Ciberataques en Latinoamérica han aumentado un 24 % este año

Los ataques cibernéticos en Latinoamérica han aumentado un 24% en lo que va de año en comparación con los primeros 8 meses de 2020, según un informe presentado este martes, en el que se advierte de la creciente amenaza de programas maliciosos para espiar a la pareja y de «apps» de intrusión de acceso remoto.

El Panorama de Amenazas en América Latina 2021, realizado por el gigante ruso de la ciberseguridad Kaspersky y presentado este martes en una rueda de prensa virtual, indica que el vertiginoso crecimiento de los ciberataques se refleja en todos los países de la región, con la excepción de Costa Rica, que registró un leve aumento del 2%.

El repunte, que se da en medio de un auge del teletrabajo a causa de la pandemia, lo lidera Ecuador, con un alza del 75%, seguido por Perú (+71%), Panamá (+60%), Guatemala (+43%) y Venezuela (+29%), de acuerdo con el reporte basado en datos obtenidos por las soluciones de Kaspersky instaladas en usuarios de la región.

Centroamérica en la mira
El Top 20 de malware (programas maliciosos) genera un promedio de 35 ataques por segundo en la región, con Brasil a la cabeza (mil 390 intentos de infección por minuto), seguido de México (299 por minuto), Perú (96), Ecuador (89) y Colombia (87).

«Costa Rica, Guatemala y Panamá sufrieron dos explosiones de ataques, una en febrero y otra en junio. No sabemos a qué se debe, pero se detectó que los criminales están poniendo mucho interés en estos tres países», dice Dmitry Bestuzhev, director del Equipo de Investigación y Análisis de Kaspersky para América Latina.

Esto, añade el experto, muestra que el blanco de los delincuentes está cambiando a países no tan grandes en términos de cantidad de población.

Programas piratas, archivos PDF y anuncios maliciosos
El estudio subraya que el alto índice de programas piratas es un factor determinante para el cibercrimen.

En ese sentido, Bestuzhev dijo que, lamentablemente, «los internautas latinoamericanos le abren la puerta a las ciberamenazas a través de programas piratas, permitiendo que los

cibercriminales obtengan control total de los dispositivos infectados».

Para lograr la intrusión, los delincuentes también se están valiendo de archivos PDF y troyanos web (un malware que se camufla como un software legítimo) para, por ejemplo, robar datos de tarjetas de crédito.

En tanto, el «phishing» o ataque de ingeniería social (mediante mensajes de correo fraudulentos) ha disminuido, aunque varios países de la región se encuentran aún entre los más atacados del mundo por esa modalidad.

«Considerando la proporción de usuarios atacados durante los primeros ocho meses del año, Brasil figura en el primer lugar con 15,37% de usuarios que registraron algún intento de ataque. Le sigue Ecuador (13,36%), Panamá (12,60%), Chile (11,90%) y Colombia (11,09%)», sostiene el informe.

En contraste, Venezuela (7,19%) y la República Dominicana (5,62 %) figuran entre las naciones con la menor cantidad de ataques de ingeniería social a nivel mundial.

Móviles, troyanos y espionaje a las mujeres
Kaspersky detectó más de 173 mil intentos de infección a dispositivos móviles entre enero y agosto de este año en la región- un promedio de casi 20 ataques por hora-, contando como una de las principales amenazas los troyanos.

Entre ellos, la firma alertó de los programas espías comerciales conocidos como «stalkerware».

«Estos son creados por empresas verdaderas que hacen pasar el software como programas para monitorear las actividades en línea de niños o empleados, pero su objetivo real es espiar a cónyuges y parejas, principalmente a las mujeres», resaltó Bestuzhev, al recordar que la mayor cantidad víctimas en estos casos están en Brasil, México y Perú.

Finalmente, el analista Fabio Assolini apuntó los riesgos del ataque «de la mano fantasma», en la que el ciberdelincuente entra a un dispositivo móvil mediante un engaño, haciendo que el usuario dé clic y descargue un archivo malicioso de una web.

«Esa intrusión le permite acceder al dispositivo de manera remota, abrir aplicaciones financieras instaladas y hacer transacciones de manera sigilosa, incluso cuando el móvil parece que está apagado», añadió.

Con información de EFE