APT28

Mauro Piano
Diego Camilo Silva
Iñigo Calero
Antton Urtiaga

INTRODUCCIÓN

En un mundo cada vez más interconectado, la ciberseguridad se ha convertido en una preocupación crítica. Dentro de este panorama, destacan las amenazas avanzadas persistentes, o APTs, que representan una forma altamente sofisticada de ataque cibernético. En esta presentación, exploraremos el caso del APT28, también conocido como Fancy Bear, y sus implicaciones en la seguridad digital.

OBJETIVOS

El APT28 tiene como objetivo principal el espionaje cibernético y la recopilación de información sensible. Sus actividades han apuntado a gobiernos, organizaciones militares, agencias de inteligencia, partidos políticos y empresas de tecnología, entre otros.

MÉTODO DE PROPAGACIÓN

El APT28 utiliza una variedad de métodos de propagación, incluyendo campañas de phishing altamente sofisticadas que emplean correos electrónicos y sitios web falsos para engañar a las víctimas y obtener acceso a sus sistemas. También se han observado casos de exploits de día cero y técnicas de ingeniería social.

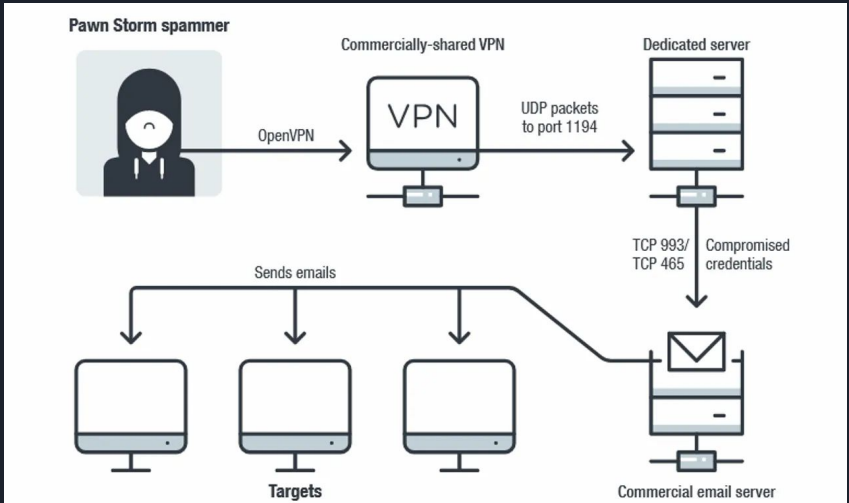
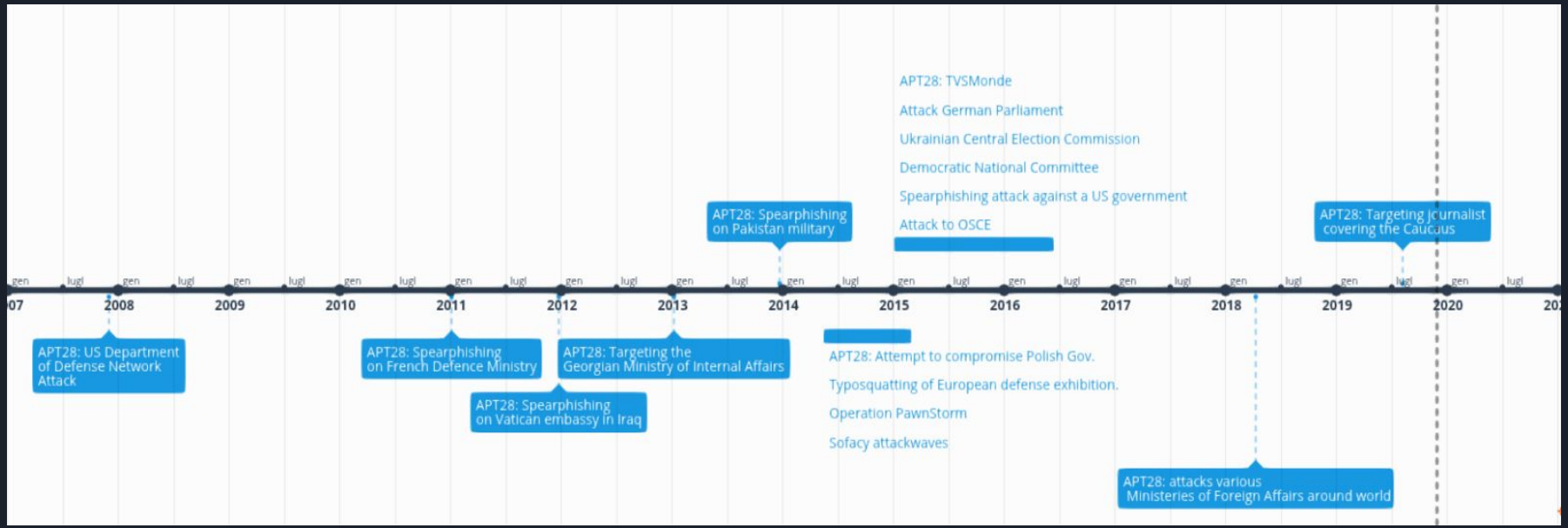


Figure 1. The setup Pawn Storm frequently used to send credential phishing spam in 2019

AÑO DE DESCUBRIMIENTO

Las actividades del APT28 fueron identificadas por primera vez en 2007, aunque su presencia se ha mantenido desde entonces con diversas campañas y objetivos en todo el mundo.

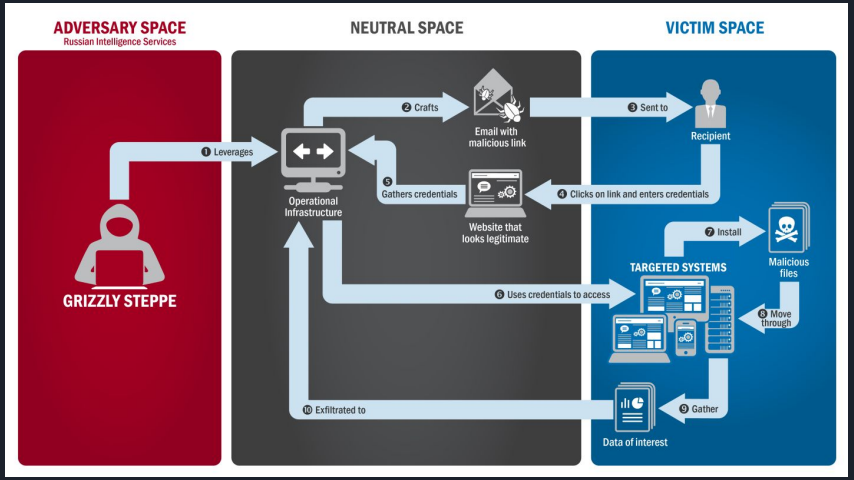


ALCANCE DEL ATAQUE

El APT28 ha afectado a una amplia gama de organizaciones en diferentes sectores, incluyendo gobiernos, militares, empresas de defensa, medios de comunicación, empresas de tecnología y organizaciones no gubernamentales. Sus ataques han tenido un alcance global, con víctimas en varios países.

TECNICAS Y HERRAMIENTAS

El APT28 emplea una variedad de técnicas y herramientas avanzadas, incluyendo malware personalizado, exploits de día cero, herramientas de phishing sofisticadas y técnicas de evasión de detección. Su capacidad para adaptarse y utilizar nuevas tácticas lo hace especialmente difícil de detectar y contener.



CONEXIONES CON ACTORES ESTATALES

Se cree que el APT28 tiene vínculos con agencias de inteligencia rusas, aunque esto no ha sido confirmado de manera definitiva. Sus actividades han sido consistentes con los intereses geopolíticos de Rusia, especialmente en lo que respecta al espionaje cibernético y la influencia política.

CONCLUSIONES

El APT28 representa una seria amenaza para la seguridad cibernética global, con capacidad para llevar a cabo operaciones altamente sofisticadas y dirigidas. La detección temprana, la educación en ciberseguridad y la colaboración internacional son fundamentales para mitigar su impacto y proteger los sistemas digitales contra este tipo de amenazas.