INVESTIGACIÓN SOBRE EL GRUPO SANDWORM

Historia y Origen

Sandworm es un grupo de amenazas persistentes avanzadas (APT), que se cree que está vinculado a la inteligencia rusa, específicamente al GRU (Dirección Principal de Inteligencia de Rusia). Se menciona por primera vez en 2014, cuando se sospecha que el grupo fue responsable de ataques cibernéticos dirigidos a Ucrania durante la crisis de Crimea. Su primer ataque conocido ocurrió en diciembre de 2015, cuando afectó el sistema energético de Ucrania, causando un apagón que impactó a miles de hogares.

Desde sus inicios, Sandworm ha evolucionado en sus tácticas y técnicas, utilizando herramientas cada vez más sofisticadas, incluyendo malware específico como BlackEnergy y NotPetya.

Objetivos y Finalidad

Los objetivos primarios de Sandworm son la desestabilización y el sabotaje. El grupo busca desestabilizar y deslegitimar gobiernos considerados enemigos de Rusia, especialmente en la región de Europa del Este. Sus ataques han estado dirigidos a infraestructuras críticas, como redes eléctricas, sistemas de transporte y telecomunicaciones. A través de sus operaciones, Sandworm no solo causa daño inmediato, sino que también recolecta inteligencia y envía un mensaje de poder y capacidad de respuesta de Rusia frente a sus adversarios.

Organización y Estructura

Se cree que Sandworm está compuesto por un grupo de hackers altamente capacitados, muchos de los cuales tienen antecedentes en ciberseguridad y en inteligencia militar. Su estrategia de operaciones incluye el uso de malware como BlackEnergy, que se utiliza para ataques de denegación de servicio y sabotaje de sistemas industriales, y NotPetya, diseñado inicialmente para un ataque contra Ucrania, pero que se extendió posteriormente a nivel global causando daños significativos a múltiples organizaciones.

El grupo emplea tácticas de *phishing* y explotación de vulnerabilidades para obtener acceso a redes objetivo y ha utilizado técnicas de ingeniería social para infiltrarse en organizaciones. Además, se ha sugerido que Sandworm tiene conexiones con otros grupos de APT rusos, lo que indica un posible apoyo y colaboración dentro del ecosistema de ciberespionaje ruso.

Herramientas Más Utilizadas por Sandworm

- **Industroyer e Industroyer2**: Estas herramientas de *malware* están diseñadas para atacar sistemas de control industrial (ICS) y redes SCADA. Han sido utilizadas en ataques a la infraestructura eléctrica de Ucrania, permitiendo a Sandworm causar interrupciones significativas en el suministro de energía.
- **BlackEnergy**: Este kit de herramientas permite crear *botnets* que pueden realizar ataques de denegación de servicio (DDoS). BlackEnergy ha sido parte de varios ataques dirigidos a infraestructuras críticas, siendo un componente clave en la estrategia del grupo para generar caos.
- **NotPetya**: Originalmente una variante del *ransomware* Petya, NotPetya se caracteriza por destruir datos en sistemas infectados y tiene la capacidad de propagarse a través de redes usando vulnerabilidades conocidas. Su uso en 2017 provocó daños económicos globales que superaron los 10 mil millones de dólares.
- **KillDisk**: Esta herramienta se utiliza para eliminar de forma permanente los datos de los discos duros, dejando los sistemas inoperativos. Sandworm la ha empleado en ataques contra Ucrania, buscando desestabilizar el funcionamiento de infraestructuras esenciales.
- **Olympic Destroyer**: Utilizada durante los Juegos Olímpicos de Pyeongchang en 2018, esta herramienta está diseñada para hacer que los sistemas infectados sean inoperativos, y se propaga de manera que maximiza el daño en las redes afectadas.
- **CaddyWiper**: Este *malware* se centra en borrar datos y aplicaciones de los sistemas, dejando a las víctimas sin acceso a su información. Ha sido utilizado en ataques a agencias gubernamentales en Ucrania, mostrando su efectividad en operaciones destructivas.
- **Cyclops Blink**: Lanzado en 2022, este *malware* permite a los atacantes construir *botnets* que afectan dispositivos específicos, como *routers*, facilitando el control remoto y la recopilación de datos.
- **Infamous Chisel**: Este conjunto de herramientas fue identificado en ataques recientes, apuntando a dispositivos móviles utilizados por el ejército ucraniano. Permite la recolección continua de datos de los dispositivos comprometidos.