

## 2020 - North Korean hackers targeted U.S. pharmaceutical companies



Alejandro González Flórez – 16674  
José David González Villa - 13528

### **Seguridad Informática**

Gustavo Isaza

Manizales-Caldas

## Contenido

2020 - North Korean hackers targeted U.S. pharmaceutical companies .....	1
1. Descripción del ataque .....	3
a. Fecha: Diciembre de 2023.....	3
b. Lugar: Estados Unidos (empresas farmacéuticas con sedes globales) .....	3
c. Infraestructura: .....	3
d. Grupo atacantes: .....	3
2. Estrategia de explotación .....	4
a. Vector de entrada: .....	4
b. Técnicas y herramientas utilizadas: .....	4
c. Nivel de sofisticación: .....	4
3. Impacto y alcance .....	5
a. Sectores o servicios interrumpidos: .....	5
b. Magnitud de los daños:.....	5
c. Repercusiones internacionales:.....	5
4. Resultados logrados por el ataque .....	6
a. Qué se logró:.....	6
b. Ataque lateral: .....	6
c. Tiempo de recuperación: .....	6
d. Respuesta de NOAA/gobierno:.....	6
5. Descripción técnica breve.....	7
a. Tipo de malware/exploit:.....	7
b. Cómo funcionaba: .....	7
c. Contramedidas aplicadas y recomendadas (según entrevistas dadas):.....	7
6. Referencias .....	8

## 1. Descripción del ataque

**a. Fecha:** Diciembre de 2023

**b. Lugar:** Estados Unidos (empresas farmacéuticas con sedes globales)

**c. Infraestructura:**

Sistemas internos y redes corporativas de Johnson & Johnson y Novavax, enfocados en investigación y desarrollo de vacunas COVID-19.

**d. Grupo atacantes:**

Actores vinculados al gobierno de Corea del Norte (APT), específicamente Lazarus Group (según reportes de inteligencia surcoreana).

## **2. Estrategia de explotación**

### **a. Vector de entrada:**

Campañas de phishing dirigidas a personal con acceso a datos de investigación, posiblemente mediante correos electrónicos fraudulentos y enlaces maliciosos.

### **b. Técnicas y herramientas utilizadas:**

- Ingeniería social para obtener credenciales.
- Malware personalizado para infiltración en redes corporativas.
- Exploits en sistemas de correo y servidores VPN.

### **c. Nivel de sofisticación:**

Alto. Los atacantes usaron tácticas de ciber espionaje avanzado, indicativo de un grupo APT estatal.

### **3. Impacto y alcance**

#### **a. Sectores o servicios interrumpidos:**

No se reportaron interrupciones operativas visibles, pero se comprometieron datos sensibles sobre investigación de vacunas.

#### **b. Magnitud de los daños:**

El valor potencial de los datos es significativo, dado que incluían estudios clínicos y fórmulas experimentales.

#### **c. Repercusiones internacionales:**

- Aumento de tensiones diplomáticas entre EE.UU. y Corea del Norte.
- Preocupación sobre ciberseguridad en el sector farmacéutico global.
- Confirmación de que la pandemia incrementó la actividad de ciberespionaje.

## **4. Resultados logrados por el ataque**

### **a. Qué se logró:**

No se confirmó robo exitoso de datos, pero se detectaron intentos significativos. Las empresas reforzaron sus sistemas tras el incidente.

### **b. Ataque lateral:**

Posible movimiento lateral dentro de redes corporativas, aunque sin evidencia pública de filtración masiva.

### **c. Tiempo de recuperación:**

No hubo interrupción de producción, pero se implementaron medidas adicionales de seguridad en semanas posteriores.

### **d. Respuesta de NOAA/gobierno:**

Advertencias públicas y coordinación con agencias de ciberseguridad (CISA, FBI) para proteger el sector salud.

## 5. Descripción técnica breve

### a. Tipo de malware/exploit:

Probable uso de malware de puerta trasera (backdoor) y herramientas APT de Lazarus, además de phishing masivo.

### b. Cómo funcionaba:

El ataque comenzó con phishing, seguido de instalación de malware que permitía persistencia y exfiltración de datos.

### c. Contramedidas aplicadas y recomendadas (según entrevistas dadas):

- Autenticación multifactor (MFA).
- Segmentación de redes críticas.
- Monitoreo avanzado de intrusiones y actualización de políticas anti-phishing.

## 6. Referencias

- <https://www.reuters.com/article/us-health-coronavirus-northkorea-idUSKBN2A90ZC>
- [https://www.washingtonpost.com/world/asia\\_pacific/north-korea-covid-vaccine-hacking/2021/02/16/](https://www.washingtonpost.com/world/asia_pacific/north-korea-covid-vaccine-hacking/2021/02/16/)
- <https://www.wsj.com/articles/north-korea-tried-to-hack-into-pharma-firms-working-on-covid-vaccines-11613338800>
- <https://www.bbc.com/news/world-asia-56070618>
- [https://www.cisa.gov/news-events/alerts/2020/07/16/apt-actors-targeting-covid-19-vaccine-development?utm\\_source=chatgpt.com](https://www.cisa.gov/news-events/alerts/2020/07/16/apt-actors-targeting-covid-19-vaccine-development?utm_source=chatgpt.com)