

# Biotech Startup Research Data Leak Investigation Report

## 1 Overview

On September 12, 2025, BioNet found a leak of confidential genetic research data. The investigation revealed combined insider misconduct and external hacking.

## 2 Incident Summary

- 0730UTC: Abnormal database queries detected
- 0810UTC: Employee login from foreign IP
- 0900UTC: Files copied to unauthorized cloud
- 1120UTC: Breach confirmed, network isolated

## 3 Root Cause

A staff member shared credentials with a hacker group, allowing internal exfiltration and external intrusion.

## 4 Impact

Exposure of key breeding data, ~USD 5 million loss, potential regulatory penalties, reputation damage.

## 5 Measures

Revoke and reset credentials, enforce MFA, deploy continuous anomaly detection, perform insider risk audits, and strengthen security training.

## 6 Key Investigation Data

Item	Detail	Time	Note
Initial Detection	Abnormal database query	0730UTC	Alert triggered
Compromised Log	Foreign IP access	0810UTC	Credential misuse
Data Exfiltration	Unauthorized cloud upload	0900UTC	Core files copied
Containment	Network isolation	1120UTC	Leak stopped

1. 概述

2025 年 9 月 12 日，BioNext 发现机密基因研究数据泄露。调查显示内部员工失职与外部黑客入侵共同导致。

2. 事件摘要

- 07:30 UTC：检测到异常数据库查询。
- 08:10 UTC：员工从海外 IP 异常登录。
- 09:00 UTC：文件被复制到未授权云端。
- 11:20 UTC：确认泄露并隔离网络。

3. 原因

一名员工向黑客团体泄露访问凭证，导致内部外泄与外部入侵并行。

4. 影响

核心基因编辑数据暴露，损失约 500 万美元，或面临监管处罚与声誉受损。

5. 措施

撤销并重置凭证，实施多因素认证，持续异常检测，执行内部风险审计，加强员工安全培训。

6

		07:30UTC	
	IP	08:10UTC	
		09:00UTC	
		11:20UTC	

1

12 2025 BioNext

□

2

- 07:30UTC:

- 08:10UTC: □ IP

- 09:00UTC:

- 11:20UTC: , □

3

□

,

4 Ñ

□

,

5

W ,

□ , Ñ

5

-

,

Ñ

,

,

,

W Ñ W

6

		07:30UTC	
	IP	08:10UTC	
		09:00UTC	
		11:20UTC	

# **Informe de investigación de fuga de datos de investigación – BioNext**

## **1 Resumen**

**El 12 de septiembre de 2025 BioNext detectó fuga de datos genéticos confidenciales. La investigación reveló complicidad interna y ataque externo**

## **2 Resumen del incidente**

- **07:30 UTC:** Consultas anómalas en base de datos detectadas
- **08:10 UTC:** Inicio de sesión desde IP extranjera inusual
- **09:00 UTC:** Copia de archivos en nube no autorizada
- **11:20 UTC:** Fuga confirmada, red aislada

## **3 Causa**

**Un empleado compartió credenciales con un grupo de hackers, permitiendo extracción de datos y acceso externo**

## **4 Impacto**

**Exposición de datos de edición genética, pérdidas de ~5 millones USD, posibles sanciones y daño reputacional**

## **5 Medidas**

**Revocar y cambiar credenciales, aplicar MFA, implementar detección continua de anomalías, auditoría interna y capacitación de seguridad**

## **6 Datos clave**

<b>Elemento</b>	<b>Detalle</b>	<b>Hora</b>	<b>Nota</b>
<b>Detección inicial</b>	<b>Consulta anómala en base de datos</b>	<b>07:30 UTC</b>	<b>Alerta</b>
<b>Inicio de sesión comprometido</b>	<b>Acceso desde IP extranjera</b>	<b>08:10 UTC</b>	<b>Mal uso de credenciales</b>
<b>Exfiltración de datos</b>	<b>Carga a nube no autorizada</b>	<b>09:00 UTC</b>	<b>Archivos críticos copiados</b>
<b>Contención</b>	<b>Aislamiento de red</b>	<b>11:20 UTC</b>	<b>Fuga detenida</b>

# Rapport d'enquête sur une fuite de données de recherche - BioNext

## 1. Vue d'ensemble

Le 12 septembre 2025, BioNext a découvert une fuite de données génétiques confidentielles. L'enquête a révélé une complicité interne et une intrusion externe.

## 2. Résumé de l'incident

- 07:30 UTC : Requêtes de base de données anormales détectées.
- 08:10 UTC : Connexion d'un employé depuis une IP étrangère inhabituelle.
- 09:00 UTC : Copie de fichiers vers un cloud non autorisé.
- 11:20 UTC : Fuite confirmée, réseau isolé.

## 3. Cause

Un employé a partagé ses identifiants avec un groupe de pirates, permettant extraction interne et intrusion externe.

## 4. Impact

Exposition de données d'édition génétique, pertes estimées à 5 MUSD, risques de sanctions et atteinte à la réputation

## 5. Mesures

Révoquer et renouveler les identifiants, appliquer MFA, détection continue des anomalies, audit interne, formation sécurité renforcée.

## 6. Données clés

Élément	Détail	Heure	Remarque
Détection initiale	Requête anormale en base de données	07:30 UTC	Alerte
Connexion compromise	Accès depuis IP étrangère	08:10 UTC	Identifiants abusés
Exfiltration de données	Envoi vers cloud non autorisé	09:00 UTC	Fichiers copiés
Confinement	Isollement du réseau	11:20 UTC	Fuite stoppée

- BioNext

1.

2025 12 BioNext .

2.

- 07: 30 UTC .
- 08: 10 UTC IP .
- 09: 00 UTC .
- 11: 20 UTC .

3.

.

4.

5

.

5.

.

6

		0730UTC	
	IP	0810UTC	
		0900UTC	
		1120UTC	