the future.

### Key Findings

* **Attribution:** The attack was conducted by the SafePay ransomware group, a sophisticated and centrally-operated threat actor that first emerged in late 2024.1 Known for its "double-extortion" methodology, which combines data encryption with the threat of public data leakage, SafePay has rapidly become one of the most active ransomware operations globally.6
* **Primary Attack Vector:** The initial intrusion was not the result of a sophisticated software vulnerability. Instead, threat actors achieved initial access by using compromised credentials against Ingram Micro's Palo Alto Networks GlobalProtect VPN infrastructure.1 This highlights a fundamental failure in identity and access management controls, particularly the apparent lack of enforced multi-factor authentication (MFA), rather than a flaw in the VPN product itself.8
* **Business Impact:** The multi-day outage of critical platforms, including the AI-powered Xvantage distribution system and the Impulse licensing portal, halted Ingram Micro's global transaction flow.1 With a daily turnover of approximately $190 million, analyst estimates place the direct revenue loss at over $100 million per day of the crisis.4 The disruption forced thousands of Managed Service Providers (MSPs), resellers, and their end-customers to halt projects, delay deployments, and seek alternative distributors, causing a significant bottleneck in the IT supply chain.10
* **Data Exfiltration:** As part of its double-extortion strategy, the SafePay group claimed to have exfiltrated 3.5TB of sensitive data from Ingram Micro's network.6 The allegedly stolen data included financial statements, intellectual property, accounting records, and personnel files, which the group threatened to leak on its dark web portal to increase pressure on the victim to pay the ransom.1

### Strategic Implications

The Ingram Micro incident serves as a stark case study in systemic risk, demonstrating how the compromise of a single, hyper-connected entity can trigger a global supply chain crisis. The attack's impact was magnified not by the technical complexity of the intrusion but by Ingram Micro's central position of trust within the IT ecosystem. Furthermore, the significant delays and perceived lack of transparency in the company's initial communications with its partners severely eroded that trust, compounding the operational damage and creating long-term reputational harm.4

### Summary of High-Priority Recommendations

This analysis culminates in a series of strategic recommendations designed to prevent and mitigate similar attacks. The highest priorities include the mandatory enforcement of phishing-resistant MFA on all remote access points and privileged accounts; the aggressive adoption of a Zero Trust security architecture that limits the blast radius of a potential breach; the implementation of robust network segmentation to isolate critical systems; and the development of a transparent, partner-focused crisis communication plan to maintain trust during a security incident.

## Mission Context: Systemic Risk in Data-Intensive Ecosystems

The ransomware attack on Ingram Micro should not be viewed as an isolated corporate breach but rather as a bellwether event, exposing the inherent fragility of highly centralized global supply chains. Its analysis provides critical lessons for any large-scale, data-intensive ecosystem where trust and operational uptime are paramount, offering a direct and cautionary parallel to the risks facing initiatives like the healthcare data aggregation project known as "Project Nightingale."

### The Ingram Micro Incident as a Supply Chain Bellwether

Ingram Micro functions as a central nervous system for the global IT economy. With a distribution network capable of reaching nearly 90% of the world's population, it is a critical node connecting thousands of technology manufacturers and cloud providers with a vast base of resellers and MSPs.10 This central role makes it a high-value, high-impact target for adversaries who understand that disrupting such a linchpin maximizes downstream chaos and pressure.14 The attack demonstrated with alarming clarity that modern adversaries are strategically targeting these critical infrastructure nodes to amplify their impact far beyond the initially compromised network.16 The paralysis of Ingram Micro was not merely an IT outage; it was a systemic failure that halted commerce, delayed projects, and created uncertainty across multiple interdependent sectors.

### Analyzing Third-Party Risk: Lessons for 'Project Nightingale'

The strategic implications of the Ingram Micro breach extend far beyond logistics and commerce, offering a powerful analog for the risks inherent in large-scale data aggregation platforms, most notably the Google and Ascension partnership known as "Project Nightingale".17 This initiative, which involves the collection and processing of tens of millions of patient health records, represents a centralization of highly sensitive data. The Ingram Micro case provides a critical framework for understanding the potential consequences of a security failure in such an environment.

The fundamental parallel lies in the concept of a centralized point of failure. If the compromise of a *logistics* and *commerce* hub like Ingram Micro can cause billions of dollars in economic disruption and paralyze a global industry, the compromise of a centralized *health data* hub would carry far more severe and direct human consequences. The concerns raised by whistleblowers regarding Project Nightingale—specifically around data access, patient consent, and the potential for misuse—are magnified when viewed through the lens of the Ingram Micro attack.17 The incident underscores that the primary risk is not just the technical breach itself, but the catastrophic failure of the trust placed in a central data custodian.

### Vulnerabilities in Centralized Distribution and Data Aggregation Models

Centralization, whether for distributing IT hardware or aggregating patient data, offers immense efficiencies. However, it also creates a concentrated point of risk, a single target whose compromise can have a disproportionately large impact.12 The very interconnectedness that makes Ingram Micro a powerful economic engine is also what made the attack's impact so profound and widespread. A vulnerability in one part of its system rapidly cascaded into a full-blown crisis for its thousands of dependent partners.

This dynamic reveals a critical lesson about the relationship between technology and trust. The ultimate impact of the Ingram Micro breach was defined less by the technical sophistication of the ransomware and more by the company's foundational role as a trusted intermediary. The initial breach was technically straightforward: a credential-based VPN intrusion, a common and preventable security lapse.1 However, Ingram Micro is not just a technology company; it is a logistics and trust broker for a vast ecosystem of smaller businesses that depend entirely on its operational uptime to serve their own customers.11 When Ingram's systems went down, the primary damage was not the encryption of its servers, but the severing of these critical business dependencies. MSPs were suddenly unable to quote prices, place orders, or provision essential cloud services for their clients.2

This dependency, built on an implicit trust in Ingram's resilience, became the primary vulnerability exploited by the attackers. The attack's "blast radius" was therefore determined not by the number of encrypted servers within Ingram's network, but by the number of dependent partners in the global supply chain. This provides a crucial warning for any large-scale data aggregation initiative. The risk to a project like Nightingale is not merely that a server could be breached, but that the trust of millions of patients and thousands of healthcare providers in a centralized data custodian could be shattered, potentially causing a systemic failure in the delivery of healthcare itself.

## Attack Overview: A Chronological Reconstruction

The Ingram Micro ransomware attack unfolded over several weeks, beginning with a period of undetected attacker presence within the network and culminating in a multi-day global outage and a public extortion attempt. The following timeline synthesizes information from numerous public statements, security reports, and news articles to provide a consolidated and authoritative sequence of events. This reconstruction highlights the delta between the internal discovery of the attack and the company's public communications, a key factor in the erosion of partner trust.

| Date/Time (UTC) | Event Description | Key Actors | Public/Internal Status | Source(s) |
| --- | --- | --- | --- | --- |
| **~June 2025 (Estimated)** | The SafePay group achieves initial access to Ingram Micro's network, reportedly via compromised VPN credentials. The attackers move laterally and perform reconnaissance undetected for several weeks. | SafePay | Internal | 1 |
| **July 3, 2025** | Employees begin discovering ransom notes (readme\_safepay.txt) on their computer systems. Core business platforms, including the Xvantage portal, go offline. Customers and partners globally lose access to ordering and licensing systems. | Ingram Micro, SafePay | Internal Discovery, Public Outage | 1 |
| **July 4, 2025** | In response to the spreading attack, Ingram Micro proactively shuts down additional internal systems to contain the breach. Employees are instructed to work from home. The global outage continues with no official explanation. | Ingram Micro | Internal Response, Public Outage | 1 |
| **July 5, 2025 (02:07 UTC, July 6)** | Ingram Micro issues its first official public statement via a press release and an SEC Form 8-K. The company confirms it "identified ransomware on certain of its internal systems" and has engaged cybersecurity experts and notified law enforcement. | Ingram Micro | Public Acknowledgement | 13 |
| **July 6-8, 2025** | Forensic investigation and system remediation efforts are underway. The company begins a phased restoration of services, first enabling subscription-based orders and then allowing orders via phone or email in limited regions. The main customer portal remains down. | Ingram Micro, Third-Party Experts | Public Update | 4 |
| **July 8, 2025** | In an updated statement, Ingram Micro announces that it believes "the unauthorized access to our systems in connection with the incident is contained and the affected systems remediated." The investigation into the scope of data theft remains ongoing. | Ingram Micro | Public Update | 2 |
| **July 9-10, 2025** | Ingram Micro announces that all business operations have been restored globally across all regions. The company states that it can process and ship orders received via EDI, phone, or email. | Ingram Micro | Public Update | 1 |
| **July 29-30, 2025** | The SafePay ransomware group officially adds Ingram Micro to its dark web leak site. The group claims to have stolen 3.5TB of data and threatens to release it unless a ransom is paid, escalating the incident to a public extortion phase. | SafePay | Public Extortion | 1 |

## Affected Organizations Analysis

The ransomware attack on Ingram Micro created a powerful ripple effect, with consequences extending far beyond the company's own network. The direct impact was severe, but the cascading disruption to its vast ecosystem of partners, vendors, and end-customers illustrates the profound interconnectedness of the modern IT supply chain.

### Direct Impact on Ingram Micro

For Ingram Micro, the attack resulted in both operational paralysis and staggering financial losses.

* **Operational Paralysis:** The moment the ransomware was activated, the company's core business functions ceased. Critical platforms, including the AI-powered Xvantage system, the Impulse licensing portal, and other essential ordering and fulfillment systems, were proactively taken offline to contain the threat.1 This decisive action, while necessary from a security standpoint, effectively halted the company's ability to conduct its primary business: processing quotes, fulfilling hardware and software orders, and managing cloud licenses for its global customer base.5 For several days, the company was disconnected from its own value chain, unable to serve its partners or transact with its vendors.2
* **Financial Losses:** The financial repercussions of this shutdown were immediate and substantial. With a reported turnover of approximately $190 million per working day, the outage represented a massive loss of revenue.4 Some analysts estimated the daily cost of the disruption to be as high as $136 million.1 Beyond the lost revenue, the company incurred significant costs related to the incident response, including the hiring of leading cybersecurity experts, forensic investigation, system remediation, and potential regulatory fines or legal fees.

### The Partner Ecosystem Under Duress: MSPs and Resellers

The impact on Ingram Micro's partners—primarily MSPs and value-added resellers—was arguably more complex and damaging in the long term. These businesses rely on Ingram Micro not just for procurement but for the operational backbone of their service delivery.

* **Business Interruption:** With Ingram's systems offline, thousands of MSPs were unable to conduct daily business. They could not provision new Microsoft 365 or Dropbox licenses for clients, fulfill hardware orders for customer projects, or generate quotes for new sales.4 This created a cascading failure, where the distributor's problem immediately became the partner's problem, and subsequently, the end-customer's problem.12
* **Communication Vacuum and Frustration:** A recurring and vehement complaint from the partner community was the lack of timely and transparent communication from Ingram Micro during the initial 36-48 hours of the crisis.5 Many partners reported learning more about the nature of the incident from news articles and industry forums than from official company channels.4 This information vacuum left them unable to answer questions from their own anxious clients, forcing them to manage a crisis without information and damaging their credibility.23
* **Security Concerns and Precautionary Measures:** The breach triggered immediate and serious security concerns among technically savvy MSPs. Recognizing that Ingram Micro, as a Cloud Solution Provider (CSP), held privileged access to their clients' cloud tenants, many partners feared the attack could be used as a pivot point for a much larger supply chain attack.21 This fear prompted a wave of defensive actions across the MSP community. Partners proactively audited their clients' Microsoft 365 environments and, in many cases, revoked Ingram's Granular Delegated Admin Privileges (GDAP) as a precautionary measure to sever the connection and prevent potential lateral movement by the attackers.21

This widespread revocation of GDAP permissions represents a critical dynamic in the incident. The permissions that are essential for the efficient, automated management of cloud licenses in the CSP model are the very same permissions that create systemic risk in the event of a distributor breach. The crisis forced a channel-wide, emergency re-evaluation of this trust model. MSPs' immediate reaction to revoke Ingram's GDAP roles revealed a fundamental tension: the trust required for operational efficiency is fragile and can be instantly withdrawn when a partner's security posture is questioned. This action highlights that the "trust" in a supply chain partner is not an abstract concept but is encoded in tangible API permissions and administrative roles. The breach forced a manual, emergency "un-trusting" at a massive scale, demonstrating the inherent vulnerability of the entire model.

### End-Customer and Vendor Impact

The disruption inevitably flowed downstream to end-customers and upstream to technology vendors.

* **End-Customers:** Businesses that had placed orders through Ingram's partners faced unexpected project delays, uncertainty about equipment shipments, and delays in the provisioning of critical software licenses.2
* **Vendors:** Major technology manufacturers such as Dell, HPE, and Cisco, who rely on distributors like Ingram Micro to move their products, saw a critical sales channel disrupted.5 The timing of the attack, near the end of a financial quarter for some, likely impacted their sales targets and revenue forecasts.

## Cross-Sector Impact: The IT Supply Chain as Critical Infrastructure

The Ingram Micro ransomware attack transcends the definition of a typical corporate data breach. It serves as a potent illustration of how the digital supply chain has become a form of critical infrastructure, where the failure of a single, central node can precipitate a cross-sector crisis. The incident's true significance lies in its demonstration of systemic risk, the erosion of trust, and the strategic targeting of digital linchpins by modern threat actors.

### Quantifying the Disruption: A Node Failure Analysis

In network theory, the removal of a highly connected node can cause a disproportionate collapse of the entire network. Ingram Micro represents such a node in the global IT supply chain. Its temporary failure created a massive bottleneck, simultaneously impacting manufacturing (vendors unable to ship products), retail (resellers unable to sell), cloud services (licenses unable to be provisioned), and enterprise IT (customers unable to receive equipment and software).11 The event proves that digital distributors are as vital to the modern economy as physical shipping ports, energy grids, or financial clearinghouses. The paralysis of its operations did not just affect technology companies; it affected every business sector that relies on technology to function. This incident should compel governments and regulatory bodies to consider major digital distributors as elements of national critical infrastructure, requiring a higher standard of security and resilience.

### Erosion of Trust and Reputational Damage

While Ingram Micro eventually restored its systems, the long-term reputational damage may prove more costly than the immediate financial losses. The primary driver of this damage was the widespread perception of poor communication and a lack of transparency in the critical early days of the incident.5 Partners felt abandoned and uninformed, a failure that directly impacts the trust essential for a distribution model.12 This trust deficit creates opportunities for competitors. Reports indicated that rival distributors, such as D&H, actively reached out to affected Ingram partners during the outage, potentially signaling a long-term shift in market share and partner loyalty.22 In a relationship-driven industry, the failure to manage the communication and trust aspects of a crisis can be as devastating as the technical failure itself.

### The Strategic Targeting of Digital Linchpins

The choice of Ingram Micro as a target was likely not random. It reflects a strategic evolution in the tactics of sophisticated ransomware groups like SafePay. These groups have recognized that the most effective way to compel a ransom payment is to inflict the maximum possible downstream pain.16 By targeting an organization whose failure disrupts thousands of other businesses, the attackers create immense pressure not only from the victim's own operational losses but also from its entire ecosystem of furious partners and customers.12 This strategy, targeting digital linchpins, turns the victim's own value chain into a weapon against it. The Ingram Micro attack is a clear signal that any organization occupying a central, critical role in a supply chain—be it in technology, manufacturing, healthcare, or finance—is now a prime target for high-tier ransomware operations.

## Attack Path Analysis: Deconstructing the Intrusion

The attack on Ingram Micro followed a classic ransomware intrusion pattern, progressing through distinct phases from initial access to final impact. The tactics, techniques, and procedures (TTPs) employed by the SafePay group, while not groundbreaking, were executed effectively against a high-value target, leveraging common security weaknesses to achieve a catastrophic outcome.

### Phase 1: Initial Access

The consensus among security researchers and incident reports indicates that the initial point of entry was Ingram Micro's corporate Virtual Private Network (VPN).1

* **Vector:** The specific platform identified was Palo Alto Networks GlobalProtect VPN.4 It is critical to note that this was not a software vulnerability or zero-day exploit. Palo Alto Networks issued a statement confirming that none of its products were the source of a vulnerability in the breach.8
* **Method:** The breach was accomplished through the use of **Valid Accounts (MITRE ATT&CK T1078)**.1 The SafePay group gained access by using compromised credentials that were likely obtained through one of several common methods: password spraying attacks against the VPN gateway, brute-forcing weak passwords, or purchasing previously stolen credentials from dark web marketplaces.7 The success of this initial access vector points directly to a critical security control failure: the lack of universally enforced, phishing-resistant multi-factor authentication (MFA) on the VPN gateway.9

### Phase 2: Discovery & Lateral Movement

Once inside the network, the attackers entered a dwell period, which reportedly lasted for several weeks, allowing them to perform reconnaissance and move laterally without being detected.1

* **Network Reconnaissance:** A known TTP of the SafePay group is the use of PowerShell-based scripts for network discovery.28 Specifically, the script  
  ShareFinder.ps1 has been observed in other SafePay incidents. This tool is used to enumerate accessible network shares, helping the attackers map the internal network and identify high-value data repositories.28
* **Lateral Movement:** To move from their initial foothold to other systems within the network, the attackers utilized common and often-unmonitored administrative protocols. The primary method cited was **Remote Desktop Protocol (RDP) (T1021.001)**, which allowed them to log in to servers and workstations interactively using the compromised credentials.30

### Phase 3: Defense Evasion

A key part of the SafePay playbook involves actively dismantling the target's security and recovery capabilities before deploying the final payload.

* **Disabling Security Tools:** SafePay is known to terminate security processes and services to avoid detection. This includes using "Living Off the Land Binaries" (LOLBins)—legitimate system tools—to disable endpoint protection products like Windows Defender and other third-party antivirus solutions.26
* **Inhibiting System Recovery (T1490):** To maximize damage and prevent easy restoration, the attackers systematically deleted Volume Shadow Copies. This is a hallmark of modern ransomware attacks and is typically accomplished by executing command-line tools such as vssadmin.exe and wmic.exe with specific arguments (e.g., vssadmin delete shadows /all /quiet).28 The group is also known to modify boot configurations using  
  bcdedit.exe to disable Windows Automatic Repair, further hampering recovery efforts.31

### Phase 4: Exfiltration

In line with their double-extortion model, the SafePay operators exfiltrated a massive volume of data before initiating encryption.

* **Data Staging and Compression (T1560.001):** The attackers first collected and staged sensitive data from across the network. This data was then compressed into large archive files, often using common utilities like **WinRAR** or **7-Zip** to prepare it for transfer.28
* **Data Transfer (T1048):** The compressed archives were then exfiltrated from the network to attacker-controlled infrastructure. SafePay has been observed using common file transfer tools like **FileZilla** (using FTP) or **Rclone** (often used for transferring data to cloud storage) for this purpose.27 In this incident, the group claimed to have successfully exfiltrated 3.5TB of Ingram Micro's data.6

### Phase 5: Impact

With data exfiltrated and defenses disabled, the attackers proceeded to the final, destructive phase of the attack.

* **Data Encrypted for Impact (T1486):** The SafePay ransomware payload was executed across compromised systems. The malware encrypted files, rendering them inaccessible, and appended the .safepay extension to each affected file.27
* **Defacement/Ransom Note (T1491.001):** On each encrypted system, the ransomware dropped a ransom note file named readme\_safepay.txt.8 This note contained the attackers' greetings, a confirmation that the network had been breached, and instructions for contacting them to negotiate a ransom payment for the decryption key and the deletion of the stolen data.

## Forensic Evidence & Indicators of Compromise (IOCs)

Effective threat hunting, incident response, and post-breach analysis rely on specific, actionable forensic artifacts. This section collates known and plausible Indicators of Compromise (IOCs) associated with the SafePay ransomware group. While specific IOCs from the Ingram Micro breach have not been publicly disclosed by the company, analysis of other SafePay incidents provides a reliable set of indicators for detection and investigation.

| IOC Type | Indicator | Description & Context | Source(s) |
| --- | --- | --- | --- |
| **File Hash (SHA256)** | a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526 | A known SHA256 hash for a SafePay ransomware sample. Can be used for static file scanning on endpoints and in malware repositories. | 34 |
| **File Artifact** | readme\_safepay.txt | The standard name for the ransom note file dropped by the malware on encrypted systems. The presence of this file is a definitive sign of a SafePay infection. | 27 |
| **File Artifact** | \*.safepay | The file extension appended to all files encrypted by the SafePay ransomware. Monitoring for the mass creation of files with this extension can detect an active encryption event. | 27 |
| **File Artifact** | ShareFinder.ps1 | A PowerShell script used by SafePay operators during the discovery phase to enumerate network shares. Its presence or execution in logs is a strong indicator of compromise. | 28 |
| **Mutex** | Victim-Specific Mutex | SafePay creates a unique mutex on each infected machine to prevent multiple instances of the ransomware from running simultaneously. The mutex name is often derived from the victim ID. | 29 |
| **C2 IP Address** | 45.91.201.247 | A known Command and Control (C2) IP address associated with SafePay infrastructure. Network traffic to or from this IP should be blocked and investigated. | 34 |
| **C2 IP Address** | 77.37.49.40 | A known Command and Control (C2) IP address associated with SafePay infrastructure. Network traffic to or from this IP should be blocked and investigated. | 34 |
| **C2 IP Address** | 80.78.28.63 | A known Command and Control (C2) IP address associated with SafePay infrastructure. Network traffic to or from this IP should be blocked and investigated. | 34 |
| **Tor Domain** | iieavvi4wtiuijas3zw4w54a5n2srnccm2fcb3jcrvbb7ap5tfphw6ad.onion | A Tor.onion address used by SafePay for its dark web leak site or payment portal. DNS queries or traffic to this domain are highly suspicious. | 34 |
| **Tor Domain** | qkzxzeabulbbaevqkoy2ew4nukakbi4etnnkcyo3avhwu7ih7cql4gyd.onion | A Tor.onion address used by SafePay for its dark web leak site or payment portal. DNS queries or traffic to this domain are highly suspicious. | 34 |
| **Log Evidence** | Failed login attempt from [IP]... Successful login from [IP] | A pattern of multiple failed VPN login attempts from a single IP address, followed by a successful login, is a strong indicator of a password spraying or brute-force attack. | 30 |
| **Command Line** | vssadmin.exe delete shadows /all /quiet | A command executed by SafePay to delete all Volume Shadow Copies on a system, preventing file-level recovery. | 28 |
| **Command Line** | wmic.exe shadowcopy delete | An alternative command used by SafePay to delete Volume Shadow Copies via Windows Management Instrumentation (WMI). | 31 |
| **Command Line** | bcdedit.exe /set{default} recoveryenabled no | A command used by SafePay to disable the Windows Automatic Repair feature, further hindering system recovery. | 31 |

## MITRE ATT&CK® Mapping

To provide a standardized understanding of the adversary's behavior, the observed and reported Tactics, Techniques, and Procedures (TTPs) of the SafePay ransomware group are mapped to the MITRE ATT&CK® for Enterprise framework. This matrix serves as a crucial tool for security teams to assess their defensive posture, develop detection strategies, and simulate adversary behavior.

| Tactic | Technique ID | Technique Name | Description of Use by SafePay |
| --- | --- | --- | --- |
| **Reconnaissance** | T1595.002 | Vulnerability Scanning | Actors use scanning tools like Shodan to identify publicly exposed and potentially vulnerable services, particularly VPN gateways.30 |
|  | T1589.001 | Credentials | Actors acquire credentials for initial access by purchasing them from dark web markets or obtaining them from infostealer malware logs.1 |
| **Initial Access** | T1133 | External Remote Services | Actors exploit external-facing services, primarily VPN gateways, to gain initial access to the corporate network.29 |
|  | T1078 | Valid Accounts | The primary initial access method involves using compromised but legitimate credentials to authenticate to VPN services, bypassing perimeter defenses.1 |
| **Execution** | T1059.001 | PowerShell | Actors use PowerShell to execute discovery scripts, most notably ShareFinder.ps1, to enumerate network shares and identify data for exfiltration.28 |
|  | T1204.002 | Malicious File | Actors may use social engineering (phishing, vishing) to trick users into executing a malicious payload, often disguised as a legitimate file.33 |
| **Persistence** | T1547.001 | Registry Run Keys / Startup Folder | The ransomware payload creates a new registry key under Software\Microsoft\Windows\CurrentVersion\Run to ensure it executes automatically every time Windows starts.28 |
|  | T1136 | Create Account | In some intrusion scenarios, ransomware affiliates may create new local or domain user accounts to maintain persistent access to the network.37 |
| **Privilege Escalation** | T1134.002 | Create Process with Token | Actors are known to use token impersonation techniques to escalate privileges after gaining an initial foothold.9 |
|  | T1548.002 | Bypass User Account Control | The ransomware abuses the CMSTPLUA COM interface to bypass Windows User Account Control (UAC) and execute commands with elevated permissions without prompting the user.28 |
| **Defense Evasion** | T1562.001 | Disable or Modify Tools | The ransomware binary contains a list of security-related processes and services (e.g., Sophos, Veeam, sqlsvc) that it terminates to disable endpoint protection and backup agents.26 |
|  | T1490 | Inhibit System Recovery | A core tactic is the deletion of Volume Shadow Copies using vssadmin.exe and wmic.exe to prevent easy restoration of encrypted files.31 |
|  | T1070 | Indicator Removal on Host | Actors may clear Windows and Linux system logs to erase their tracks and inhibit forensic investigation and incident response.28 |
|  | T1027 | Obfuscated Files or Information | The ransomware binary stores all its internal strings (e.g., API names, commands) in an encrypted format, decrypting them at runtime to evade static analysis.28 |
| **Credential Access** | T1003 | OS Credential Dumping | During post-exploitation, affiliates may use tools like Mimikatz to dump credentials from memory, allowing them to harvest additional accounts for lateral movement.37 |
| **Discovery** | T1135 | Network Share Discovery | Actors execute the ShareFinder.ps1 script to discover accessible network shares across the local domain, identifying targets for data theft and encryption.28 |
|  | T1082 | System Information Discovery | The ransomware gathers information about the infected system, including the Windows UI language, to avoid executing in Commonwealth of Independent States (CIS) countries.28 |
|  | T1018 | Remote System Discovery | After gaining access, actors conduct network scanning using tools like AngryIPScanner or Nmap to identify other live hosts and potential targets for lateral movement.37 |
| **Lateral Movement** | T1021.001 | Remote Desktop Protocol | RDP is a primary method used by actors to move between systems within the compromised network, using stolen credentials to access workstations and servers.26 |
|  | T1021.002 | SMB/Windows Admin Shares | Actors may use tools like PsExec to leverage administrative shares (e.g., C$, ADMIN$) for lateral movement and remote code execution.29 |
| **Collection** | T1560.001 | Archive Collected Data: Archive via Utility | Before exfiltration, actors use utilities like WinRAR and 7-Zip to compress collected data into large archive files, making it easier to transfer.28 |
| **Exfiltration** | T1048 | Exfiltration Over Alternative Protocol | Actors use common file transfer clients like FileZilla (FTP) to exfiltrate the staged and compressed data to their own servers.27 |
|  | T1567.002 | Exfiltration to Cloud Storage | The tool Rclone is often used to exfiltrate large volumes of data to various cloud storage services controlled by the attackers.29 |
| **Impact** | T1486 | Data Encrypted for Impact | The primary objective is to encrypt critical files on victim systems, appending the .safepay extension and rendering them unusable without the decryption key.27 |
|  | T1491.001 | Defacement: Internal Defacement | The ransomware drops a note named readme\_safepay.txt on encrypted systems, which serves as a form of internal defacement and provides instructions for ransom payment.8 |

## Detection, Response, and Hardening

Based on the comprehensive analysis of the Ingram Micro incident and the known TTPs of the SafePay ransomware group, this section provides actionable guidance for security practitioners. It includes specific detection rules for identifying malicious activity, a structured incident response plan for containment and recovery, and a set of long-term strategic recommendations to harden defenses against similar threats.

### Detection Rules

The following rules are designed for use in various security platforms to detect SafePay activity at different stages of the attack lifecycle.

#### YARA

These YARA rules can be used to scan files on disk or in memory to identify the SafePay ransomware binary. They are based on unique strings and code structures observed during forensic analysis.

Code snippet

rule SafePay\_Ransomware\_Strings {  
 meta:  
 description = "Detects unique strings associated with SafePay ransomware notes and behavior."  
 author = "Senior Cybersecurity Analyst"  
 date = "2025-10-26"  
 reference = "[8, 31, 32]"  
 strings:  
 $note\_filename = "readme\_safepay.txt" wide ascii  
 $note\_greeting = "Greetings! Your corporate network was attacked by Safepay team." wide ascii  
 $ext = ".safepay" wide ascii  
 $mutex\_pattern = "Global\\{victim-id}" wide ascii // Illustrative pattern  
 condition:  
 uint16(0) == 0x5a4d and (2 of them)  
}  
  
rule SafePay\_Anti\_Recovery\_Commands {  
 meta:  
 description = "Detects embedded command-line strings used by SafePay to inhibit system recovery."  
 author = "Senior Cybersecurity Analyst"  
 date = "2025-10-26"  
 reference = "[31]"  
 strings:  
 $vssadmin = "vssadmin delete shadows /all /quiet" ascii wide  
 $wmic = "wmic shadowcopy delete" ascii wide  
 $bcdedit\_recovery = "bcdedit /set{default} recoveryenabled no" ascii wide  
 $bcdedit\_boot = "bcdedit /set{default} bootstatuspolicy ignoreallfailures" ascii wide  
 condition:  
 uint16(0) == 0x5a4d and any of them  
}  
  
rule SafePay\_Code\_Structure\_Signatures {  
 meta:  
 description = "Detects code-level artifacts and cryptographic constants seen in SafePay, linking it to LockBit and other families."  
 author = "Senior Cybersecurity Analyst"  
 date = "2025-10-26"  
 reference = "[28, 32]"  
 strings:  
 // CRC32 polynomial 0x4c11db7 used for import resolution  
 $crc32\_poly = { B7 DB 11 4C }  
 // Use of MurmurHash, also seen in Conti  
 $murmur\_seed = { FF FF FF FF } // Common seed value  
 condition:  
 uint16(0) == 0x5a4d and all of them  
}

#### Sigma

These SIEM-agnostic Sigma rules are designed to detect behavioral indicators of a SafePay intrusion based on log data.

YAML

title: Suspicious VPN Login Pattern  
id: 5f8a3d1b-4c2e-4b9f-8d7a-1c6f0e9b4a5c  
status: stable  
description: Detects a high number of failed VPN login attempts from a single source IP address followed by a successful login, indicative of a password spraying or brute-force attack.  
references:  
 - [30]  
 - [32]  
logsource:  
 product: vpn  
 category: authentication  
detection:  
 selection\_fail:  
 action: 'login'  
 status: 'failure'  
 selection\_success:  
 action: 'login'  
 status: 'success'  
 timeframe: 10m  
 condition: selection\_fail | count(source\_ip) > 20 and 1 of selection\_success  
falsepositives:  
 - Legitimate user repeatedly entering incorrect password  
level: high

YAML

title: Shadow Copy Deletion via Command Line  
id: 8c1b2f9e-3a4d-4e8c-9b0a-5d6f7a8b9c0d  
status: stable  
description: Detects the execution of commands used to delete Volume Shadow Copies, a common ransomware tactic to inhibit system recovery.  
references:  
 - [31]  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection\_vssadmin:  
 Image|endswith: '\vssadmin.exe'  
 CommandLine|contains|all:  
 - 'delete'  
 - 'shadows'  
 selection\_wmic:  
 Image|endswith: '\wmic.exe'  
 CommandLine|contains|all:  
 - 'shadowcopy'  
 - 'delete'  
 condition: 1 of selection\_\*  
falsepositives:  
 - Legitimate administrative activity (should be rare and investigated)  
level: critical

YAML

title: PowerShell Network Share Discovery  
id: a2d4e6f8-1b3c-4a7d-8b9c-0d1f2e3a4b5c  
status: stable  
description: Detects PowerShell command line patterns consistent with network share enumeration scripts like ShareFinder.ps1.  
references:  
 - [29]  
 - [28]  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection:  
 Image|endswith:  
 - '\powershell.exe'  
 - '\pwsh.exe'  
 CommandLine|contains:  
 - 'Invoke-ShareFinder'  
 - 'Net.Sockets.TCPClient'  
 - 'Get-NetShare'  
 condition: selection  
falsepositives:  
 - Legitimate network administration scripts  
level: medium

### Incident Response Procedures

A swift and structured response is critical to minimizing the impact of a ransomware attack.

#### Immediate Containment (First 1-2 Hours)

1. **Isolate Affected Systems:** Immediately disconnect compromised endpoints and servers from the network to prevent further lateral movement and encryption. This can be done by unplugging network cables, disabling switch ports, or using EDR host isolation features.
2. **Block Malicious Infrastructure:** Ingest all known SafePay IOCs (IPs, domains) into firewalls, proxies, and DNS blocklists to sever any active C2 communication channels.
3. **Secure Remote Access:** Disable the corporate VPN immediately to prevent further unauthorized access. Preserve VPN logs for forensic analysis.
4. **Initiate Credential Reset:** Trigger a forced password reset for all user accounts, prioritizing privileged accounts (Domain Admins, service accounts). If feasible, re-enroll MFA for all users.6
5. **Audit and Revoke Partner Access:** For organizations that provide services to others (e.g., MSPs), immediately begin an audit of all delegated administrative privileges, such as Microsoft GDAP. As a precaution, revoke or severely restrict permissions for any potentially compromised partner or system, mirroring the defensive actions taken by MSPs during the Ingram breach.21

#### Eradication & Recovery (Days 1-7)

1. **Preserve Forensic Evidence:** Before wiping any systems, ensure that forensic images (full disk and memory captures) are taken from a representative sample of compromised machines. This is crucial for the investigation.
2. **Rebuild from a Known-Good State:** Do not attempt to "clean" infected systems. The only safe method is to re-image them using a trusted, golden image of the operating system and applications.
3. **Secure Data Restoration:** Restore data from clean, offline, and preferably immutable backups. Before restoring, use a secure, isolated environment to mount the backups and scan them with up-to-date antivirus and YARA rules to ensure no dormant malware is reintroduced into the production environment.39
4. **Phased Restoration:** Bring systems back online in a controlled, phased manner, starting with the most critical services. Continuously monitor network traffic and endpoint logs for any signs of residual malicious activity.

### Long-Term Strategic Hardening

To build resilience against future attacks, organizations must address the root causes exploited by SafePay.

#### Identity and Access Management

* **Mandate Phishing-Resistant MFA:** Enforce strong, phishing-resistant MFA (e.g., FIDO2/WebAuthn) for all remote access points (VPN, RDP), cloud administration portals, and privileged accounts. This is the single most effective control to prevent credential-based intrusions like the one that befell Ingram Micro.9
* **Implement the Principle of Least Privilege (PoLP):** Aggressively audit and reduce all user and system permissions to the absolute minimum required for their function. This is especially critical for third-party and partner access (e.g., GDAP), where roles should be time-bound and restricted to specific necessary tasks.21

#### Infrastructure Hardening

* **Harden VPN and Remote Access Infrastructure:** Regularly apply security patches to all internet-facing appliances. Audit configurations to disable legacy protocols, enforce strong encryption, and ensure robust logging and monitoring are in place.30
* **Implement Network Segmentation:** Divide the corporate network into smaller, isolated segments based on business function and trust level. Use internal firewalls to restrict traffic between segments, preventing an attacker who compromises one area (e.g., user workstations) from easily moving to another (e.g., critical servers or backup infrastructure).14

#### Proactive Defense & Communication

* **Deploy and Tune EDR:** An effective Endpoint Detection and Response (EDR) solution is essential for detecting the behavioral TTPs of ransomware, such as LOLBin abuse, credential dumping, and process termination. Ensure the EDR is configured in block mode and that alerts are monitored 24/7.30
* **Develop a Transparent Crisis Communication Plan:** Learn from the communication failures of the Ingram Micro incident. Develop a pre-approved crisis communication plan that prioritizes rapid, transparent, and actionable updates for customers and supply chain partners. The plan should have clear templates and designated spokespeople to ensure trust is maintained, even during a significant security event.4

## Conclusion

The July 2025 ransomware attack on Ingram Micro was a watershed moment for the global IT industry, serving as a powerful and costly reminder of the systemic risks embedded within highly interconnected digital supply chains. The incident was not the result of an exotic zero-day exploit but rather the successful exploitation of fundamental security gaps in identity and access management by a determined and capable adversary, the SafePay ransomware group.

The analysis reveals several critical conclusions. First, the impact of a cyberattack on a central infrastructure node is amplified exponentially by the dependencies of its ecosystem. The financial and operational damage to Ingram Micro was severe, but the cascading disruption to its thousands of partners defined the true scale of the crisis. This demonstrates that for organizations in such pivotal roles, cybersecurity is not merely an internal IT issue but a matter of ecosystem stability and a core component of their value proposition.

Second, trust in the digital supply chain is a tangible asset that is encoded in administrative permissions and API access. The immediate reaction of MSPs to revoke Ingram Micro's GDAP privileges was a rational act of self-preservation that exposed the fragility of this trust. When a central partner is breached, the implicit trust model collapses, forcing a rapid and disruptive decoupling that further exacerbates the crisis.

Finally, the incident underscores the inadequacy of reactive and opaque communication strategies. In an environment where partners depend on real-time information to manage their own operations and customer relationships, a communication vacuum fuels uncertainty and erodes confidence far more than the technical details of the breach itself.

Moving forward, the lessons from this attack must catalyze a fundamental shift in how organizations approach supply chain security. Resilience cannot be achieved in isolation. It requires a collective commitment to enforcing robust security baselines, including mandatory MFA and the principle of least privilege, across all partners. It demands a move toward Zero Trust architectures that assume breach and limit the blast radius of any single compromise. Above all, it requires building a foundation of transparency and collaboration, ensuring that when an incident inevitably occurs, the response strengthens the ecosystem rather than shattering it. The Ingram Micro attack was a painful stress test for the entire IT supply chain; the ultimate outcome will be determined by whether the industry heeds its clear and urgent warnings.

#### Works cited

1. The Ingram Micro Ransomware Hack: What Happened and Why It ..., accessed August 14, 2025, <https://blacksmithinfosec.com/the-ingram-micro-ransomware-hack-what-happened-and-why-it-matters/>
2. How Ingram Micro Overcame a Major Ransomware Attack | BlackFog, accessed August 14, 2025, <https://www.blackfog.com/how-ingram-micro-overcame-a-major-ransomware-attack/>
3. Ingram Micro Confirms Cybersecurity Breach in 2025 - TECHi, accessed August 14, 2025, <https://www.techi.com/two-takes/ingram-micro-confirms-cybersecurity-breach/>
4. Ingram Micro begins restarting orders for limited customers • The ..., accessed August 14, 2025, <https://www.theregister.com/2025/07/09/ingram_micro_restarts_orders_for/>
5. The Ingram Micro Ransomware Attack: Lessons Learned - Proven Data, accessed August 14, 2025, <https://www.provendata.com/blog/ingram-micro-ransomware-attack/>
6. SafePay ransomware threatens to leak 3.5TB of Ingram Micro data, accessed August 14, 2025, <https://www.bleepingcomputer.com/news/security/safepay-ransomware-threatens-to-leak-35tb-of-ingram-micro-data/>
7. Ingram Micro Working Through Ransomware Attack by SafePay ..., accessed August 14, 2025, <https://www.msspalert.com/news/ingram-micro-working-through-ransomware-attack-by-safepay-group>
8. Ingram Micro outage caused by SafePay ransomware attack, accessed August 14, 2025, <https://www.bleepingcomputer.com/news/security/ingram-micro-outage-caused-by-safepay-ransomware-attack/>
9. Ingram Micro Struck by SafePay Ransomware Attack - Ampcus Cyber, accessed August 14, 2025, <https://www.ampcuscyber.com/shadowopsintel/safepay-ransomware-cripples-ingram-micro/>
10. Ingram Micro Suffers Huge Ransomware Attack - Tech.co, accessed August 14, 2025, <https://tech.co/news/ingram-micro-data-breach>
11. Ingram Micro Legacy Systems Outage: How the SafePay Ransomware Attack Disrupted Global Supply Chain Operations - Rescana, accessed August 14, 2025, <https://www.rescana.com/post/ingram-micro-legacy-systems-outage-how-the-safepay-ransomware-attack-disrupted-global-supply-chain>
12. Ingram Micro's Breach: Ransomware and the Trust Gap it Opened | ChannelE2E, accessed August 14, 2025, <https://www.channele2e.com/news/too-big-to-fail-too-quiet-to-reassure-ingram-micros-breach-and-the-trust-gap-it-opened>
13. information | Ingram Micro, accessed August 14, 2025, <https://www.ingrammicro.com/en-us/information>
14. The Ingram Micro Hack and Increasing Concerns Around Digital Supply Chain Security, accessed August 14, 2025, <https://www.mbtmag.com/cybersecurity/blog/22947387/the-ingram-micro-hack-and-increasing-concerns-around-digital-supply-chain-security>
15. Ingram Micro Ransomware Attack: Critical Supply Chain Vulnerability Exposes IT Distribution Sector Risks - Kahana, accessed August 14, 2025, <https://kahana.co/blog/ingram-micro-ransomware-attack-critical-supply-chain-vulnerability-2025>
16. Ransomware Attack Disrupts Ingram Micro Operations - Distribution Strategy Group, accessed August 14, 2025, <https://distributionstrategy.com/ransomware-attack-disrupts-ingram-micro-operations/>
17. Project Nightingale - Wikipedia, accessed August 14, 2025, <https://en.wikipedia.org/wiki/Project_Nightingale>
18. Google's Project Nightingale highlights the necessity of data science ethics review - PubMed, accessed August 14, 2025, <https://pubmed.ncbi.nlm.nih.gov/32064790/>
19. Ingram Micro Ransomware Attack: A Comprehensive Overview - TeckPath, accessed August 14, 2025, <https://teckpath.com/ingram-micro-ransomware-attack-overview/>
20. Ingram Micro Issues Statement Regarding Cybersecurity Incident, accessed August 14, 2025, <https://ir.ingrammicro.com/press-releases/detail/945/ingram-micro-issues-statement-regarding-cybersecurity-incident>
21. Ingram Micro shutdown due to ransomware : r/msp - Reddit, accessed August 14, 2025, <https://www.reddit.com/r/msp/comments/1lsdzre/ingram_micro_shutdown_due_to_ransomware/>
22. This Is Insane : r/msp - Reddit, accessed August 14, 2025, <https://www.reddit.com/r/msp/comments/1lurs3a/this_is_insane/>
23. Ingram Micro Update : r/msp - Reddit, accessed August 14, 2025, <https://www.reddit.com/r/msp/comments/1ltxgfh/ingram_micro_update/>
24. Ingram Breach- Limiting the Ingram GDAP Roles : r/msp - Reddit, accessed August 14, 2025, <https://www.reddit.com/r/msp/comments/1ltf5i6/ingram_breach_limiting_the_ingram_gdap_roles/>
25. A Deeper Look at SafePay Following Ingram Micro Attack | Channel Insider, accessed August 14, 2025, <https://www.channelinsider.com/news-and-trends/safepay-ransomware-threat-group/>
26. SafePay Ransomware: An Emerging Threat in 2025 - Check Point Software, accessed August 14, 2025, <https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/safepay-ransomware/>
27. Ransomware Attack Halts Ingram Micro Operations - Bank Info Security, accessed August 14, 2025, <https://www.bankinfosecurity.com/ransomware-attack-halts-ingram-micro-operations-a-28908>
28. SafePay ransomware: The fast-rising threat targeting MSPs - Acronis, accessed August 14, 2025, <https://www.acronis.com/en-us/tru/posts/safepay-ransomware-the-fast-rising-threat-targeting-msps/>
29. SafePay ransomware explained: IOCs, TTPs, and defense strategies | ThreatLocker Blog, accessed August 14, 2025, <https://www.threatlocker.com/blog/safepay-ransomware-explained-iocs-ttps-and-defense-strategies>
30. Ingram Micro Ransomware Attack: Strengthening Supply Chain Risk Assessment, accessed August 14, 2025, <https://firecompass.com/ingram-micro-ransomware-attack-strengthening-supply-chain-risk-assessment/>
31. Weak Passwords Led to (SafePay) Ransomware…Yet Again - NCC Group, accessed August 14, 2025, <https://www.nccgroup.com/us/research-blog/weak-passwords-led-to-safepay-ransomware-yet-again/>
32. SafePay: The new kid on the block | by DCSO CyTec Blog | Medium, accessed August 14, 2025, <https://medium.com/@DCSO_CyTec/safepay-the-new-kid-on-the-block-4141188a626d>
33. Unmasking the SafePay Ransomware Group - Infosecurity Magazine, accessed August 14, 2025, <https://www.infosecurity-magazine.com/news-features/unmasking-safepay-ransomware-group/>
34. What is SafePay Ransomware? - Everything You Need to Know - Red Piranha, accessed August 14, 2025, <https://redpiranha.net/news/what-is-safepay-ransomware-everything-you-need-know>
35. SafePay Ransomware Report - Quorum Cyber, accessed August 14, 2025, <https://www.quorumcyber.com/malware-reports/safepay-ransomware-report/>
36. SafePay Ransomware Targets 260+ Victims Across Various Countries - Cyber Press, accessed August 14, 2025, <https://cyberpress.org/safepay-ransomware-targets-260-victims/>
37. #StopRansomware: RansomHub Ransomware | CISA, accessed August 14, 2025, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
38. Emerging Threat Actor: SafePay Ransomware - Halcyon, accessed August 14, 2025, <https://www.halcyon.ai/blog/emerging-threat-actor-safepay-ransomware>
39. What are YARA Rules? A Complete Guide with Examples - Veeam, accessed August 14, 2025, <https://www.veeam.com/blog/yara-rules-malware-detection-analysis.html>