Publicado en Madrid el 18/05/2022

# Fake news sobre el conflicto ruso y falsas campañas humanitarias, nuevos reclamos del cibercrimen en España

**Según el Observatorio de Ciberseguridad de Exprivia, en el primer trimestre del año los datos empeoran en comparación con los tres primeros meses de 2021. Sin embargo, se han perpetrado cerca de un 16% menos delitos cibernéticos que en el último trimestre de 2021**

El último Informe sobre ciberamenazas del Observatorio de Ciberseguridad de Exprivia aporta datos actualizados sobre los delitos cometidos en la red en el primer trimestre del 2022, principalmente relacionados con la pandemia y el conflico bélico ruso-ucraniano. Y así, entre enero y marzo, registra 97 casos entre ataques, incidentes y violaciones de la privacidad, ligeramente por debajo de la media registrada en trimestres anteriores.

En concreto, hubo cerca de un 16% menos de casos que en el último trimestre de 2021 (cuando se produjeron 113 incidentes), con 24 eventos en enero, 38 en febrero y 35 en marzo, un mes de especial importancia ya que los ciberdelincuentes aprovecharon la inestabilidad internacional con el pretexto de la guerra entre Rusia y Ucrania. Según el Observatorio Exprivia, que tiene en cuenta 113 fuentes públicas, en estos primeros meses de 2022, además del GDPR y la banca, que mantienen la primacía, entre los pretextos para atacar a las víctimas también está la guerra entre Rusia y Ucrania con frecuentes engaños que se esconden detrás de noticias falsas sobre el conflicto o de falsas campañas de ayuda humanitaria.

El informe muestra que entre enero y marzo se produjeron 20 ataques, 39 incidentes de seguridad con éxito y 38 violaciones de la privacidad. Así, sigue creciendo la percepción de que, a pesar de las inversiones realizadas en seguridad en los últimos años, los delincuentes son cada vez más numerosos y eficaces, causando daños relacionados principalmente con el robo de datos y dinero.

"En los dos últimos años, los acontecimientos de gran repercusión política y económica y las tensiones sociales asociadas han permitido a los delincuentes aprovechar ocasiones como el Covid o el conflicto entre Rusia y Ucrania para engañar a las víctimas, en la mayoría de los casos con ánimo de lucro", comenta Domenico Raguseo, director de Ciberseguridad de Exprivia. En el ilimitado ecosistema digital en el que todos vivimos, no es fácil atribuir las causas y los orígenes geográficos de los ciberdelitos; si un ataque se desarrolla para una víctima determinada, también podría afectar a otros sujetos y, si un malware se utiliza para un fin concreto, pronto pasará a ser propiedad de otros delincuentes que lo utilizarán para fines distintos. Por lo tanto, si en este momento estamos experimentando los primeros daños causados en estos meses por el conflicto bélico, que se está produciendo no sólo sobre el terreno sino también en la red, las consecuencias podrían ser aún más graves en los próximos meses.

Según el Observatorio Exprivia, en el primer trimestre de 2022, el sector de las Finanzas -que abarca desde las entidades bancarias hasta las compañías de seguros y las plataformas de criptomonedas-

fue el que registró un mayor número de delitos (18), con un pico de 12 casos sólo en febrero, entre los que se encuentran robos de datos de tarjetas de crédito, accesos a cuentas bancarias y peticiones de dinero. Le siguió el sector del entretenimiento, con 15 casos de ataques, incidentes y violaciones de la privacidad. En tercer lugar, con 14 casos, se encuentra el sector de Software/Hardware, es decir, empresas de TIC, servicios digitales, plataformas de comercio electrónico, dispositivos y sistemas operativos, que sufren principalmente el robo de datos, como credenciales de acceso o información sensible.

"Existe una creciente preocupación por la ciberdelincuencia en las fuentes analizadas por nuestro Informe, en parte como resultado de la creciente criticidad de los servicios digitales de los que dependemos. Cuanto mayor sea el impacto y la duración de un incidente o simplemente de un ataque, menos probable será que pase desapercibido", señala Raguseo. Incluso en los medios de comunicación, la visibilidad y la relevancia de la ciberdelincuencia está aumentando a medida que los delincuentes explotan nuevas vulnerabilidades".

Entre las técnicas más utilizadas por los ciberdelincuentes está el uso de malware, con 31 casos. Por otro lado, hay un alto uso de técnicas de phishing -con 20 casos- como vector de ataque para robar información sensible. Tampoco hay que subestimar la explotación de vulnerabilidades conocidas que están causando graves daños reputacionales y económicos a diversas organizaciones y empresas.

Exprivia
Exprivia dirige un grupo internacional especializado en Tecnologías de la Información y la Comunicación, capaz de abordar los motores del cambio en el negocio de sus clientes a través de las tecnologías digitales.

Con un know-how consolidado y una larga experiencia por su constante presencia en el mercado, el grupo cuenta con un equipo de expertos especializados en diferentes campos y dominios tecnológicos, desde Mercado de Capitales, Credit & Risk Management a IT Governance, desde BPO a Ciberseguridad, desde Big Data a Cloud, desde IoT a Mobile, desde networking a colaboración empresarial y SAP. El grupo presta apoyo a sus clientes en los sectores de la banca y las finanzas, las telecomunicaciones y los medios de comunicación, la energía y los servicios públicos, la industria aeroespacial y la defensa, la fabricación y la distribución, la sanidad y el sector público. Su oferta incluye soluciones consistentes en productos propios y de terceros, y servicios de ingeniería y consultoría.

Hoy el grupo cuenta con unos 2.400 profesionales en 7 países del mundo.

Exprivia S.p.A. cotiza en la Bolsa italiana en el mercado Euronext de Milán (XPR).

La empresa está sujeta a la dirección y coordinación de Abaco Innovazione S.p.A.www.exprivia.it

**Datos de contacto:**

Elena Gallego
SEC Newgate Spain
+34 618 553 747

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Finanzas Sociedad E-Commerce Ciberseguridad