ALLIANCE PRO



WHEN HOSTING DOES NOT EQUAL SECURITY

A LOCKBIT V5.0 RANSOMWARE INCIDENT IN A HOSTED ENVIRONMENT

AN EYE-OPENING CASE STUDY

ALLIANCE PRO©

DISCLAIMER

This case study has been prepared by **Alliance Pro** for informational and illustrative purposes only. All client-specific identifiers, sensitive details, and proprietary information have been intentionally anonymized or generalized to protect confidentiality and security interests.

The methodologies, processes, and technical approaches described herein constitute the intellectual property of Alliance Pro and may not be reproduced, distributed, or used without prior written consent. This document does not disclose complete operational procedures or security configurations and should not be interpreted as a comprehensive incident response playbook.

Any resemblance to specific organizations, systems, or environments is purely coincidental.

OVERVIEW

A mid-sized digital services organization operating a large **multi-tenant environment** suffered a **severe LockBit v5.0 ransomware attack**, resulting in the encryption of significant volumes of **business-critical and customer data**.
The organization hosted its infrastructure within a **third-party data center**, relying on the provider's **managed firewall and hosting services** under the assumption that these controls were sufficient to ensure security.
This incident exposed a critical misconception seen across many enterprises: **while data centers provide physical infrastructure and basic network services, they do not inherently provide cybersecurity posture, threat detection, or resilience against modern ransomware.**
Alliance Pro was engaged to perform a **deep forensic investigation**, determine the **true root cause**, assess the **overall security posture**, and provide findings that could withstand **customer, executive, and contractual scrutiny**.

THE CHALLENGE

The ransomware incident created a multi-dimensional crisis for the organization. Large portions of the virtualized environment and management infrastructure became inaccessible, directly impacting customer-facing services. At the same time, customers demanded transparency—specifically a **credible Root Cause Analysis (RCA)** explaining how the breach occurred and whether their data was affected.

Several factors compounded the challenge:

- Limited historical visibility due to **inadequate log retention and monitoring**
- Unclear **security responsibility boundaries** between the organization and the data center
- Assumption that the data center's **managed firewall was secure by default**
- Technical complexity introduced by **LockBit v5.0's anti-forensics capabilities**
- Presence of **cracked VMware components**, increasing exposure and limiting traceability

The organization required an investigation based on **evidence, not assumptions**—and findings that could be confidently shared with stakeholders.

ALLIANCE PRO'S ENGAGEMENT APPROACH

Alliance Pro initiated a structured **Incident Response and Forensic Engagement**, aligned with globally recognized frameworks such as **NIST Incident Response**, **MITRE ATT&CK**, and **CIS Controls**.

The engagement focused on three parallel objectives:

- **Reconstruct the incident timeline** using factual forensic evidence
- **Identify systemic security weaknesses** beyond the ransomware payload
- **Clearly distinguish hosting responsibilities from cybersecurity accountability**

This approach ensured technical accuracy while also addressing executive and customer expectations.

FORENSIC INVESTIGATION & ROOT CAUSE ANALYSIS

Alliance Pro conducted a comprehensive forensic analysis across the hosted infrastructure and associated systems. The investigation focused on reconstructing attacker behaviour across the full kill chain, despite the anti-forensic design of LockBit v5.0.

Key forensic activities included:

- Examination of **compromised virtualization management components**
- Reconstruction of:
  - Initial access
  - Lateral movement
  - Privilege escalation
- Correlation of available **system, network, and authentication logs**
- Mapping attacker actions to **known ransomware tactics and techniques**
- Assessment for **indicators of data exfiltration**

The analysis confirmed that the incident was **not caused by a single control failure**, but by a **sequence of long-standing security gaps** that existed well before ransomware execution.

KEY FINDINGS

The investigation revealed several critical weaknesses that collectively enabled the attack:

- **Outdated firewall technology** provided by the data center, operating on legacy firmware
- **Overly permissive firewall rules**, exposing internal management interfaces
- Absence of advanced security capabilities, including:
  - Intrusion prevention
  - Malware inspection
  - Behavioural threat detection

- **No continuous monitoring or alerting** for suspicious activity
- Weak **identity and access controls** for privileged systems
- Poorly defined and undocumented **shared responsibility model**

Most importantly, the investigation confirmed that **hosting services did not include proactive security management or threat detection**, despite common enterprise assumptions.

VULNERABILITY ASSESSMENT & SECURITY POSTURE REVIEW

To assess broader risk exposure, Alliance Pro conducted a structured **vulnerability assessment and security posture review** across the environment.
This assessment uncovered:

- Misconfigured **management interfaces**
- **Unpatched systems** and outdated services
- Weak **segmentation between administrative and production networks**
- Inadequate **logging, monitoring, and audit mechanisms**

These findings reinforced a critical conclusion: the ransomware attack was **symptomatic of deeper security governance and design gaps**, not an isolated incident.

CORRECTIVE & PREVENTIVE MEASURES

Following the investigation, Alliance Pro worked closely with the organization to reduce risk and improve resilience through targeted corrective actions:

- Redesign and hardening of **firewall policies** using least-privilege principles
- Secure reconfiguration of **virtualization management platforms**
- Strengthening of **privileged identity and access controls**
- Introduction of **network segmentation** to limit lateral movement
- Establishment of baseline **monitoring and alerting**
- Formal documentation of **hosting vs. security responsibility boundaries**

These measures focused on **long-term risk reduction**, not just immediate recovery.

OUTCOME & BUSINESS IMPACT

The engagement delivered measurable and defensible outcomes:

- A **clear, evidence-backed Root Cause Analysis** for customers and leadership
- Remediation of **high-risk vulnerabilities** identified during the assessment
- A significantly strengthened security posture aligned with **industry best practices**
- Improved understanding of the distinction between **infrastructure hosting and cybersecurity ownership**
- Reduced likelihood of recurrence of similar ransomware incidents

KEY TAKEAWAY

This case reinforces a critical lesson for modern enterprises:

- Data centers provide **infrastructure availability**, not cybersecurity assurance
- Security must be **actively designed, validated, and continuously managed**
- Without clear ownership and monitoring, even well-hosted environments remain vulnerable

-END OF DOCUMENT-