2023 - Russian forces in occupied Crimea reported a cyberattack on Crimean Internet

Alejandro González Flórez – 16674
José David González Villa - 13528

Seguridad Informática

Gustavo Isaza

Manizales-Caldas

Contenido

1. Descripción del ataque

a. **Fecha:** Septiembre de 2023

b. **Lugar:** Crimea (territorio ocupado por Rusia)

c. **Infraestructura:**

Proveedores de Internet en la península de Crimea, con afectación en el acceso a la red y posibles interrupciones en telecomunicaciones.

d. **Grupo atacantes:**

Atribución no confirmada, pero se presume que actores vinculados a Ucrania realizaron el ataque, en el contexto de la ofensiva militar.

2. Estrategia de explotación

a. Vector de entrada:

Ataque dirigido contra la infraestructura de red de los ISP (Internet Service Providers). Posible uso de DDoS masivo o inyección de malware en sistemas de gestión.

b. Técnicas y herramientas utilizadas:

- Ataques DDoS (Distributed Denial of Service) para saturar la conectividad.
- Intrusión en redes de gestión de los proveedores.
- Posible uso de exploits en routers o sistemas SCADA/Telco.

c. Nivel de sofisticación:

Medio-alto. Se sospecha coordinación con operaciones militares, lo que indica un componente de guerra híbrida.

3. Impacto y alcance

a. Sectores o servicios interrumpidos:

- Proveedores de Internet locales.
- Servicios gubernamentales y militares que dependían de esa conectividad.
- Comunicaciones civiles y comerciales en la región.

b. Magnitud de los daños:

Afectación temporal de la conectividad en varias zonas de Crimea. Se desconoce la pérdida de datos, pero se presume un impacto operativo significativo en las fuerzas rusas.

c. Repercusiones internacionales:

- Incremento de tensiones entre Rusia y Ucrania.
- Posible preocupación en OTAN sobre ciberarmas en conflictos híbridos.
- Señal de que Ucrania puede combinar ataques físicos (misiles) con ciberataques sincronizados.

4. Resultados logrados por el ataque

a. Qué se logró:

Interrupción parcial del acceso a Internet en Crimea en el mismo marco temporal que un ataque con misiles a la sede naval rusa, posiblemente retrasando comunicaciones militares.

b. Ataque lateral:

No hay confirmación pública de movimientos laterales en otras redes fuera de Crimea.

c. Tiempo de recuperación:

No se informó oficialmente, pero se estima entre horas y pocos días.

d. Respuesta de NOAA/gobierno:

Medidas de contingencia en redes militares y declaraciones acusando a Ucrania; sin detalles técnicos públicos.

5. Descripción técnica breve

a. Tipo de malware/exploit:

No confirmado públicamente. Posible uso de botnets para DDoS y explotación de vulnerabilidades en equipos de telecomunicaciones.

b. Cómo funcionaba:

El ataque probablemente consistió en:

- Saturación de enlaces críticos (DDoS).
- Posible intrusión en sistemas de gestión (mediante exploits).
- Coordinación temporal con ataque físico para maximizar el caos.

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

- Segmentación de redes críticas.
- Implementación de filtros anti-DDoS y sistemas de redundancia.
- Refuerzo de autenticación y monitoreo en dispositivos de telecomunicaciones.

6. Referencias

- https://www.reuters.com/world/europe/russian-official-says-ukraine-struck-black-sea-navy-hq-with-missile-2023-09-22

- https://www.bitdefender.com/en-us/blog/hotforsecurity/massive-ddos-attack-takes-out-crimean-internet

- https://kyivindependent.com/large-scale-cyber-attack-reported-in-occupied-crimea

- **https://www.pravda.com.ua/eng/news/2023/09/22/7420982**

- **https://www.aljazeera.com/news/2023/9/23/russia-ukraine-war-list-of-key-events-day-577**