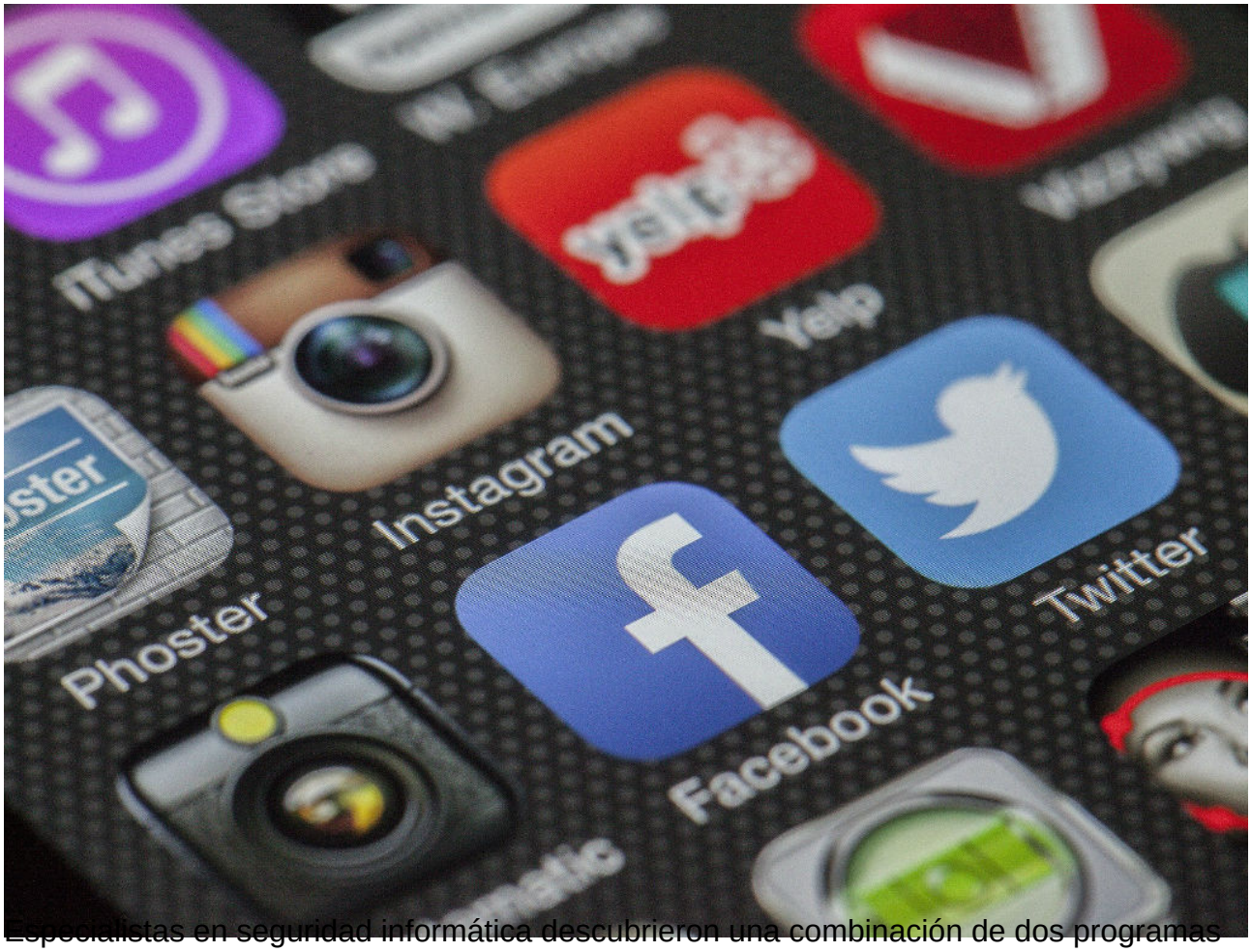
Alerta en Android: atacantes logran controlar las redes sociales de sus víctimas



Especialistas en seguridad informática descubrieron una combinación de dos programas maliciosos que comprometen las redes sociales de las víctimas, en equipos con **Android**. En conjunto, estos *malwares* consiguen acceso a las *cookies* que recolectan el navegador y algunas apps, para luego controlar perfiles.

En concreto, mediante esta práctica (la revisión de los hábitos de los usuarios) los piratas informáticos pueden **publicar contenido en las redes sociales de terceros**.

Leé tambiénBlueFrag, la falla en Android que permite enviar malware vía Bluetooth

Tal como nota *TechRadar* en su repaso, las *cookies* pueden resultar beneficiosas para la experiencia de uso (se trata de datos que recopilan las herramientas digitales y que, por ejemplo, sirven para crear atajos y un uso más personalizado de los *softwares*), aunque en manos equivocadas suponen un riesgo en términos de seguridad.

Los detalles de la vulnerabilidad

Para esta estafa se emplean dos programas maliciosos: uno que logra accesos para transferir *cookies*, y otro que engaña a los sistemas de seguridad. En específico, se "enmascara" de un acceso local para que los sistemas no sospechen que se trata de un engaño por el hecho de intentar accesos simultáneos desde zonas geográficas muy alejadas entre sí: para eso, hace funcionar un servidor proxy en el dispositivo de la víctima.

Al parecer, el objetivo de los atacantes es distribuir **spam en redes sociales y servicios de mensajería**, así como emprender campañas de *phishing*.

"Aunque esta es una amenaza relativamente nueva (hasta ahora solo han sido atacadas unas 1.000 personas), la cifra está creciendo y probablemente continuará haciéndolo, especialmente porque es muy difícil de detectar por los sitios web", señaló un representante de la firma Kaspersky, responsable del hallazgo.

Y agregó: "Aun cuando normalmente no prestamos atención a las *cookies* al navegar por la web, siguen siendo otro medio de procesar nuestra información personal, y cada vez que esa información sobre nosotros es recopilada en línea debemos prestar atención".

Según los especialistas, para evitar este tipo de estafas hay que bloquear el acceso de terceros a las *cookies* en el *browser*, eliminar ese contenido en forma periódica, y en

ocasiones usar la navegación privada que no recopilar esa información.

Fuente: TN