Una serie de vulnerabilidades de día cero que fueron abordadas el año pasado, fueron explotadas por proveedores comerciales de software espía para apuntar a dispositivos Android e iOS, según reveló el Grupo de Análisis de Amenazas de Google (TAG).

Las dos campañas distintas fueron limitadas y altamente dirigidas, aprovechando la brecha de parches entre el lanzamiento de una corrección y cuando realmente se implementó en los dispositivos objetivo.

> *«Estos proveedores están permitiendo la proliferación de herramientas de hacking peligrosas, armando a los gobiernos que no podrían desarrollar estas capacidades internamente»,* dijo Clement Lecigne de TAG.

> *«Aunque el uso de tecnologías de vigilancia puede ser legal según las leyes nacionales o internacionales, por lo general los gobiernos las utilizan para atacar a disidentes, periodistas, trabajadores de derechos humanos y políticos de partidos de oposición».*

La primera de las dos operaciones tuvo lugar en noviembre de 2022 e implicó el envío de enlaces acortados por medio de mensajes SMS a usuarios ubicados en Italia, Malasia y Kazajstán.

Al hacer clic, las URL redirigían a los destinatarios a páginas web que albergaban exploits para Android o iOS, antes de ser redirigidos nuevamente a sitios web legítimos de noticias o seguimiento de envíos.

La cadena de exploits de iOS aprovechó varios errores, incluyendo CVE-2022-42856 (entonces día cero), CVE-2021-30900 y una omisión del código de autenticación de puntero (PAC), para instalar un archivo .IPA en el dispositivo susceptible.

La cadena de exploits de Android constaba de tres exploits: CVE-2022-3723, CVE-2022-4135 y CVE-2022-38181, para entregar una carga útil no especificada.

Aunque CVE-2022-38181, una vulnerabilidad de escalada de privilegios que afectaba al controlador del núcleo de la GPU de Mali, fue parcheado por Arm en agosto de 2022, no se sabe si el atacante ya estaba en posesión de un exploit por la falla antes del lanzamiento del parche.

Otro punto a tener en cuenta es que los usuarios de Android que hicieron clic en el enlace y lo abrieron en el navegador de Internet de Samsung fueron redirigidos a Chrome usando un método llamado redirección de intención.

La segunda campaña, observada en diciembre de 2022, consistió en varios días cero y días n dirigidos a la última versión del navegador de Internet de Samsung, con los exploits entregados como enlaces únicos por medio de SMS a dispositivos ubicados en los Emiratos Árabes Unidos.

La página web, similar a las que utilizó la empresa española de spyware Variston IT, finalmente implantó un conjunto de herramientas maliciosas basado en C++ capaz de recopilar datos de las aplicaciones de chat y navegador.

Las vulnerabilidades explotadas constituyen CVE-2022-4262, CVE-2022-3038, CVE-2022-22706, CVE-2023-0266 y CVE-2023-26083. Se cree que la cadena de explotación fue usada por un cliente o socio de Variston IT.

Las revelaciones se producen pocos días después de que el gobierno de Estados Unidos anunciara una orden ejecutiva que restringe a las agencias federales el uso de software espía comercial que presenta un riesgo para la seguridad nacional.

> *«Estas campañas son un recordatorio de que la industria del spyware comercial sigue prosperando. Incluso los proveedores de vigilancia más pequeños tienen*

> *acceso a los días cero, y los proveedores que almacenan y usan vulnerabilidades de día cero en secreto representan un grave riesgo para Internet»,* dijo Lecigne.

> *«Estas campañas también pueden indicar que los proveedores de vigilancia comparten exploits y técnicas, lo que permite la proliferación de herramientas de hacking peligrosas».*