Aplicaciones de espionaje para Android: una amenaza cada vez más peligrosa

El equipo de investigación de ESET reveló que muchas aplicaciones de stalkerware para Android están plagadas de vulnerabilidades que ponen más en peligro a las víctimas y exponen la privacidad y seguridad de las propias personas que espían.

Buenos Aires, Argentina – El stalkerware para dispositivos móviles, también conocido en inglés como spouseware, es un software para monitorear que un acosador instala silenciosamente en el dispositivo de una víctima sin que la víctima lo sepa. ESET, compañía líder en detección proactiva de amenazas, revela que muchas aplicaciones de este tipo contienen vulnerabilidades que exponen la privacidad y seguridad de quienes son espiados y también de quienes espían.

Según la telemetría de ESET, las aplicaciones de stalkerware se volvieron cada vez más populares en los últimos años. **En 2019, vimos que las detecciones de stalkerware para Android aumentaron casi cinco veces con respecto a 2018, y este crecimiento en 2020 fue de 48% en comparación con 2019.** El stalkerware puede monitorear la ubicación GPS del dispositivo de una víctima, las conversaciones, imágenes, historial del navegador y más. También almacena y transmite todos estos datos.

"Como mínimo, las aplicaciones de stalkerware promueven un comportamiento cuestionable desde el punto de vista ético, lo que lleva a la mayoría de las soluciones de seguridad para móviles a señalar a estas aplicaciones como indeseables o dañinas. Sin embargo, dado que estas apps acceden, recopilan, almacenan y transmiten más información que cualquier otra aplicación que hayan instalado sus víctimas, nos interesaba saber qué tan bien estas aplicaciones protegían semejante cantidad de datos y tan sensibles.", comenta Lukas Stefanko, especialista de ESET.

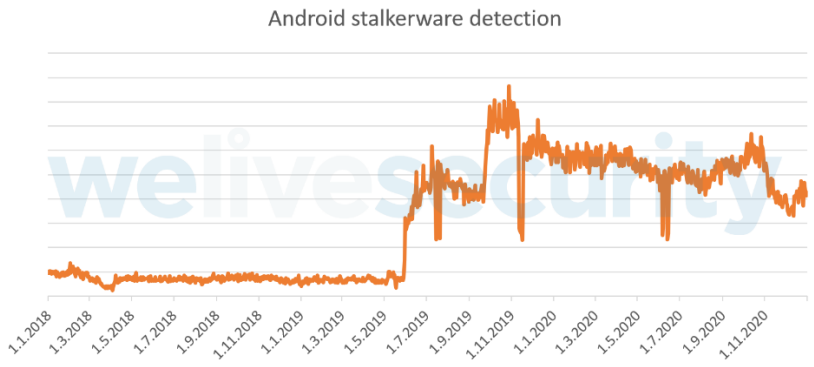

Figura 1. Según la telemetría de detección de ESET el uso de stalkerware en Android está aumentando

Por lo general, se necesita tener acceso físico al dispositivo de la víctima para realizar la instalación. Debido a esto, los acosadores suelen ser personas de los círculos familiares, sociales o laborales cercanos de sus víctimas. Para evitar ser identificados como stalkerware y permanecer fuera del radar, los proveedores de estas aplicaciones suelen catalogarlas como una protección para niños, empleados o mujeres, sin embargo, la palabra "espía" también se utiliza muchas veces en los sitios web.

Desde ESET se analizaron manualmente 86 aplicaciones de stalkerware para la plataforma Android, proporcionadas por 86 proveedores diferentes. **En 58 de estas aplicaciones para Android ESET descubrió un total de 158 problemas de seguridad y privacidad que pueden tener un impacto grave en una víctima; y, de hecho, incluso el acosador o el proveedor de la aplicación pueden correr algún riesgo.** ESET identificó problemas graves de seguridad y privacidad que podrían resultar en que un atacante tomara el control del dispositivo de una víctima y de la cuenta de la herramienta de stalkerware, interceptara los datos de la víctima, pudiendo incriminar a la víctima cargando pruebas falsas, o que lograra ejecutar código de manera remota en el teléfono de la víctima.

En este sentido, un atacante puede llevar a cabo acciones como aprovecharse de problemas de seguridad o fallas de privacidad en la aplicación de stalkerware o en los servicios de monitoreo asociados.

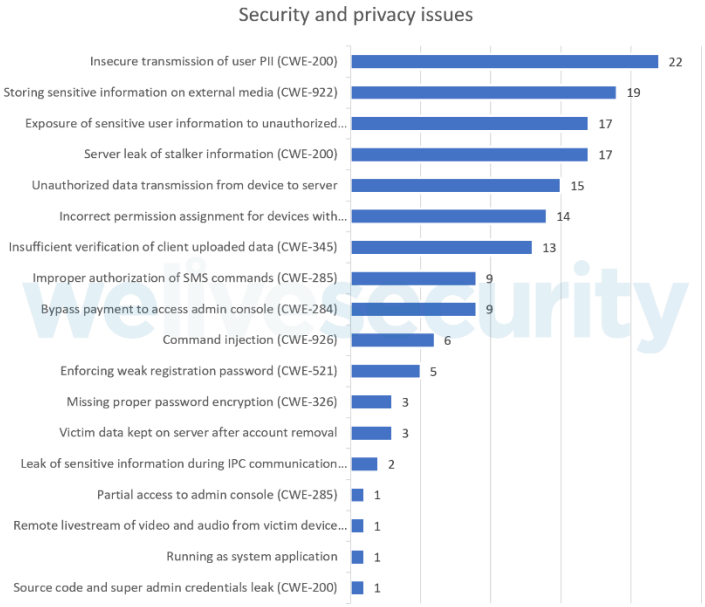

Figura 2. Desglose de los problemas de seguridad y privacidad descubiertos en la investigación de ESET.

"Esta investigación debe servir como una advertencia para los potenciales clientes de este tipo de apps para que reconsideren el uso de estos softwares para espiar a sus cónyuges y seres queridos, ya que no solo es poco ético hacer eso, sino que también puede derivar en la exposición de información privada e íntima y ponerlos en riesgo a posibles ciberataques y fraudes, tanto a quien es espiado como a quién espía. Identificamos que algunos de estos stalkerware guardan en un servidor datos de los acosadores que usan la aplicación y los datos que obtuvieron de sus víctimas, incluso después de que los acosadores solicitaron la eliminación de los datos.", menciona Stefanko de ESET.

Siguiendo con su política de divulgación coordinada de 90 días, desde ESET se informó en reiteradas ocasiones de estos problemas a los proveedores afectados. Desafortunadamente, al momento, solo seis proveedores han solucionado los problemas informados. Cuarenta y cuatro proveedores no respondieron y siete prometieron solucionar sus problemas en una próxima actualización. Además, un proveedor decidió no solucionar los problemas informados.

Para acceder al informe completo, ingrese a: **Vulnerabilidades en aplicaciones de stalkerware para Android**

Para conocer más sobre seguridad informática ingrese al portal de noticias de ESET: https://www.welivesecurity.com/la-es/2021/05/17/stalkerware-para-android-fallas-seguridad-exponen-propios-espias/

Visítanos en: @ESETLA /company/eset-latinoamerica

Acerca de ESET
Desde 1987, ESET® desarrolla soluciones de seguridad que ayudan a más de 100 millones de usuarios a disfrutar la tecnología de forma segura. Su portfolio de soluciones ofrece a las empresas y consumidores de todo el mundo un equilibrio perfecto entre rendimiento y protección proactiva. La empresa cuenta con una red global de ventas que abarca 180 países y tiene oficinas en Bratislava, San Diego, Singapur, Buenos Aires, México DF y San Pablo.

Datos de Contacto de Comunicación y Prensa
Para más información se puede poner en contacto a través de ***prensa@eset-la.com*** *o al +54 11 2150-3700.*
Además, puede visitar "Somos ESET" nuestro Blog de Comunicación de ESET con las últimas novedades, disponible en: https://www.somoseset.com/