

# Security Breach Investigation Report – NovaTech Systems

## 1 Overview

On August 17, 2025, NovaTech Systems experienced a cyberattack causing temporary outages in key servers. This report provides key facts, root causes, impacts, and preventive measures.

## 2 Incident Summary

- 02:13 UTC: Abnormal database queries detected.
- 02:30 UTC: Authentication server slowed and stopped.
- 03:05 UTC: Emergency team isolated network segments.
- 04:20 UTC: Malicious processes removed.
- 09:00 UTC: Services restored.

## 3 Root Cause

Attackers exploited a compromised third-party VPN account and escalated privileges, using AI automation for lateral movement and database key theft.

## 4 Impact

Approx. 1,800 accounts possibly exposed, 6 hour downtime, ~USD 2.5 million loss, reputational damage.

## 5 Measures

Stronger partner VPN audits, enforce MFA and least privilege, deploy AI anomaly detection, regular penetration tests, and stronger encryption.

## 6. Key Data Table

Item	Detail	Time	Note
Initial Intrusion	Third-party VPN account	02:13 UTC	Account compromise
Spread Method	Privilege escalation, lateral move	02:30-03:30 UTC	AI automation
Affected Systems	Auth server, database	02:30-04:20 UTC	Temporary outage
Final Action	Network isolation, process removal	04:20 UTC	Recovery complete

# - NovaTech Systems

1.

2025 8 17 NovaTech Systems

2.

- 02:13 UTC
- 02:30 UTC
- 03:05 UTC
- 04:20 UTC
- 09:00 UTC

3.

VPN AI

4.

1,800 6 250

5.

VPN AI

6. 核心数据表

项目	细节	时间	备注
初始入侵	第三方 VPN 账号	02:13 UTC	账号被盗用
扩散方式	权限提升，横向移动	02:30–03:30 UTC	AI 自动化
受影响系统	认证服务器，数据库	02:30–04:20 UTC	短时中断
最终处理	隔离网络，清除进程	04:20 UTC	恢复完成

W

→ NovaTechSystems

1

17 2025 NovaTechSystems ,  
 , ,

2

- 0213UTC
- 0230UTC
- 0305UTC
- 0420UTC
- 0900UTC

3

VPN AI

4

1,800 , 6 , 25 ,

5

VPN , MFA , AI ,

6

	VPN	0213UK	
	,	0230-0330UK	AI
	,	0230-0420UK	
	,	0420UK	

# **Informe de investigación de intrusión de seguridad – NovaTech Systems**

## **1 Resumen**

**El 17 de agosto de 2025 NovaTech Systems sufrió un ataque que provocó cortes temporales en servicios clave. Este informe resume hechos, causas, impacto y medidas preventivas.**

## **2 Resumen de Incidente**

- 02:15 UE Consultas de base de datos anómalas detectadas
- 02:30 UE Servidor de autenticación lateralizado
- 03:05 UE Aislamiento de segmentos de red
- 04:20 UE Procesos maliciosos eliminados
- 08:00 UE Servicios restaurados

## **3 Causa**

**El atacante utilizó una cuenta VPN de un tercero, elevó privilegios y usó automatización con IA para moverse lateralmente y acceder a bases de datos.**

## **4 Impacto**

**~180 cuentas expuestas, 6 horas de inactividad, ~25 millones USD de pérdidas, daño reputacional.**

## **5 Medidas**

**Auditorías más estrictas de VPN, aplicar MFA y privilegio mínimo, detección de anomalías con IA, pruebas de penetración y cifrado reforzado.**

## **6 Datos clave**

<b>Elemento</b>	<b>Detalle</b>	<b>Hora</b>	<b>Nota</b>
<b>Intrusión inicial</b>	<b>Cuenta VPN de tercero</b>	<b>02:13 UTC</b>	<b>Cuenta comprometida</b>
<b>Método de propagación</b>	<b>Escalada de privilegios, movimiento lateral</b>	<b>02:30-03:30 UTC</b>	<b>Automatización IA</b>
<b>Sistemas afectados</b>	<b>Servidor de autenticación, base de datos</b>	<b>02:30-04:20 UTC</b>	<b>Interrupción temporal</b>
<b>Acción final</b>	<b>Aislamiento de red, eliminación de procesos</b>	<b>04:20 UTC</b>	<b>Recuperación completa</b>

# Rapport d'enquête sur une intrusion de sécurité – NovaTech Systems

## 1 Vue d'ensemble

Le 17 août 2025, NovaTech Systems a subi une cyberattaque provoquant une interruption temporaire de serveurs clés. Ce rapport présente faits, causes, impacts et mesures préventives.

## 2 Résumé de l'incident

- 02:13 UTC: Requêtes de base de données anormales détectées
- 02:30 UTC: Serveur d'authentification ralenti et arrêté
- 03:05 UTC: Segments de réseau isolés
- 04:20 UTC: Processus malveillants supprimés
- 09:00 UTC: Services rétablis

## 3 Cause

Un compte VPN tiers compromis a été utilisé, avec élévation de privilèges et automatisation IA pour mouvement latéral et vol de clés de base de données.

## 4 Impact

Environ 1800 comptes exposés, 6h d'arrêt, perte estimée à 2,5M USD, atteinte à la réputation.

## 5 Mesures

Renforcer les audits VPN tiers, appliquer MFA et privilège minimal, détection d'anomalies IA, tests de pénétration réguliers, chiffrement renforcé.

## 6 Données clés

Élément	Détail	Heure	Remarque
Intrusion initiale	Compte VPN tiers	02:13 UTC	Compte compromis
Méthode de propagation	Élévation de privilèges, mouvement latéral	02:30-03:30 UTC	Automatisation IA
Systèmes affectés	Serveur d'authentification, base de données	02:30-04:20 UTC	Interruption temporaire
Action finale	Isollement du réseau, suppression des processus	04:20 UTC	Rétablissement

**-NovaTechSystems**

**1**  
**2025 17 NovaTechSystems**

- 2**  
**- 02:13 UTC**  
**- 02:30 UTC**  
**- 03:05 UTC**  
**- 04:20 UTC**  
**- 09:00 UTC**

**3**  
**VPN**

**4**  
**25 6 1,800**

**5**  
**VPN**

**6**

	<b>VPN</b>	<b>02:13 UTC</b>	
		<b>02:30-03:30 UTC</b>	
		<b>02:30-04:20 UTC</b>	
		<b>04:20 UTC</b>	