2021. The French national cybersecurity agency announced that a four-year campaign

Alejandro González Flórez – 16674
José David González Villa - 13528

Seguridad Informática

Gustavo Isaza

Manizales-Caldas

Contenido

2021. The French national cybersecurity agency announced that a four-year campaign.....1
1. Descripción del ataque.....3
a. Fecha: Campaña descubierta en febrero de 2021 (actividad desde 2017).....3
b. Lugar: Francia (empresas proveedoras de servicios TI).....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:** Campaña descubierta en febrero de 2021 (actividad desde 2017)

b. **Lugar:** Francia (empresas proveedoras de servicios TI)

c. **Infraestructura:**

- Proveedores de servicios TI franceses.
- Redes corporativas de clientes finales a través de dichos proveedores (efecto en cadena).

d. **Grupo atacantes:**

Atribuido al grupo APT29 (también conocido como Cozy Bear), vinculado a los servicios de inteligencia rusos (SVR).

2. Estrategia de explotación

a. Vector de entrada:

Compromiso de proveedores TI para obtener acceso indirecto a sistemas de clientes, mediante la cadena de suministro (supply chain attack).

b. Técnicas y herramientas utilizadas:

- Explotación de vulnerabilidades en software de gestión.
- Ataques de spear-phishing a personal clave.
- Uso de credenciales comprometidas y escalamiento de privilegios.
- Herramientas personalizadas y técnicas similares a las usadas en la operación SolarWinds.

c. Nivel de sofisticación:

Muy alto. Se trató de un ataque persistente y prolongado, operado con gran discreción durante años.

3. Impacto y alcance

a. Sectores o servicios interrumpidos:

- Empresas de TI en Francia.
- Riesgo de compromiso para empresas clientes en sectores sensibles: energía, telecomunicaciones, defensa.

b. Magnitud de los daños:

Impacto potencial elevado por el acceso a redes críticas a través de proveedores. No se divulgaron cifras exactas.

c. Repercusiones internacionales:

- Refuerzo de la preocupación sobre ataques a la cadena de suministro tras SolarWinds.
- Tensiones diplomáticas entre Francia y Rusia.
- Recomendaciones internacionales de endurecer la seguridad en proveedores TI.

4. Resultados logrados por el ataque

a. Qué se logró:

Compromiso prolongado de proveedores TI, lo que permitió espionaje y posible exfiltración de información sensible de múltiples organizaciones francesas.

b. Ataque lateral:

Sí, a través del acceso a redes de los clientes de los proveedores comprometidos.

c. Tiempo de recuperación:

La mitigación completa llevó meses, dado que la campaña estuvo activa durante cuatro años sin ser detectada.

d. Respuesta de NOAA/gobierno:

- Emisión de una alerta oficial con detalles técnicos y recomendaciones.
- Coordinación con empresas afectadas y autoridades europeas para la contención.

5. Descripción técnica breve

a. Tipo de malware/exploit:

- Herramientas personalizadas de APT29 (Cozy Bear).
- Backdoors persistentes en sistemas de administración de red.

b. Cómo funcionaba:

El ataque probablemente consistió en:

- Compromiso inicial mediante spear-phishing o exploits.
- Persistencia mediante puertas traseras en redes TI.
- Movimiento lateral hacia entornos de clientes.
- Exfiltración silenciosa de información crítica

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

- Segmentación estricta entre redes internas y de proveedores.
- Monitoreo continuo y auditoría de conexiones de terceros.
- Autenticación multifactor en accesos privilegiados.
- Parches urgentes en herramientas de administración vulnerables.

6. Referencias

- https://www.cert.ssi.gouv.fr/actualite/CERTFR-2021-ACT-005
- **https://www.reuters.com/article/us-france-cyber-russia-idUSKBN2AA1M8**
- https://thehackernews.com/2021/02/france-says-russian-hackers-are-behind.html
- https://www.bbc.com/news/world-europe-56046768