Publicado en Madrid el 26/10/2023

Ciberespionaje, desinformación o phising, las 'ciberconsecuencias' del conflicto palestino-isaraelí

La compañía de ciberseguridad S2 Grupo ha realizado un análisis del impacto del conflicto entre Palestina e Israel en el ámbito cibernético y ha constatado que se está desarrollando principalmente por parte de grupos hacktivistas. Aun así, los expertos en ciberseguridad prevén que en breve comience la acción de organizaciones APT a través de ciberespionaje, desinformación o phising, entre otras acciones

En un comunicado, la empresa de origen valenciano S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, ha advertido de que el conflicto palestino-israelí, además de desarrollarse en el plano físico, ya está teniendo impacto en el ámbito de la ciberseguridad mundial.

"Uno de los principales impactos de este conflicto es el incremento del riesgo cibernético contra entidades públicas y privadas de países occidentales que se hayan mostrado cercanos a Israel, principalmente por grupos hacktivistas y en menor medida de grupos APT (amenazas persistentes avanzadas, por sus siglas en inglés)", ha afirmado José Rosell, socio-director de S2 Grupo.

En este sentido, la compañía asegura que los grupos de ciberamenazas aprovecharán el conflicto para aumentar las campañas de explotación, ataque e influencia. Los principales objetivos de esas campañas de ciberdelincuencia serán, según S2 Grupo, las infraestructuras críticas de sectores estratégicos de entidades occidentales ubicadas tanto en Oriente Medio como en Occidente.

Según los datos de S2 Grupo, desde que comenzó el conflicto armado "se ha registrado un aumento de acciones ciberofensivas por parte de numerosos grupos hacktivistas mayoritariamente propalestinos contra organismos gubernamentales israelíes". No obstante, también hay constancia de la participación de grupos hacktivistas favorables a Israel. Es el caso del ciberataque contra Alfanet, el mayor proveedor de servicios de Internet en Palestina.

Los objetivos de los ciberataques en este contexto "se centrarán en actuar contra las infraestructuras críticas y sectores estratégicos" de los países enfrentados.

En su comunicado, S2 Grupo advierte de que también serán foco de los ciberdelincuentes los organismos públicos y entidades privadas que les puedan prestar algún apoyo ya sea económico, político, militar o humanitario, entre otros.

Aunque, por el momento, la actividad ciberofensiva se está centrando en acciones procedentes de hacktivistas, el equipo de S2 Grupo advierte que es fundamental tener en cuenta a los grupos APT con supuestas vinculaciones a otros Estados alineados con las tesis palestinas, que podrían estar desarrollando campañas de explotación o ataque para las próximas semanas.

Junto a esto, desde la compañía de seguridad se ha enfatizado que también es probable que grupos APT vinculados a otros Estados no directamente implicados puedan utilizar este conflicto para llevar a cabo campañas de phising o influencia (a través de desinformación o fakenews, por ejemplo).

Datos de contacto:
Luis Núñez
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Sociedad Madrid Ciberseguridad