VPN
Initial access goldmines

Erik Westhovens

05-01-2026

Ransomwared
CTI Report

1. Executive Summary

Between 2023 and 2025, the global threat landscape has undergone a notable shift in how adversaries achieve initial access to enterprise environments. Threat actors—including ransomware affiliates, access brokers, and state-aligned intrusion sets—have increasingly deprioritized traditional entry methods such as phishing emails, malicious document delivery, and commodity malware. Instead, they have concentrated their efforts on the exploitation and abuse of internet-facing VPN and remote access appliances. This strategic pivot reflects a broader adaptation to improving endpoint detection capabilities and growing user awareness, which have raised the cost and reduced the reliability of user-centric attack vectors.

SSL VPN gateways and similar remote access technologies have emerged as particularly attractive targets. These systems are designed to provide trusted, authenticated access to internal networks and are frequently deployed at the network perimeter with broad connectivity into corporate environments. In many organizations, VPN appliances are implicitly trusted, lightly monitored, and operationally siloed from standard endpoint security and logging pipelines. As a result, successful compromise of a VPN device or VPN authentication mechanism often grants adversaries immediate, high-value access that bypasses multiple layers of defense.

Observed intrusion campaigns during this period demonstrate that VPN compromise can provide attackers with access to privileged network segments, authenticated user sessions, and reusable credential material without generating alerts from endpoint detection and response (EDR) platforms. Unlike phishing-based intrusions, which often leave artifacts on user endpoints or rely on malware execution, VPN-centric access paths frequently enable attackers to operate entirely within the bounds of “legitimate” authentication and network activity. This dynamic significantly reduces detection opportunities during the earliest and most critical stages of an intrusion.

A key operational advantage for threat actors is that VPN-based access often allows them to blend seamlessly into normal administrative and remote-work traffic. Once authenticated, attackers may leverage native operating system tools, built-in administrative utilities, and standard network protocols to conduct reconnaissance, move laterally, and escalate privileges. This living-off-the-land approach minimizes the need to deploy custom malware and reduces reliance on command-and-control infrastructure during the early phases of the intrusion. As a result, many VPN-originated compromises exhibit extended dwell times, with attackers maintaining access for days or weeks before being detected—if detection occurs at all.

Across multiple investigations, successful VPN compromise has frequently enabled attackers to harvest credentials, access directory services, and enumerate internal resources within minutes of initial entry. In environments with flat network architectures or limited segmentation, this access can rapidly expand to include domain controllers, file servers, virtualization platforms, and backup infrastructure. The implicit trust afforded to VPN connections often means that network security controls treat attacker activity as indistinguishable from that of legitimate remote users or administrators.

Another defining trend observed during this period is the decoupling of initial access from final impact. In many cases, ransomware deployment is delayed or never occurs. Instead, attackers use their VPN-based foothold to quietly stage operations that include sensitive data discovery, selective exfiltration, and preparation for extortion. This shift reflects a growing recognition among threat actors that encryption-based ransomware operations carry increased operational risk, visibility, and law enforcement attention. Data theft and extortion-only campaigns, by contrast, can be executed with lower noise and reduced forensic footprints while still achieving financial or strategic objectives.

In ransomware-driven intrusions that do progress to encryption, VPN compromise often enables a level of preparation that significantly increases the likelihood of success. Prior to deploying ransomware, attackers frequently disable or tamper with backup systems, identify hypervisors and critical servers, and ensure they possess sufficient privileges to deploy payloads at scale. By the time ransomware is executed, the organization

is already operating from a position of severe disadvantage, with limited recovery options and incomplete visibility into the scope of compromise.

The growing prevalence of VPN-centric intrusions also highlights systemic weaknesses in how organizations manage and monitor perimeter infrastructure. VPN appliances are often treated as “set-and-forget” components, with patching cycles that lag behind those of endpoints and servers. Firmware vulnerabilities—particularly those enabling remote code execution or authentication bypass—are frequently exploited within days or weeks of disclosure, yet many organizations struggle to apply patches quickly due to availability concerns, change management processes, or lack of asset visibility. In several high-impact cases, attackers exploited vulnerabilities that had been publicly disclosed and patched but remained unaddressed in production environments.

Even in scenarios where no software vulnerability is exploited, credential-based access to VPNs remains a persistent risk. Password reuse, weak authentication policies, legacy VPN portals, and MFA fatigue attacks continue to provide attackers with reliable entry points. Long-lived VPN sessions, insufficient session invalidation following credential changes, and limited monitoring of anomalous authentication behavior further compound this risk. Once established, such access is difficult to distinguish from legitimate remote work activity without dedicated detection logic and contextual analysis.

From a defensive perspective, VPN-centric intrusions expose a critical gap between perimeter security and internal detection capabilities. Many organizations collect limited VPN telemetry, retain logs for short periods, or fail to correlate VPN access data with downstream authentication and network activity. As a result, early indicators—such as anomalous login locations, unusual session durations, or rapid internal reconnaissance following VPN authentication—are often missed. By the time suspicious behavior is detected on endpoints or servers, attackers may already have achieved their objectives.

The implications of this trend extend beyond technical security concerns. VPN compromise frequently results in regulatory exposure, particularly in sectors subject to data protection and critical infrastructure regulations. Unauthorized access through a trusted remote access system can lead to large-scale data breaches, operational disruption, and non-compliance with frameworks such as NIS2, GDPR, and sector-specific resilience requirements. The silent nature of many VPN-based intrusions also increases the likelihood that incidents go undetected for extended periods, exacerbating legal, financial, and reputational impact.

This report examines the evolution of VPN-centric intrusion chains between 2023 and 2025, focusing on how and why threat actors have elevated VPN appliances to primary initial access targets. It analyzes the threat actors involved, the techniques used to compromise and abuse VPN infrastructure, and the post-exploitation tradecraft that enables sustained, low-noise operations. Particular attention is given to the operational patterns observed after initial access, including credential harvesting, lateral movement, command-and-control approaches, and impact preparation.

In addition to documenting adversary behavior, this report provides actionable defensive guidance designed to help organizations reduce risk and improve detection. Emphasis is placed on early-stage visibility, rapid containment following suspected VPN compromise, and architectural measures that limit the blast radius of remote access systems. Rather than treating VPN security as a narrow patching or authentication problem, this report frames VPN infrastructure as a high-risk, high-value attack surface that must be monitored and defended with the same rigor applied to domain controllers, identity platforms, and other Tier-0 assets.

Ultimately, the continued exploitation of VPN appliances underscores a broader lesson in modern intrusion defense: as attackers adapt to hardened endpoints and improved email security, they will increasingly target trusted access paths that sit outside traditional detection models. Organizations that fail to reassess the role of VPNs in their threat models—and that continue to view them as mere connectivity tools rather than strategic

security assets—will remain vulnerable to silent, high-impact compromises that are discovered only after significant damage has occurred.

2. Threat Actor Overview

VPN-based initial access is leveraged by a **diverse and increasingly specialized ecosystem of threat actors**, spanning financially motivated ransomware groups, initial access brokers (IABs), and state-aligned intrusion sets. What unites these actors is not ideology or end goal, but a shared recognition that VPN and remote access infrastructure provides a uniquely efficient, low-friction path into enterprise environments. The convergence of perimeter exposure, implicit trust, and inconsistent monitoring has made VPN compromise a foundational capability across multiple threat models.

Rather than being confined to a single class of adversary, VPN abuse now functions as a **horizontal enabler** across the threat landscape. This section outlines the primary actor categories involved, highlights representative groups, and examines the growing operational separation between initial access and post-exploitation activities.

2.1 Financially Motivated Ransomware Actors

Financially motivated ransomware groups remain the most visible users of VPN-based initial access. These actors prioritize speed, reliability, and scale, and VPN compromise satisfies all three requirements. By bypassing phishing, malware delivery, and user interaction, ransomware affiliates significantly reduce uncertainty in the earliest phase of an intrusion.

A prominent example is **Akira**, which has repeatedly demonstrated a preference for perimeter-based access vectors. Akira-affiliated intrusions frequently begin with exploitation of VPN appliances or abuse of valid VPN credentials, followed by rapid internal reconnaissance and credential harvesting. Once inside, Akira operators commonly rely on living-off-the-land techniques, including native Windows administration tools, to move laterally and prepare for impact. Notably, Akira intrusions often exhibit a deliberate pacing: attackers may delay ransomware deployment while assessing backup coverage, identifying high-value systems, or staging data for exfiltration.

Similarly, **Black Basta** has been observed leveraging VPN access to enable aggressive post-compromise activity. In contrast to slower-moving actors, Black Basta affiliates tend to exploit VPN access as a springboard for rapid escalation. Within hours of initial access, operators frequently attempt domain-wide reconnaissance, lateral movement via PsExec or SMB, and privilege escalation. This operational tempo suggests a high degree of confidence in VPN-derived access and an expectation that defenders are unlikely to detect anomalous activity originating from authenticated VPN sessions.

LockBit represents a slightly different model. While LockBit affiliates certainly exploit VPN vulnerabilities directly, the group is also known for leveraging VPN access obtained through third parties. LockBit's scale and affiliate-driven structure make it particularly well-suited to consuming pre-established access, allowing affiliates to focus on execution rather than discovery. In such cases, VPN access may already be days or weeks old by the time ransomware operators become active, further complicating attribution and incident reconstruction.

Across ransomware groups, a consistent pattern emerges: VPN access is treated as a **high-confidence foothold** that enables attackers to operate with reduced risk during the most sensitive phases of an intrusion. This confidence has directly contributed to longer dwell times and more thorough impact preparation.

2.2 Initial Access Brokers (IABs)

A critical and often underappreciated component of the VPN threat ecosystem is the role of initial access brokers. These actors specialize exclusively in obtaining and monetizing access to corporate networks, typically without participating in subsequent exploitation or impact activities.

IABs frequently target VPN infrastructure due to its scalability and resale value. A single compromised VPN credential or appliance can yield persistent access to an environment and command premium prices on underground marketplaces. Unlike phishing-derived access, VPN access is often stable, repeatable, and difficult for defenders to invalidate comprehensively.

Operationally, IABs employ a range of techniques, including:

- Exploitation of unpatched VPN vulnerabilities
- Credential stuffing using previously breached passwords
- Brute-force attacks against legacy VPN portals
- Abuse of weak or inconsistent MFA implementations

Once access is established, brokers may perform minimal validation—such as confirming internal reachability or privilege level—before advertising the access for sale. In some cases, they maintain access for extended periods, refreshing credentials or sessions to increase reliability for buyers.

The existence of a mature IAB market has fundamentally altered the threat landscape. Ransomware affiliates no longer need to invest in perimeter reconnaissance or exploit development, allowing them to scale operations and focus on post-compromise efficiency. This division of labor has also reduced the operational barrier to entry for less technically sophisticated actors, accelerating the overall volume of VPN-based intrusions.

2.3 State-Aligned and Espionage-Focused Actors

VPN infrastructure is not solely abused by financially motivated actors. State-aligned and espionage-focused groups have also demonstrated sustained interest in VPN and edge device compromise, particularly for long-term access and strategic intelligence collection.

One such actor is **UNC5221**, which has been associated with exploitation of edge devices, including VPN appliances, for persistent access. Unlike ransomware groups, UNC5221 and similar actors prioritize stealth, durability, and operational security over speed. VPN compromise provides an ideal entry point for these objectives, enabling actors to blend into normal administrative traffic and avoid the need for malware deployment on endpoints.

State-aligned actors often leverage VPN access to:

- Establish long-term footholds for intelligence collection
- Access sensitive internal systems without triggering endpoint alerts
- Pivot into cloud or hybrid identity environments
- Maintain access across patch cycles and infrastructure changes

In contrast to ransomware-driven intrusions, these campaigns may persist for months, with minimal observable impact until discovery. This reinforces the notion that VPN compromise is not merely a precursor to ransomware, but a strategic access vector applicable across multiple threat objectives.

2.4 Decoupling of Initial Access and Post-Exploitation

One of the most significant developments observed between 2023 and 2025 is the **decoupling of initial access from post-exploitation and impact activities**. In earlier threat models, a single actor or tightly coordinated group often controlled the full intrusion lifecycle. Today, that lifecycle is increasingly fragmented across specialized roles.

In VPN-centric intrusions, this separation is particularly pronounced. Initial access may be obtained by:

- An IAB exploiting a VPN vulnerability
- A scanning-focused actor harvesting credentials
- A state-aligned group establishing persistent access

That access may then be:

- Sold on underground forums
- Shared within affiliate networks
- Reused months later by a different actor entirely

As a result, defenders frequently observe intrusions where the actor conducting ransomware deployment bears little resemblance—technically or operationally—to the actor that originally compromised the VPN. Tooling, tradecraft, and objectives may differ significantly, complicating attribution and response.

This decoupling also increases defender risk. VPN access that appears low-risk or inactive may later be weaponized with little warning. Organizations that treat VPN compromise as a transient or contained incident may underestimate its long-term implications, particularly if credentials, session tokens, or appliance-level persistence mechanisms remain unaddressed.

2.5 Implications for Attribution and Defense

The diversity of actors leveraging VPN-based access has direct implications for both threat attribution and defensive strategy. From an attribution perspective, VPN compromise blurs traditional indicators such as malware families, command-and-control infrastructure, and phishing lures. Multiple actors may operate sequentially—or even concurrently—within the same environment, each using the same initial access point.

From a defensive standpoint, this diversity underscores the need to shift focus away from actor-specific indicators and toward **access-centric detection and response**. Rather than attempting to predict which group is most likely to target an organization, defenders must assume that **any exposed or poorly monitored VPN infrastructure will eventually be abused**, regardless of industry or geography.

Ultimately, VPN-based initial access represents a shared capability across the modern threat ecosystem. Its widespread adoption by financially motivated, criminal, and state-aligned actors alike highlights its effectiveness—and its danger. Understanding the actors involved is therefore less about cataloging names and more about recognizing the structural weaknesses that enable such a wide range of adversaries to succeed.

3. Evolution & Operational Trends (2023–2025)

Between 2023 and 2025, the operational use of VPN and remote access infrastructure by threat actors evolved from an opportunistic tactic into a **core pillar of modern intrusion strategy**. This evolution was not driven by a single breakthrough vulnerability or toolset, but rather by a convergence of defensive improvements elsewhere and persistent structural weaknesses at the network perimeter. Over this period, VPN compromise transitioned from a "high-reward but situational" technique into a **reliable, repeatable, and scalable initial access vector**.

This section examines how attacker behavior matured over time, highlighting key trends in targeting, tradecraft, and operational decision-making.

3.1 2023: Opportunistic Exploitation and Tactical Experimentation

In 2023, VPN exploitation was already well understood by threat actors, but its use was largely **opportunistic rather than strategic**. Attackers primarily focused on newly disclosed vulnerabilities in popular SSL VPN products, often exploiting them en masse shortly after public disclosure. These campaigns were typically characterized by broad internet scanning, limited targeting, and rapid follow-on activity.

At this stage, VPN compromise was often treated as a means to an end rather than a strategic foothold. Once access was obtained, attackers moved quickly to deploy malware, escalate privileges, or pivot internally. Persistence on the VPN appliance itself was uncommon, and attackers showed limited concern for long-term access stability. Detection, while still challenging, was more feasible due to the relatively noisy nature of post-compromise activity.

Operationally, many 2023-era VPN intrusions resembled traditional breach patterns, with the VPN serving merely as an alternative entry point. Phishing and malware delivery remained dominant initial access vectors, and VPN exploitation was frequently combined with these techniques rather than replacing them. Nonetheless, successful intrusions demonstrated to attackers that VPN compromise could bypass multiple defensive layers simultaneously, planting the seeds for broader adoption.

3.2 2024: Normalization and Process Refinement

By 2024, VPN-centric access had moved firmly into the mainstream of attacker playbooks. Multiple high-impact VPN vulnerabilities were exploited at scale, and threat actors began to recognize that **VPN access offered a level of reliability unmatched by user-focused techniques**. This period marked a transition from opportunistic exploitation to **process-driven operations**.

Attackers increasingly integrated VPN compromise into standardized intrusion workflows. Rather than rushing immediately to deploy ransomware or malware, many actors adopted a phased approach:

1. Establish VPN access
2. Validate internal reachability and privilege level
3. Conduct quiet reconnaissance
4. Harvest credentials and session material
5. Delay impact until conditions were optimal

This shift reflected a growing emphasis on operational security and risk management. Threat actors became more selective in how they used VPN access, prioritizing stealth and control over speed. Living-off-the-land techniques gained prominence, allowing attackers to operate almost entirely within the bounds of legitimate administrative behavior.

Another notable trend in 2024 was the increased role of **initial access brokers**. VPN-derived access became a commodity, traded and reused across multiple campaigns. This further decoupled initial access from post-exploitation and reinforced the perception of VPN compromise as a durable asset rather than a one-time event.

Defenders, meanwhile, struggled to adapt. Many organizations continued to treat VPN appliances as infrastructure components rather than security-critical assets. Patch cycles lagged behind vulnerability disclosures, and VPN telemetry remained poorly integrated into SOC workflows. This imbalance between attacker maturity and defensive posture accelerated the adoption of VPN-centric intrusions.

3.3 2025: Strategic Weaponization of the Perimeter

By 2025, VPN and edge device compromise had become a **strategic capability** rather than a tactical option. Threat actors demonstrated a clear understanding of the systemic weaknesses associated with perimeter infrastructure and tailored their operations accordingly.

A defining characteristic of this period was the **intentional delay between initial access and observable malicious activity**. In many incidents, attackers maintained VPN access for extended periods without triggering alerts, using the connection intermittently to avoid suspicion. This approach allowed them to:

- Monitor defender behavior
- Identify logging gaps
- Time operations to coincide with holidays or staffing shortages
- Coordinate multi-stage attacks across environments

VPN compromise was also increasingly used as a gateway to **identity-centric attacks**, particularly in hybrid and cloud-connected environments. Access obtained through VPNs was leveraged to enumerate directory services, abuse trust relationships, and pivot into identity platforms without relying on endpoint compromise. This trend reflected a broader shift toward identity as the primary control plane in enterprise networks.

Additionally, attackers began to prioritize **high-impact internal assets earlier in the intrusion lifecycle**. Backup systems, virtualization platforms, and administrative management servers were often targeted shortly after VPN access was established. This reduced the need for widespread lateral movement and minimized exposure while maximizing potential impact.

3.4 Decline of User-Centric Initial Access

One of the most consequential trends observed during this period was the **relative decline of phishing and malware-based initial access** for high-impact intrusions. While these techniques did not disappear, their effectiveness diminished in environments with mature email security and endpoint detection capabilities.

VPN compromise offered several advantages over user-centric methods:

- No reliance on user interaction
- Reduced exposure to EDR and antivirus controls
- Higher likelihood of privileged or semi-privileged access
- Greater persistence and reusability

As a result, attackers increasingly reserved phishing for low-value or opportunistic campaigns, while using VPN-centric access for targeted, high-impact operations. This bifurcation reflects a rational allocation of resources based on expected return and operational risk.

3.5 Increased Focus on Stealth and Dwell Time

Across all actor categories, the period from 2023 to 2025 saw a marked increase in **dwell time following VPN compromise**. Rather than pursuing immediate impact, attackers emphasized persistence, reconnaissance, and preparation. In some cases, VPN access was maintained for weeks before any disruptive activity occurred.

This extended dwell time was enabled by:

- Limited VPN log retention
- Infrequent review of authentication anomalies
- Overreliance on MFA as a compensating control
- Poor visibility into management-plane activity

From an attacker perspective, this approach reduced the likelihood of detection and increased the probability of successful extortion or espionage. From a defender perspective, it eroded the traditional assumption that rapid detection of malicious payloads equates to effective security.

3.6 Strategic Implications of the Trend

The evolution of VPN-centric intrusions reflects a broader strategic reality: **as defenders harden endpoints and users, attackers will continue to target trusted access paths that sit outside conventional detection models**. VPN infrastructure, by design, bridges external and internal trust zones, making it an ideal exploitation point when not rigorously monitored.

By 2025, VPN compromise was no longer an emerging trend—it was a normalized, expected component of serious intrusion campaigns. Organizations that failed to adapt their threat models accordingly were repeatedly caught off guard, often discovering intrusions only after data exfiltration or operational disruption had occurred.

3.7 Summary

From 2023 to 2025, VPN exploitation evolved from a tactical alternative into a **foundational element of modern intrusion operations**. Attackers refined their methods, professionalized their workflows, and demonstrated a clear preference for VPN-based access over noisier, less reliable techniques. This evolution underscores the need for defenders to reassess the role of VPNs within their security architecture and to treat perimeter infrastructure as a first-class security concern rather than a passive conduit for remote access.

.

4. Initial Access Vectors

VPN and remote access infrastructure emerged as one of the most consistently abused initial access vectors across financially motivated and state-aligned intrusion campaigns. Threat actors demonstrated a clear preference for compromising VPN technologies due to their exposure, privileged network position, and the operational trust placed in authenticated remote access. This section details the primary initial access vectors observed, with specific reference to commonly targeted vendors and platforms.

4.1 Exploitation of VPN Appliance Vulnerabilities

The most direct and high-impact initial access vector involved the exploitation of vulnerabilities in VPN appliance firmware and management interfaces. Vendors most frequently observed in incident investigations include **Fortinet**, **Ivanti**, **SonicWall**, and **Palo Alto Networks**.

Common vulnerability classes exploited during this period included:

- Unauthenticated remote code execution (RCE)
- Command injection in web-based management interfaces
- Authentication bypass vulnerabilities
- Arbitrary file write leading to code execution

These vulnerabilities were particularly attractive because they enabled attackers to gain access without valid credentials or user interaction. In several campaigns, exploitation occurred within days of public disclosure, and in some cases prior to widespread defensive guidance being available.

Once exploited, attackers often gained shell-level access to the appliance or the ability to execute commands within the VPN context. This allowed them to extract configuration data, harvest credentials, and in some cases establish persistence directly on the device. The appliance itself effectively became a staging point for further operations.

4.2 Abuse of Valid VPN Credentials

Credential-based access remained a dominant vector, particularly in environments where VPN vulnerabilities were patched but authentication controls remained weak. Threat actors obtained VPN credentials through a variety of means, including prior data breaches, credential stuffing, brute-force attacks against legacy portals, and targeted phishing unrelated to the final intrusion phase.

Even in environments with multi-factor authentication (MFA) enabled, attackers frequently succeeded through:

- MFA fatigue or push bombing attacks
- Use of legacy VPN portals without MFA enforcement
- Exploitation of conditional access misconfigurations
- Use of stolen session cookies or refresh tokens

VPN credentials were highly valued due to their durability and reusability. Unlike endpoint compromise, which is often remediated through reimaging, VPN credentials could remain valid for extended periods, particularly when password rotation and session invalidation were inconsistently enforced.

4.3 Session Hijacking and Token Reuse

Beyond traditional credential theft, attackers increasingly leveraged VPN session hijacking techniques. In these scenarios, threat actors reused existing authenticated VPN sessions by capturing session identifiers, cookies, or tokens. This technique was particularly effective in environments where VPN sessions were long-lived or where session invalidation did not occur following password changes.

Session hijacking provided several advantages:

- Bypassed MFA entirely
- Reduced likelihood of triggering authentication alerts
- Enabled seamless blending with legitimate user activity

In hybrid environments, VPN access was sometimes combined with token abuse in identity platforms, allowing attackers to pivot from network access into cloud resources without reauthentication.

4.4 Management Plane Exposure

A recurring weakness across multiple incidents was the exposure of VPN management interfaces to the internet. Administrative portals for VPN appliances were frequently accessible from external networks, sometimes protected only by basic authentication or shared credentials.

Threat actors actively targeted these interfaces, using them to:

- Enumerate users and configuration details
- Create new VPN users or modify existing ones
- Extract logs and credentials
- Deploy appliance-level persistence mechanisms

In several cases, compromise of the management plane preceded or replaced exploitation of user-facing VPN portals. This vector was particularly damaging because it allowed attackers to manipulate the VPN infrastructure itself, undermining trust in all subsequent remote access activity.

4.5 Supply Chain and Third-Party Access

VPN access was also obtained indirectly through third-party relationships. Managed service providers (MSPs), contractors, and vendors often maintained persistent VPN connections into client environments. Compromise of these third-party credentials provided attackers with immediate access to multiple downstream organizations.

This vector was especially prevalent in environments where:

- Shared VPN credentials were used across clients
- Network segmentation for third-party access was limited
- Monitoring of vendor VPN activity was minimal

From an attacker perspective, compromising a single third-party VPN account could yield access to dozens of environments, making it a highly efficient initial access strategy.

4.6 Why VPN Initial Access Is So Effective

Across all vectors, VPN-based initial access offered several systemic advantages:

- Access occurs outside endpoint security visibility

- Activity is often indistinguishable from legitimate remote work
- VPN users are frequently granted broad network access
- Detection relies on log correlation rather than malware signatures

These advantages explain why VPN compromise became a preferred entry point for high-impact intrusions during the period under review.

4.7 Summary

Initial access via VPN and remote access infrastructure represents a convergence of technical weakness and operational trust. Whether through exploitation of vendor vulnerabilities, abuse of valid credentials, session hijacking, or management plane compromise, threat actors consistently demonstrated the ability to bypass traditional perimeter defenses and establish reliable footholds.

The continued exploitation of platforms from vendors such as **Fortinet**, **Ivanti**, **SonicWall**, and **Palo Alto Networks** underscores that this risk is systemic rather than vendor-specific. As long as VPN appliances remain exposed, trusted, and under-monitored, they will continue to function as initial access goldmines for a wide range of adversaries.

5. Post-Exploitation Tradecraft

Post-exploitation activity following VPN-based initial access represents the **most decisive phase of modern intrusions**. By the time threat actors reach this stage, they are no longer attempting to breach defenses; instead, they are exploiting trust, visibility gaps, and architectural weaknesses to consolidate control and prepare for long-term access or high-impact operations. Between 2023 and 2025, incident response investigations repeatedly demonstrated that once VPN access was achieved—whether via vulnerability exploitation or credential abuse—attackers were able to progress through post-exploitation phases with minimal resistance.

This section details the post-exploitation tradecraft observed after VPN compromise, with emphasis on how specific VPN vulnerabilities and access conditions shape attacker behavior.

5.1 From VPN Foothold to Trusted Insider

Unlike phishing-based intrusions, VPN-derived access places attackers immediately inside the network perimeter as **authenticated users**. In many environments, VPN users inherit broad network visibility and are subject to fewer behavioral controls than endpoints accessed locally. This trusted positioning fundamentally alters the post-exploitation dynamic.

When VPN access is obtained through exploitation of vulnerabilities such as Fortinet FortiOS SSL-VPN flaws (e.g., CVE-2024-21762) or Ivanti Connect Secure authentication bypass and RCE vulnerabilities (e.g., CVE-2025-0282), attackers may enter the environment without any associated user context. In these cases, defenders often lack clarity on *which* identity is compromised, complicating containment and investigation.

In credential-based scenarios, attackers frequently authenticate as legitimate users whose access profiles align with normal remote work patterns. This allows post-exploitation activity to blend seamlessly with expected VPN usage, particularly in organizations with distributed IT teams or extensive remote administration.

5.2 Rapid Internal Reconnaissance and Environment Mapping

The first operational priority after VPN access is **environmental reconnaissance**. Threat actors seek to determine the value of the compromised environment, the feasibility of escalation, and the presence of defensive controls.

Reconnaissance activities typically begin within minutes and include:

- Enumeration of Active Directory domains, forests, and trust relationships
- Identification of domain controllers and identity infrastructure
- Discovery of file servers, SharePoint farms, and collaboration platforms
- Identification of backup servers, hypervisors, and management networks

Because VPN compromise often grants access to internal DNS and directory services, attackers can perform extensive reconnaissance using LDAP queries and native command-line tools. No malware deployment is required, and activity is frequently logged—if at all—as routine directory access.

In cases involving exploitation of VPN appliances themselves, attackers may extract configuration files, cached credentials, or authentication logs directly from the device. Vulnerabilities such as arbitrary file read or command execution on appliances allow adversaries to harvest VPN user credentials en masse, accelerating subsequent lateral movement.

5.3 Credential Harvesting and Privilege Escalation

Credential access remains the linchpin of post-exploitation success. VPN access alone rarely grants sufficient privilege for full domain compromise, but it provides a launch point for aggressive credential harvesting.

Observed credential access techniques include:

- Memory dumping of authentication processes on reachable systems
- Abuse of administrative shares and remote registry access
- Extraction of credentials from scripts, configuration files, and scheduled tasks
- Identification and exploitation of service accounts with excessive privileges

In environments affected by VPN vulnerabilities such as CVE-2023-46805 and CVE-2024-21887 (Ivanti Connect Secure), attackers were observed chaining appliance-level access with internal credential harvesting, effectively bypassing user authentication entirely. This approach allowed operators to escalate privileges rapidly without triggering endpoint security alerts.

Privilege escalation often occurred organically as attackers moved laterally. In many cases, VPN users were permitted access to systems where local administrator passwords were reused or poorly managed. This enabled attackers to pivot from a single compromised account to domain-level privileges in a short timeframe.

5.4 Living-off-the-Land Lateral Movement at Scale

One of the defining characteristics of post-exploitation following VPN compromise is the **near-total reliance on living-off-the-land techniques**. Threat actors deliberately avoid introducing new binaries or malware during early post-exploitation phases, opting instead for native Windows functionality.

Common lateral movement methods include:

- Remote service creation and execution
- Scheduled task deployment across hosts
- SMB-based command execution
- Remote management via WinRM and PowerShell remoting

These techniques are particularly effective when initiated from VPN-originated sessions, as they mirror legitimate administrative workflows. In multiple investigations, lateral movement activity originating from VPN IP ranges was initially dismissed as routine IT operations.

The exploitation of VPN vulnerabilities exacerbates this issue. When attackers enter through appliance-level compromise, lateral movement activity may not be associated with any user VPN session at all, further obscuring attribution and delaying detection.

5.5 Persistence Mechanisms and Access Hardening

Post-exploitation persistence following VPN compromise is often **multi-layered and redundant**. Rather than relying on a single persistence mechanism, attackers establish multiple footholds to ensure continued access even if one vector is remediated.

Common persistence mechanisms include:

- Creation of scheduled tasks running under SYSTEM or service accounts

- Deployment of new Windows services with benign naming conventions
- Modification of Group Policy Objects to reintroduce access
- Addition of new directory users or elevation of existing accounts
- Manipulation of VPN appliance configurations to retain access

In several cases involving SonicWall and Fortinet appliances, attackers created hidden VPN users or modified authentication rules directly on the device. These changes often persisted through partial remediation efforts, allowing attackers to regain access even after endpoint cleanup.

Persistence is also frequently established through identity systems rather than hosts. Attackers may register OAuth applications, modify federation settings, or abuse directory synchronization mechanisms to maintain access without relying on VPN sessions alone.

5.6 Operational Security and Blending Techniques

Attackers demonstrate high levels of operational discipline during post-exploitation following VPN access. Because their success depends on remaining undetected for as long as possible, they adopt behaviors designed to minimize suspicion.

Observed operational security practices include:

- Restricting activity to normal business hours
- Throttling reconnaissance and lateral movement
- Avoiding high-risk actions until sufficient intelligence is gathered
- Using legitimate administrative tools exclusively during early phases

VPN-based access is particularly conducive to these practices. Activity originating from known VPN gateways or corporate IP ranges is less likely to be flagged, especially in organizations where remote administration is common.

5.7 Targeting of High-Impact Infrastructure

As post-exploitation progresses, attackers increasingly focus on **high-impact infrastructure components**. VPN access often provides direct or indirect reachability to these systems, reducing the need for broad lateral movement.

Priority targets include:

- Backup servers and repositories
- Virtualization management platforms (e.g., ESXi, vCenter)
- Identity and access management systems
- Centralized file servers and databases

In ransomware-driven campaigns, attackers frequently disable or tamper with backup systems well before deploying encryption. In several cases, backup deletion or corruption occurred days prior to ransomware execution, significantly reducing recovery options.

5.8 Divergence of Post-Exploitation Outcomes

Not all VPN-originated intrusions culminate in ransomware deployment. Increasingly, post-exploitation activity diverges into one of several outcomes:

- Data exfiltration and extortion without encryption
- Long-term persistent access for espionage or resale
- Staged ransomware deployment following extended reconnaissance

This divergence reflects a broader shift in attacker economics and risk tolerance. VPN compromise enables attackers to assess and monetize access in flexible ways, rather than committing immediately to high-visibility actions.

5.9 Defensive Blind Spots Exposed

The effectiveness of post-exploitation tradecraft following VPN compromise highlights several persistent defensive blind spots:

- Limited correlation between VPN access and internal activity
- Insufficient monitoring of administrative behavior
- Overreliance on endpoint detection for intrusion visibility
- Poor visibility into appliance-level compromise

Organizations affected by VPN exploitation vulnerabilities frequently lacked the telemetry required to reconstruct early post-exploitation phases, discovering intrusions only after significant damage had occurred.

5.10 Summary

Post-exploitation following VPN-based initial access has matured into a **disciplined, low-noise, and highly effective operational model**. By exploiting trusted access paths, leveraging native tooling, and abusing architectural assumptions, threat actors consistently achieve deep and durable control over compromised environments.

The inclusion of VPN-specific vulnerabilities—such as CVE-2024-21762, CVE-2025-0282, and related appliance flaws—further amplifies attacker advantage by enabling access that bypasses traditional identity and endpoint controls entirely. Once inside, attackers exploit the same trust relationships that organizations depend on for remote access and administration.

Understanding post-exploitation tradecraft in the context of VPN compromise is therefore critical. Defenders who focus solely on preventing initial access, without addressing the realities of post-exploitation behavior, will continue to face silent, high-impact intrusions that are detected only after irreparable harm has been done.

6. Divergent Post-Exploitation Paths: Ransomware vs. Non-Ransomware Operations

Following successful VPN-based initial access and post-exploitation groundwork, threat actor operations increasingly diverge into **two distinct execution paths**: ransomware-driven impact operations and non-ransomware intrusions focused on data theft, espionage, or access monetization. While these paths share common early-stage tradecraft, their objectives, timelines, and risk profiles differ significantly. Understanding this divergence is critical for defenders, as it directly influences detection priorities, response timing, and business impact.

This section examines how attackers transition from post-exploitation into either ransomware or non-ransomware outcomes, and why VPN-based access enables this operational flexibility.

6.1 Shared Foundations Before Divergence

In both ransomware and non-ransomware intrusions, the preparatory post-exploitation phases are often indistinguishable. Attackers leverage VPN-derived access to conduct reconnaissance, harvest credentials, and establish persistence while maintaining a low operational profile. At this stage, defenders frequently struggle to determine attacker intent, as no overtly destructive actions have occurred.

Key shared activities include:

- Validation of domain-level privileges
- Enumeration of sensitive data repositories
- Assessment of backup and recovery capabilities
- Identification of security tooling and monitoring gaps

VPN access allows attackers to **delay commitment to a specific outcome** until sufficient intelligence is gathered. This optionality is a major advantage over traditional phishing-based intrusions, where early malware deployment often reveals attacker intent.

6.2 Ransomware-Driven Post-Exploitation Path

In ransomware-focused intrusions, post-exploitation activity is ultimately oriented toward **maximizing operational impact and financial leverage**. Once attackers determine that an environment is sufficiently valuable and exploitable, they begin preparing for encryption and extortion.

6.2.1 Impact Preparation and Environmental Conditioning

Prior to ransomware deployment, attackers invest significant effort in shaping the environment to ensure successful execution. This conditioning phase often includes:

- Disabling or corrupting backup repositories
- Deleting volume shadow copies
- Identifying and neutralizing endpoint protection controls
- Mapping virtualization and storage infrastructure

VPN access plays a crucial role here, as it allows attackers to perform these actions using legitimate administrative channels. In many cases, backup systems are accessed and modified days before ransomware deployment, reducing the likelihood of rapid recovery.

6.2.2 Lateral Deployment Readiness

Attackers then prepare mechanisms for **domain-wide ransomware deployment**, often using:

- Group Policy Objects
- Remote service creation
- Centralized task scheduling
- Administrative shares

These mechanisms are tested incrementally to avoid detection. Small-scale executions or dry runs may occur to validate privileges and execution paths before full deployment.

6.2.3 Execution and Extortion

Once conditions are deemed optimal, ransomware is deployed rapidly across targeted systems. Encryption windows are intentionally short, minimizing defender response opportunities. Simultaneously, attackers may initiate extortion by threatening data publication or contacting executive leadership directly.

Groups such as **Akira** have demonstrated a willingness to abandon encryption entirely if data exfiltration alone provides sufficient leverage. This reinforces the notion that ransomware is a tactical option rather than a mandatory endpoint.

6.3 Non-Ransomware Post-Exploitation Path

In contrast, non-ransomware intrusions prioritize **stealth, persistence, and long-term value extraction**. These operations may be conducted by state-aligned actors, access brokers, or financially motivated groups seeking lower-risk monetization.

6.3.1 Data-Centric Objectives

Non-ransomware actors often focus on:

- Exfiltration of intellectual property
- Theft of sensitive personal or financial data
- Access to strategic communications or research
- Collection of credentials for resale or reuse

VPN-based access is particularly advantageous for these objectives, as it allows attackers to access internal data stores directly without deploying malware that might raise suspicion.

6.3.2 Persistence Over Impact

Rather than disabling systems or drawing attention, non-ransomware actors emphasize **durable access**. Persistence mechanisms are designed to survive password resets, endpoint remediation, and even infrastructure changes.

These may include:

- Backdoor accounts in directory services
- Appliance-level persistence on VPN or edge devices
- Abuse of identity federation or cloud trust relationships

In some cases, attackers deliberately limit activity to reduce forensic artifacts, accepting slower data collection in exchange for longevity.

6.3.3 Monetization Without Disruption

For access brokers and extortion-focused actors, monetization may occur without any direct impact on the victim environment. Access can be sold multiple times, or data quietly exfiltrated and offered for sale on underground markets. This approach significantly reduces legal and operational risk compared to ransomware deployment.

6.4 Decision Factors Influencing Path Selection

The choice between ransomware and non-ransomware outcomes is rarely arbitrary. Threat actors evaluate several factors before committing:

- Size and financial capacity of the organization
- Quality and availability of backups
- Detection maturity and SOC responsiveness
- Regulatory exposure and reputational sensitivity
- Stability and privilege level of VPN access

VPN compromise enables attackers to perform this evaluation from a position of safety. If conditions are unfavorable, attackers may disengage temporarily or repurpose access for alternative objectives.

6.5 Defensive Implications of Divergent Paths

From a defender perspective, the divergence between ransomware and non-ransomware post-exploitation paths presents a significant challenge. Early indicators are often subtle and identical across both scenarios. Organizations that rely solely on ransomware-specific detections—such as mass file encryption or ransom note creation—will fail to detect non-ransomware intrusions entirely.

Key defensive implications include:

- The absence of ransomware does not indicate a benign outcome
- VPN compromise must be treated as a potential enterprise-wide breach
- Detection strategies must focus on behavior, not payloads
- Long-term access may be more damaging than immediate disruption

6.6 Strategic Risk of Misclassification

A recurring failure observed in incident response is the **misclassification of VPN-originated intrusions** as failed or incomplete ransomware attempts. In reality, many such incidents represent successful non-ransomware operations where attackers achieved their objectives without triggering encryption.

This misclassification leads to:

- Incomplete remediation
- Persistence mechanisms left intact
- Underestimation of data exposure
- Increased likelihood of reintrusion

Understanding that ransomware is only one possible outcome of VPN compromise is therefore essential to effective response and recovery.

6.7 Summary

VPN-based post-exploitation enables threat actors to **choose their outcome** rather than commit prematurely to a single attack path. Whether pursuing ransomware deployment or non-ransomware objectives such as data theft and long-term access, attackers exploit the same foundational weaknesses: trusted remote access, limited visibility, and delayed detection.

For defenders, this reality demands a shift in mindset. The absence of ransomware does not equate to safety, and the presence of VPN compromise should always be treated as a high-severity incident requiring comprehensive investigation. Only by addressing both ransomware and non-ransomware post-exploitation paths can organizations hope to mitigate the full spectrum of risk posed by VPN-centric intrusions.

7. 7. Regulatory Impact: NIS2, GDPR, and DORA Implications of VPN-Centric Intrusions

VPN-based intrusions introduce a **high-risk regulatory exposure profile** precisely because they exploit trusted access paths and often evade early detection. From a regulatory standpoint, the absence of visible malware or ransomware does not mitigate impact; rather, the silent nature of these intrusions increases the likelihood of **late discovery, incomplete scoping, and underreporting**, all of which amplify legal and compliance risk.

Across NIS2, GDPR, and DORA, VPN compromise directly challenges foundational assumptions around access control, monitoring, and incident response timeliness.

7.1 NIS2: Failure of Preventive and Detective Controls

Under NIS2, organizations classified as essential or important entities are required to implement **appropriate and proportionate technical, operational, and organizational measures** to manage cybersecurity risks. VPN compromise directly undermines several of these obligations.

Key NIS2 implications include:

- **Risk Management Failure**
  VPN appliances are perimeter systems that directly affect service continuity. Inadequate patching, exposed management interfaces, or weak authentication controls may be interpreted as failures to manage known risks.
- **Detection and Response Deficiencies**
  Many VPN-based intrusions remain undetected for extended periods due to insufficient logging, short retention, or lack of correlation with internal activity. This conflicts with NIS2 expectations around timely detection and response.
- **Incident Notification Obligations**
  If VPN compromise results in unauthorized access to internal systems or sensitive data, even without ransomware, it may constitute a reportable incident. Organizations that delay reporting due to uncertainty about impact risk regulatory penalties.

Crucially, NIS2 shifts regulatory focus from **incident outcome** to **control effectiveness**. An organization does not need to experience encryption or service outage to be found non-compliant; demonstrable failure to secure and monitor VPN access may be sufficient.

7.2 GDPR: Unauthorized Access and Silent Data Exposure

From a GDPR perspective, VPN-based intrusions present a particularly dangerous scenario because **data exposure may occur without obvious indicators**. Attackers operating through authenticated VPN sessions can access personal data repositories, file shares, and collaboration platforms in ways that resemble legitimate user behavior.

Key GDPR risks include:

- **Personal Data Breach Without Encryption**
  Data exfiltration, inspection, or copying via VPN access constitutes unauthorized access, even if no data is publicly leaked. Encryption is not a prerequisite for a personal data breach.

- **Delayed or Missed Breach Detection**
  VPN-centric intrusions frequently result in delayed discovery, complicating the 72-hour breach notification requirement. Regulators increasingly scrutinize *why* detection was delayed.
- **Accountability and Evidence Gaps**
  Inadequate VPN logging or retention impairs an organization's ability to determine which data was accessed. This lack of evidence may be interpreted as insufficient technical and organizational measures.

Importantly, regulators assess GDPR compliance based on **reasonable detection capability**, not certainty of harm. Organizations that cannot conclusively rule out data access due to logging gaps may still face enforcement action.

7.3 DORA: ICT Risk and Third-Party Exposure

For financial entities subject to DORA, VPN compromise intersects directly with **ICT risk management, access governance, and third-party dependency controls**.

Relevant DORA considerations include:

- **Critical ICT Asset Protection**
  VPN infrastructure enabling access to core banking, trading, or payment systems is inherently critical. Weak VPN security may constitute failure to safeguard ICT assets.
- **Access Control and Privilege Management**
  VPN access that enables lateral movement into sensitive environments raises questions about least privilege enforcement and segmentation.
- **Third-Party Risk Amplification**
  Many VPN intrusions occur via MSP or vendor access. DORA explicitly requires oversight of third-party ICT risk, and shared or poorly monitored VPN access channels are likely to be viewed as non-compliant.

DORA places particular emphasis on **resilience rather than reaction**. Silent VPN compromise that persists undetected undermines an organization's ability to demonstrate operational resilience, even in the absence of service disruption.

7.4 Regulatory Convergence: Why VPN Compromise Is a High-Risk Event

Across all three frameworks, a consistent regulatory theme emerges:

Trusted access paths must be treated as high-risk assets.

VPN compromise challenges assumptions about perimeter security, detection capability, and response readiness. Regulators increasingly view silent intrusions not as edge cases, but as indicators of systemic control failure.

8. SOC Detection Strategy for VPN-Centric Intrusions

Traditional SOC detection models are poorly suited to VPN-originated attacks. These intrusions frequently involve **no malware, no exploit artifacts on endpoints, and no anomalous outbound traffic** during early stages. Effective detection therefore requires a **shift from payload-centric alerts to access- and behavior-centric analysis**.

This section outlines a practical SOC detection strategy tailored to VPN-based post-exploitation.

8.1 Treat VPN Access as a Security Event, Not Connectivity

The first and most critical shift is conceptual:
VPN authentication is not benign by default.

SOC teams should treat every VPN session as a potential intrusion vector and apply contextual scrutiny comparable to that used for privileged logins.

Minimum telemetry requirements include:

- Source IP and geolocation
- Authentication method (password, MFA, certificate)
- Session duration
- User-agent or client type
- Accessed network segments

Without this baseline, meaningful detection is impossible.

8.2 Correlate VPN Sessions with Downstream Activity

VPN compromise becomes detectable primarily through **what happens after authentication**, not the authentication itself.

High-risk correlations include:

- VPN login followed by rapid internal reconnaissance
- VPN session immediately preceding multiple authentication attempts across hosts
- First-time VPN access followed by privileged actions
- VPN sessions coinciding with creation of scheduled tasks or services

SOC detection logic must bridge VPN logs, identity telemetry, and endpoint or server activity. Siloed analysis is insufficient.

8.3 Detect Behavioral Deviations, Not Known Badness

Because attackers frequently use legitimate tools, signature-based detection has limited value. Instead, SOC teams should focus on **behavioral deviations** such as:

- New VPN users accessing administrative systems
- VPN users performing directory-wide enumeration
- Unusual timing patterns (e.g., administrative activity outside normal user behavior)
- VPN access from rare geographies followed by sensitive system access

The objective is not to detect “malicious commands,” but **malicious context**.

8.4 Prioritize Early-Stage Indicators Over Impact Signals

SOC teams often focus heavily on ransomware indicators such as encryption behavior or ransom notes. In VPN-centric intrusions, this focus is misplaced.

Higher-value early indicators include:

- Abnormal VPN session reuse
- Authentication bursts originating from VPN IP ranges
- Administrative actions from accounts with no prior history
- Lateral movement within minutes of VPN access

By the time ransomware indicators appear, defensive options are already severely constrained.

8.5 Response Strategy: Assume Full Compromise Until Proven Otherwise

When suspicious VPN activity is identified, SOC response should assume **environment-wide risk**, not isolated user compromise.

Key response principles:

- Invalidate VPN sessions and credentials immediately
- Assess appliance-level compromise, not just user accounts
- Correlate VPN access with historical internal activity
- Expand investigation scope beyond ransomware indicators

Failure to adopt this posture is a common cause of reintrusion and regulatory escalation.

8.6 Summary

VPN-based intrusions exploit a structural blind spot between connectivity and security. Regulators increasingly view this blind spot as unacceptable, and attackers exploit it with growing efficiency.

For SOC teams, effective detection requires abandoning assumptions that:

- Authentication equals legitimacy
- Malware equals compromise
- Encryption equals impact

VPN compromise must be treated as a **high-severity security event**, regardless of immediate outcome. Organizations that align detection, response, and regulatory expectations around this reality will be significantly better positioned to mitigate both operational and compliance risk.

9. Risk Assessment and Defensive Recommendations

VPN-centric intrusions represent one of the most consequential shifts in the modern threat landscape. Unlike traditional attack vectors that rely on user interaction, malware execution, or overt exploitation of endpoints, VPN-based compromises exploit **trusted access paths** that are foundational to modern enterprise operations. This chapter assesses the risk posed by such intrusions and outlines defensive recommendations designed to reduce likelihood, limit impact, and improve detection and response capability.

This assessment intentionally treats VPN compromise not as an isolated technical issue, but as a **systemic organizational risk** with operational, regulatory, and strategic consequences.

9.1 Likelihood of VPN-Centric Compromise

The likelihood of VPN-based compromise should be assessed as **high** for the majority of medium and large organizations. Several structural factors contribute to this elevated likelihood:

- VPN and remote access systems are internet-facing by design
- Patch cycles for appliances frequently lag behind vulnerability disclosure
- VPN telemetry is often incomplete or insufficiently analyzed
- Authentication success is commonly equated with legitimacy
- Third-party and contractor access expands exposure beyond internal users

Unlike phishing or malware campaigns, VPN compromise does not depend on user behavior, awareness, or error. Attackers can operate continuously, automate scanning and exploitation, and opportunistically harvest access at scale. The repeated exploitation of known VPN vulnerabilities demonstrates that adversaries view these systems as **low-effort, high-reward targets**.

Additionally, the presence of a mature initial access broker ecosystem further increases likelihood. Organizations may be compromised **without being explicitly targeted**, simply because VPN access is harvested opportunistically and later resold. In such cases, the initial compromise may go unnoticed for extended periods, only becoming apparent when access is weaponized.

From a probabilistic standpoint, any organization operating exposed VPN infrastructure should assume that compromise is **a question of when, not if**.

9.1.1 Impact Severity

The potential impact of VPN compromise is **severe to critical**, even in the absence of ransomware deployment. VPN-based intrusions grant attackers a privileged foothold that bypasses multiple layers of traditional security controls.

Impact dimensions include:

Confidentiality
VPN access frequently enables direct access to file shares, collaboration platforms, internal applications, and identity systems. Because access is authenticated, data exposure may occur without triggering alarms or leaving obvious forensic artifacts. Sensitive personal data, intellectual property, and strategic information are all at risk.

Integrity
Attackers operating through VPN access can modify configurations, credentials, backups, and security controls

long before detection. This undermines trust in system integrity and complicates recovery, as organizations may be unable to determine what has been altered.

Availability
In ransomware scenarios, VPN compromise often precedes deliberate sabotage of backups and virtualization infrastructure. When encryption is deployed, recovery options are severely constrained, leading to prolonged outages and operational disruption.

Regulatory and Legal Impact
Silent intrusions increase the risk of delayed or incomplete regulatory reporting. Organizations may struggle to determine whether personal or regulated data was accessed, increasing exposure under NIS2, GDPR, and DORA.

Crucially, impact should not be measured solely by whether ransomware is deployed. **Non-ransomware outcomes—such as data theft, access resale, or long-term persistence—can be equally or more damaging** over time.

9.1.2 Detection and Response Risk

A defining risk characteristic of VPN-centric intrusions is **low detectability during early stages**. Because attackers often use legitimate credentials and native administrative tools, traditional detection mechanisms frequently fail to identify malicious activity.

Key detection challenges include:

- VPN logs retained for short periods or not centralized
- Lack of correlation between VPN access and internal activity
- Overreliance on endpoint malware indicators
- Limited visibility into appliance-level compromise
- Assumption that MFA prevents meaningful abuse

As a result, many VPN-originated intrusions exhibit extended dwell times. By the time suspicious activity is detected, attackers may have already achieved their objectives, staged data for exfiltration, or established multiple persistence mechanisms.

Delayed detection directly increases:

- Scope uncertainty
- Remediation cost
- Business disruption
- Regulatory exposure

From a risk management perspective, **poor detectability is a force multiplier** that amplifies both likelihood and impact.

9.1.3 Business and Operational Risk

VPN compromise undermines fundamental assumptions about remote work, outsourcing, and digital trust. During incident response, organizations often face difficult operational trade-offs, including:

- Disabling VPN access entirely to contain the threat

- Revoking access for third parties and contractors
- Forcing large-scale credential resets
- Interrupting business-critical remote operations

These actions can have cascading effects on service delivery, customer relationships, and supply chains. For organizations in regulated or critical sectors, such disruptions may themselves constitute reportable incidents.

9.1.4 Overall Risk Classification

Based on observed threat activity and organizational exposure, VPN-centric intrusion risk can be classified as follows:

- **Likelihood:** High
- **Impact:** Severe to Critical
- **Detectability:** Low (without targeted controls)
- **Regulatory Exposure:** High
- **Business Disruption Potential:** High

VPN compromise should therefore be treated as a **Tier-0 enterprise risk**, comparable to identity platform compromise or domain controller exposure. Treating it as a routine IT or patching issue materially increases the probability of catastrophic outcomes.

9.2 Defensive Recommendations

Mitigating VPN-centric intrusion risk requires a **defense-in-depth strategy** that assumes prevention will eventually fail. The objective is not perfect security, but **resilience**: reducing exposure, increasing visibility, and limiting blast radius when compromise occurs.

9.2.1 Strategic Control Principles

At a strategic level, organizations should adopt the following principles:

1. **Assume VPN compromise will occur**
   Defensive strategies must be resilient to failure rather than dependent on flawless prevention.
2. **Treat VPN infrastructure as Tier-0**
   VPN appliances and remote access systems should receive the same security attention as identity platforms and core authentication services.
3. **Separate connectivity from trust**
   Authentication alone should not grant broad internal access.
4. **Design for containment**
   The goal is to limit what an attacker can do *after* VPN access is obtained.

9.2.2 Preventive Controls: Reducing Attack Surface

Preventive measures remain essential for reducing opportunistic compromise:

- Enforce aggressive patch management for VPN and edge devices, with prioritization based on exploitation status rather than CVSS alone
- Restrict management interfaces to dedicated administrative networks or allowlisted IP ranges

- Disable unused VPN portals, legacy protocols, and deprecated authentication methods
- Enforce strong MFA consistently across all VPN access paths, including third-party and legacy portals
- Implement strict certificate lifecycle management where certificate-based authentication is used

While prevention alone is insufficient, these controls significantly reduce attack volume and noise.

9.2.3 Architectural Controls: Limiting Blast Radius

Architectural decisions have a profound impact on post-compromise outcomes.

Key measures include:

- Segment VPN users into dedicated network zones with minimal default access
- Prohibit direct VPN access to domain controllers, backup systems, and management networks
- Require jump hosts or privileged access workstations for administrative activity
- Enforce least privilege for VPN users, including IT staff and contractors
- Separate third-party VPN access from internal user access paths

These measures ensure that VPN compromise does not equate to unrestricted internal access.

9.2.4 Detection Controls: Making VPN Abuse Visible

Detection is the most critical gap in current defenses.

Organizations should implement:

- Centralized VPN logging with retention aligned to regulatory and forensic requirements
- Correlation of VPN authentication events with identity, endpoint, and network telemetry
- Behavioral analytics focused on post-authentication activity rather than login success
- Alerts for first-time VPN access, anomalous geolocation, and unusual session duration
- Detection of rapid internal activity bursts following VPN authentication

SOC teams should treat VPN access as a **security signal**, not a background event.

9.2.5 Incident Response and Containment

When suspicious VPN activity is detected, response must be decisive and comprehensive.

Recommended actions include:

- Immediate invalidation of VPN sessions and credentials
- Assessment of appliance-level compromise, not just user accounts
- Expansion of investigation scope to include all systems reachable via VPN
- Review of historical VPN access for evidence of prior abuse
- Parallel regulatory impact assessment, not deferred until confirmation

Crucially, organizations should **assume full compromise until proven otherwise**, rather than attempting to scope narrowly.

9.2.6 Governance and Oversight

Finally, governance structures must reflect the risk posed by VPN compromise.

This includes:

- Explicit ownership of VPN risk at the executive level
- Inclusion of VPN infrastructure in enterprise risk assessments
- Regular tabletop exercises focused on VPN compromise scenarios
- Alignment of SOC metrics with access abuse detection, not just malware events
- Clear escalation paths for potential regulatory reporting

VPN security is not merely an IT concern; it is a **business and compliance issue**.

9.3 Conclusion

VPN-centric intrusions exploit a fundamental mismatch between how organizations deploy remote access and how they defend it. As attackers continue to target trusted access paths, organizations that fail to elevate VPN infrastructure to a first-class security concern will remain vulnerable to silent, high-impact compromise.

Effective risk reduction does not require abandoning VPN technology, but it does require **rethinking trust, visibility, and containment**. Organizations that adopt this mindset—treating VPN compromise as inevitable and designing defenses accordingly—will be far better positioned to withstand both operational disruption and regulatory scrutiny.

About Ransomwared

Ransomwared is a European-based cybersecurity initiative committed to protecting organizations against the evolving threat of ransomware. Our mission is to **disrupt the economics of cyber extortion** by providing intelligence, technology, and rapid response capabilities that empower defenders to outpace attackers.

At the core of our work is a **next-generation, AI-enhanced, autonomous SOC (Security Operations Center)** that operates 24/7. This SOC continuously ingests global threat intelligence, analyzes attacker behaviors, and autonomously correlates patterns against enterprise telemetry. By leveraging **machine learning models trained on ransomware TTPs**—including those used by groups such as **Akira**—we provide real-time detection, predictive defense, and automated containment actions.

How We Stay Ahead of Threats

AI-Driven Threat Intelligence: Our models are continuously refined with data from ransomware campaigns, CVE exploit chains, and underground ecosystems, enabling proactive detection of new attack variants.

- **24/7 Autonomous SOC**: Operating around the clock, our SOC doesn't just monitor—it autonomously correlates anomalies, isolates compromised endpoints, and enforces adaptive security controls in real time.
- **Behavioral Defense**: By mapping techniques to **MITRE ATT&CK**, we detect ransomware campaigns even when adversaries change infrastructure, binaries, or ransom note formats.
- **Continuous Learning**: Every incident enriches our AI and SOC capabilities, strengthening defenses not only for individual organizations but across the entire Ransomwared community.

Our Broader Mission

- **Threat Intelligence Reports**: In-depth CTI reporting (like this Akira analysis) that provides technical, operational, and strategic insights.
- **Vulnerability-to-Exploit Correlation**: Automated pipelines that link CVEs with ransomware campaigns within hours of disclosure.
- **Resilience by Design**: Guidance for implementing Zero Trust, immutable backups, and robust incident response frameworks.

Our Vision

We believe the fight against ransomware will not be won by reacting to incidents, but by **out-automating adversaries**. By combining advanced AI, a 24/7 autonomous SOC, and a culture of open intelligence sharing, Ransomwared helps organizations move from reactive defense to **proactive resilience**—ensuring that ransomware groups lose their strategic advantage.For more information, resources, and access to our threat intelligence services, visit:

🌐 **www.ransomwared.eu**