FARO DE VIGO
VIERNES, 8 DE NOVIEMBRE DE 2019

Los peligros de la red

Vigo registra 1.400 ciberataques al día, más que Extremadura, Navarra y Cantabria juntas

La ciudad olívica sufre la mitad de los casos detectados en la provincia de Pontevedra y uno de cada cinco de Galicia ▶ La amenaza más común muestra anuncios de forma abusiva e instala aplicaciones sin consentimiento

BORJA MELCHOR

Los delincuentes han modificado su ámbito de actuación y sus herramientas: perpetran las fechorías sin necesidad de desplazarse y ya no se ven obligados a vestir pasamontañas para mantenerse en el anonimato. Con la irrupción epidémica de las nuevas tecnologías en la sociedad de la información, capital para entender el mundo globalizado e interconectado en el que vivimos, los malhechores han encontrado en Internet un novedoso procedimiento para asaltar algo tan valioso como la intimidad. Su auge es tal que, actualmente, los ciberdelitos ya son la transgresión de la ley que más se comete en Vigo. La unidad policial dedicada a estos casos está "desbordada", según advierten fuentes de la Comisaría, y los ataques informáticos registrados en la ciudad superan en número a la suma de los detectados en las comunidades autónomas de Extremadura, Navarra y Cantabria.

Así lo señala el Instituto Nacional de Ciberseguridad de España (Incibe), que descubrió en el segundo cuatrimestre de este año –entre mayo y agosto– una media mensual de 44.130 activos tecnológicos únicos con problemas de seguridad en la metrópolis olívica. Es decir, más de 1.400 equipos, sistemas, servicios o redes sufrieron cada día alguna acción maliciosa, cifra superior a la registrada en cualquier otro punto de Pontevedra, la provincia gallega más afectada: registró un total de 89.726 casos de media al mes –unos 2.900 diarios–, seguida por A Coruña, Ourense y Lugo. Vigo aglutina, así, casi la mitad de las amenazas cibernéticas que se producen en la provincia, con un 49,18%, muy por delante de la ciudad del Lérez, que se sitúa segunda, con un porcentaje del 18%, y de municipios como Vilagarcía de Arousa, Ponteareas, Cangas do Morrazo, Nigrán, Moaña, Bueu, Tomiño y Sanxenxo, que completan la lista. En términos autonómicos, acumula el 21,44% de los recursos que fueron objeto de una actividad perjudicial.

Galicia, con 205.864 amenazas de media mensuales –en torno a 6.800 cada 24 horas– es la quinta región española que recibe mayor cantidad de asaltos en la red, seguida de la Comunidad Valenciana, Andalucía, Madrid y Cataluña: estas tres últimas acumulan más del 50% del total a nivel nacional. En el otro extremo, se colocan, en este orden, Asturias, Islas Baleares, Extremadura, Navarra, Cantabria, La Rioja, Ceuta y, en la última posición, Melilla. Entre estos ataques informáticos, destacan el *phishing* –técnica fraudulenta en Internet con la que se busca obtener información privada de los usuarios, como nombres de acceso a cuentas bancarias, contraseñas o datos de las tarjetas de crédito, por medio de la falsificación de páginas que el usuario conoce, las cuales se duplican y, en ellas, se pide que se introduzcan datos confidenciales que se quiere obtener–; el *malware* –programa o código informático malicioso que tiene como función dañar un sistema o causar un mal funcionamiento–; el envío de *spam* –correo electrónico de distribución masiva y contenido normalmente publicitario o maligno que se recibe sin haberlo solicitado–; y la exfiltración de datos –sutracción de valiosa información–.

LOS ATAQUES MÁS FRECUENTES

1 ***Arrkii* (más del 60%)**
Muestra anuncios de forma abusiva, efectúa fraude publicitario haciendo clic en anuncios sin interacción por parte del usuario e instala aplicaciones sin permiso.

2 ***Elex* (menos del 10%)**
Es un *adware*: un tipo de *software* malicioso que se ejecuta para exhibir publicidad no deseada. Se considera un complemento o una extensión del navegador.

3 ***Uupay* (menos del 9%)**
Roba información del dispositivo y puede descargar *malware* adicional. Bloquea las actualizaciones de seguridad del sistema operativo.

3 ***PrizeRAT* (menos del 9%)**
Recoge datos personales del usuario, como el número de teléfono y la ubicación, y envía los datos a un servidor remoto. Opera con SMS.

Amenazas más habituales

Destaca sobremanera la actividad de *Arrkii*, presente en más del 60% de las amenazas. Según informan fuentes del Incibe, se trata de un SDK (kit de desarrollo de *software*) de publicidad que se ajusta a la definición de lo que Google considera un "comportamiento malicioso realizado por una aplicación".

> Galicia es la quinta comunidad que más amenazas recibe en activos tecnológicos

Se incluye con *apps* instaladas en una vasta cantidad de dispositivos Android en todo el mundo y realiza acciones consideradas abusivas o que atañen algún tipo de riesgo: muestra anuncios de forma abusiva, efectúa fraude publicitario haciendo clic en anuncios sin interacción por parte del usuario, instala programas de manera silenciosa y sin consentimiento y, en algunos casos, carga código oculto y/o cifrado; además, dispone de un mecanismo de actualización automática. En segundo lugar, se sitúa *Elex*, que protagoniza menos del 10% de los casos: es un *adware*, esto es, un tipo de *software* malicioso que se ejecuta en el ordenador para exhibir publicidad no deseada; se considera un complemento o una extensión del navegador web.

¿Qué hacer para no caer en las redes de los delincuentes de Internet?

Con el fin de proteger a los usuarios frente a las tentativas de pirateo, la Interpol aconseja poner en práctica una batería de medidas que ahondan en la seguridad de los equipos informáticos y ayudan a no convertir nuestra información confidencial en un blanco fácil de los delincuentes que utilizan Internet como "campo de batalla".

▪ **Actualizaciones.** Mantener al día los equipos personales y empresariales: prestar atención a las alertas de seguridad, actualizar los parches y completar periódicamente las verificaciones del sistema.

▪ **Contraseñas.** Utilizar claves distintas para cada cuenta y cambiarlas cada cierto tiempo: deben incluir cifras, símbolos y letras mayúsculas y minúsculas.

▪ **Privacidad.** La organización policial recomienda no publicar información confidencial o personal en medios sociales, ya que puede ser utilizada por los estafadores.

▪ **Correo electrónico.** No comunicar la contraseña; no pinchar en archivos adjuntos que no se hayan pedido previamente, incluso si tienen nombres que suenan inofensivos –como "factura"– ya que, a menudo, contienen códigos maliciosos que dan acceso al control de los correos electrónicos y a las actividades de los ordenadores; activar el filtro de correo *spam*; y bloquear el acceso a páginas sospechosas o que figuran en listas negras. Si el banco se pone en contacto por *e-mail* para actualizar información o proponer una oferta, no pinche. Consulte su web oficial o llame a la entidad.

▪ **Protección.** Utilizar antivirus, cortafuegos y otras herramientas; realizar análisis frecuentes de ordenadores y dispositivos para evitar las infecciones de códigos maliciosos.

▪ **Compras.** No realizar ningún pago en línea ni ninguna actividad de banca electrónica con conexión a una wifi pública, puesto que la información podría ser robada fácilmente.

▪ **Transacciones.** Tener cautela con las transacciones de grandes sumas de dinero: hay métodos de pago disponibles mucho más seguros. No se deje engañar por estafadores que le pidan transferencias a sus cuentas bancarias.