Publicado en Madrid el 31/08/2023

El apoyo de España a Ucrania pone al país en el foco de los hacktivistas rusos

La empresa S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, ha elaborado de la mano de su equipo de expertos en ciberinteligencia Lab 52, el informe 'Impacto del ciberespacio en el actual conflicto entre Rusia y Ucrania'. En éste se analiza cómo la guerra entre Rusia y Ucrania está impactando en el ámbito cibernético y en la ciberseguridad

Una de las principales conclusiones que se desprenden del informe es que la utilización del ciberespacio en el conflicto ruso-ucraniano está siendo muy recurrente, llegando incluso a afectar a las infraestructuras críticas de países no implicados directamente en la contienda, como es el caso de España.

"Últimamente se han registrado un elevado número de campañas efectuadas por grupos hacktivistas mediante ciberataques DDoS, ataques de denegación de servicio que impiden acceder a los sistemas, y España ha sido amenazada por el envío de armamento pesado a Ucrania. Esto hace que las empresas, infraestructuras críticas y organizaciones de todo tipo estén en cierto riesgo y, por tanto, es necesario incrementar las medidas de seguridad", ha explicado José Rosell, socio-director de S2 Grupo.

En el informe que ha sido remitido a los medios, se han incluido más de 20 recomendaciones de ciberseguridad que permitirán a las entidades de todo tipo, privadas o públicas, que se ciberprotejan y minimicen el riesgo de ser víctimas de un ciberataque.

Entre éstas se incluye: limitar el número de conexiones por dirección IP, implantar la autenticación multifactor para conexiones de servicios remotos autenticados desde Internet a la infraestructura (correo electrónico, VPN, etc.), eliminación de sistemas de terminal remota expuestos directamente a Internet, aplicación de parches y actualizaciones de seguridad en los sistemas, realizar copias de seguridad adecuadas y desconectadas de la red.

Además, el equipo de expertos en ciberinteligencia de S2 Grupo han resaltado que en caso de sospechar que sus sistemas pueden verse comprometidos, es decir, que puedan estar siendo víctimas de algún tipo de acción ciberdelictiva, se recomienda contactar lo antes posible con un CERT (Equipo de Respuesta ante Emergencias Informáticas).

En el informe también se recogen otros aspectos como, por ejemplo, de qué modo está afectando este conflicto bélico en el ciberespacio, principales objetivos y actores implicados o un análisis de los principales ciberataques a las infraestructuras críticas que se han producido.

Datos de contacto:

Luis Núñez Canal
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Madrid Ciberseguridad