El Financiero (Costa Rica)

Ciberdelincuentes se concentran en grupos vulnerables

Algunas poblaciones sufren más los ataques, en particular las mujeres

Crimen · Internet · Negocio

10 jul. 2021 Carlos Cordero Pérez carlos.cordero@elfinancierocr.com

Los ataques en Internet de hackers y otros delincuentes tienen la mira a algunos sectores de población y empresas que presentan mayor nivel de vulnerabilidad tanto por desigualdades sociales, de edad y de género como por su nivel de madurez digital.

La mayoría de empresas y usuarios son conscientes del problema cuando ocurre un fraude a las cuentas del banco, una suplantación de identidad, daños de reputación, saboteo de operaciones, una extorsión o se presenta una situación de acoso o violencia sexual cibernética.

"Hay dos tipos de ataques: los que son dirigidos y cuando alguien cae en una estafa por malas prácticas de seguridad", explicó Andrés Casas, socio de servicios de ciberseguridad de Deloitte.

La mayor exposición a redes sociales e Internet hace que incluso los delincuentes comunes aprovechen los medios electrónicos para estafar personas.

En Costa Rica, de acuerdo con GoLegal, una firma local especializada en derecho digital, los delitos informáticos más comunes son la estafa informática, la suplantación de identidad, la difusión de información falsa, el espionaje informático, la suplantación de páginas electrónicas, la instalación o propagación de programas informáticos maliciosos (malware), la facilitación del delito informático, el sabotaje y el daño tecnológico y la seducción o encuentro con menores por medios electrónicos.

A nivel global las Naciones Unidas advirtieron que hay un ataque cada 39 segundos desde el inicio de la pandemia. En Estados Unidos, según el Internet Complaint Centre (IC3) del FBI, se cuadruplicaron los ciberdelitos. En América Latina se reportó un aumento de 74% de delitos cibernéticos durante la pandemia, así como más de 20,5 millones de ataques informáticos a personas usuarias en el hogar y 1,2 millones de ataques a dispositivos móviles entre enero y septiembre de 2020.

A nivel global Akamai reportó en el 2020 más de 193.519 millones de ataques, de los cuales 4.100 millones se concentraron en servicios finan-

Un informe de OEA advierte del aumento de ataques a mujeres que están incursionando en el comercio en línea.

cieros, representando un incremento del 72% respecto al 2019. Más de 10,3 millones fueron ataques a usuarios y empresas de videojuegos (ataques web y a credenciales), lo que es casi cuatro veces más.

Akamai y Deloitte coinciden en que el principal pico de ataques en el 2020 ocurrió en el segundo semes-

tre. Casas explicó que desde junio se difundió un malware llamado Emotet (creado originalmente como un troyano bancario diseñado para robar información confidencial y para fines de extorsión).

Adicionalmente se propagaron otros archivos maliciosos dedicados a descargar datos desde los dispositivos de los usuarios y compañías. La firma ESET reportó el incremento en los últimos meses de malware que explota vulnerabilidades técnicas en los sistemas, de espionaje y "mineros de criptomonedas". Estos últimos aprovechan los equipos de usuarios y empresas para procesamiento de operaciones de dinero electrónico, lo que afecta el rendimiento de servidores o computadoras.

"Lo que hemos detectado es que las empresas ya han sido atacadas y tienen actores malintencionados ya dentro de los sistemas, no los detectan y solamente cuando ocurre robo de información y datos se dan cuenta", advirtió Alonso Ramírez, miembro de la comisión de ciberseguridad del Colegio de Profesionales en Informática y Computación (CPIC) y gerente regional de ciberseguridad de GBM.

Víctimas

Los hackers aprovechan que usuarios y empresas no mantienen buenas prácticas, piensan que es suficiente con un antivirus o una muralla de fuego, no actualizan el que tienen (si usan alguno), no actualizan sistemas operativos, falta capacitación de las personas (los atacantes incursionan en los sistemas corporativos a través de los usuarios) y desconocen servicios y sistemas que pueden detectar, notificar y mitigar usos irregulares de sus equipos. Hay sectores de mayor interés para ellos.

En el sector corporativo Akamai reportó este 1° de julio de 2021 más de 47 millones de ataques, de los cuales 2 millones se dirigían contra empresas de hotelería y viajes, así como a firmas de automóviles, ventas de comercio al detalle, servicios financieros y medios de comunicación o de entretenimiento.

Casas, de Deloitte, indicó que sectores como comercio e industria también están en la mira de los hackers. En el primer caso, los hackers atacan desde los sistemas de logística y abastecimiento hasta las plataformas de comercio electrónico. En el segundo caso, atacan los sistemas y equipos informáticos integrados a la gestión de la producción.

A nivel de usuarios los ciberdelincuentes se fijan en aquellos grupos de menores habilidades y conocimientos digitales, que no cuentan con herramientas ni prácticas o hábitos de protección informática. "La mayor parte de los ataques dirigidos a la población general, tienen como objetivo a aquellas víctimas que son más susceptibles a caer en engaños", dijo Martina López, especialista en seguridad informática del Laboratorio de ESET Latinoamérica.

Los hackers tienen la capacidad para ver cuáles páginas visita el usuario en redes sociales y en la web, enfocándose en emprendedores, trabajadores y profesionales independientes, adultos mayores, mujeres (en especial jefas de hogar emprendedoras que usan las plataformas para ventas de productos de sus microempresas) y menores de edad, incluyendo adolescentes.

Un informe de Organización de Estados Americanos (OEA) confirmó que, en el caso de las mujeres, los ciberdelincuentes se centran en las que están incursionando en el comercio en línea y personal femenino de salud y de empresas para insertarse en los sistemas institucionales o corporativos. Se reporta también un incremento de la violencia de género en línea y acciones de extorsión digital utilizando imágenes íntimas, acoso sexual y explotación de mujeres, jóvenes y niñas.

Usualmente utilizan engaños para llevar a los usuarios de mayor vulnerabilidad a páginas falsas donde entreguen sus contraseñas bancarias o datos personales para utilizarlas en actividades delictivas, ya sea mediante técnicas de phishing, suplantación de identidad, páginas falsas, clonación de páginas de empresas o usuarios y anuncios fraudulentos.

ESET recordó que hay señales de comunicaciones engañosas: mensajes urgentes, ofrecimiento de productos e incluso préstamos instantáneos a precios o tasas de interés muy bajas donde piden un adelanto, solicitudes de dinero para emergencias personales y también concursos o premios falsos para solicitar datos que los bancos ya tienen y no solicitan por ningún medio.

El Financiero (Costa Rica)
10 jul. 2021 (20)