Publicado en Madrid el 10/07/2024

España registra en 2024 un aumento "sin precedente" de ciberataques

Los primeros meses de 2024 han registrado un aumento histórico en incidentes de ciberseguridad en España. En este contexto, Lab52, el equipo de ciberinteligencia de S2 Grupo, ha elaborado un informe de urgencia para analizar qué tipo de amenazas están afectando a España, cómo se han realizado y cómo protegerse de ellas

Según ha anunciado la compañía de ciberseguridad en un comunicado, los ciberdelitos de ataques de denegación de servicio (DDoS) de origen prorruso, la filtración de datos confidenciales sustraídos de organizaciones y su publicación en foros clandestinos, el hacktivismo y ransomware ha afectado a España de una manera sin precedente. En este sentido, "los sectores gubernamental y transporte han sido los más afectados".

En lo que se refiere a las cifras, el informe de S2 Grupo detalla que se han producido 27 publicaciones de filtraciones y robos de datos referentes a entidades españolas. Además, Lockbit, que es el grupo más activo, ha realizado 26 ciberataques en España. En relación a los ataques ransomware en Europa, el 12% han sido realizados a organizaciones españolas.

Entre los sectores más afectados por estas filtraciones y robo de datos han destacado en primer lugar el sector público, seguido por el educativo, bancario y telecomunicaciones. Sin embargo, los ataques producidos a través de ransomware han sido los más comunes en la administración pública, manufactura, alimentación y servicios de consumo.

"Se ha identificado una posible correlación entre los ataques cibernéticos y ciertos eventos geopolíticos internacionales. Podemos ver cómo fechas reseñables a nivel político, principalmente relacionadas con las guerras Rusia-Ucrania e Israel-Palestina, coinciden con la proliferación de ciberataques", ha declarado José Rosell, CEO de S2 Grupo.

"Aunque no se ha podido determinar un origen común para todas las filtraciones, existe la posibilidad de que estos incidentes formen parte de campañas estratégicas de influencia por parte de agentes externos", ha continuado Rosell.

Grupos rusos

En el primer semestre de 2024, las ciberamenazas han estado diversificadas, los grupos hacktivistas prorrusos como NoName057(16) y CyberArmyofRussia han sido algunos de los más activos junto a grupos de ciberatacantes mediante ransomware como Lockbit, BlackBasta y Cl0p.

Desde el equipo de ciberinteligencia de S2 Grupo se ha explicado que la información robada se vende como producto (venta de bases de datos o documentos confidenciales) o servicio (venta de las credenciales para acceder a los servicios comprometidos) en plataformas clandestinas de Internet

como pueden ser la Clearnet, la Darkweb o en grupos Telegram.

¿Cómo protegerse del cibercrimen en 2024?
Desde S2 Grupo se ha señalado que en el contexto actual marcado por las tensiones a nivel político internacional, "es clave poner la atención para incrementar la ciberseguridad de administraciones públicas, empresas y organizaciones de todo tipo".

Los expertos de la compañía recomiendan "hacer seguimiento de los sucesos geopolíticos". En este sentido, el equipo de ciberinteligencia de S2 Grupo ha explicado que se ha detectado un patrón en los hacktivistas por el que aprovechan eventos clave de geopolítica para poner en marcha sus campañas cibernéticas. "Con lo que conocerlos es fundamental para poder anticiparse a posibles amenazas".

A su vez, S2 Grupo indica la importancia del "diseño de una estructura de ciberseguridad escalable" pues es "muy importante implementar redundancias en servidores y servicios críticos, reducción del tráfico por IP y la implementación de herramientas que impidan la denegación de servicios".

Otro factor esencial es estudiar a fondo la infraestructura que se ha de ciberproteger, analizar todas sus vulnerabilidades desde el punto de vista de los cibercriminales (sus activos, información de valor, países en los que está presente, etc.) para anticipar cualquier acción que pueda poner en riesgo a la entidad.

Desde S2 Grupo se ha resaltado que para llevar a cabo un plan de defensa frente a los grupos cibercriminales y ransomware "es necesario desarrollar una estrategia integral de prevención que contemple aspectos como la monitorización en tiempo real; detección y bloqueo en red; supervisión, recopilación y análisis de datos; disponer de una metodología de análisis proactivo de ciberamenazas; y la incorporación de un sistema sofisticado de inteligencia de ciberamenazas que detecte Amenazas Persistentes Avanzadas", entre otros.

Datos de contacto:
Luis Núñez
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Investigación Científica Software Ciberseguridad