El Grupo de Análisis de Amenazas (TAG) de Google, señaló el jueves a un desarrollador de spyware de Macedonia del Norte llamado Cytrox, por desarrollar exploits contra 5 vulnerabilidades de día cero, cuatro en Chrome y una en Android, para apuntar a los usuarios de Android.

> *«Los exploits de día cero se utilizaron junto con los de día n, ya que los desarrolladores aprovecharon la diferencia de tiempo entre el momento en que se parchearon algunos errores críticos pero no se marcaron como problemas de seguridad, y estos parches se implementaron por completo en el ecosistema de Android»,* dijeron los investigadores de TAG, Clement Lecigne y Christian Resell.

Se dice que Cytrox empaquetó los exploits y los vendió a distintos actores respaldados por el gobierno, ubicados en Egipto, Armenia, Grecia, Madagascar, Costa de Marfil, Serbia, España e Indonesia, quienes a su vez, armaron los errores en al menos tres campañas distintas.

La compañía de vigilancia comercial es el fabricante de Predator, un implante análogo al de Pegasus de NSO Group, y se sabe que ha desarrollado herramientas que permiten a sus clientes acceder a los dispositivos iOS y Android.

En diciembre de 2021, Meta Platforms reveló que había actuado para eliminar aproximadamente 300 cuentas en Facebook e Instagram, que la compañía usaba como parte de sus campañas de compromiso.

Las cinco vulnerabilidades de día cero explotadas en Chrome y Android son.

- CVE-2021-37973: Use-after-free en la API de portales
- CVE-2021-37976: Fuga de información en el núcleo
- CVE-2021-38000: Validación insuficiente de entrada no confiable en Intentos (análisis de causa raíz)
- CVE-2021-38003: Implementación inapropiada en V8
- CVE-2021-1048: Use-after-free en el kernel de Android (análisis de causa raíz)

Según TAG, las tres campañas en cuestión comenzaron con un correo electrónico de phishing selectivo que contenía enlaces de un solo uso, que imitaban los servicios de acortadores de URL que, una vez que se hacía clic, redirigían a los objetivos a un dominio falso que eliminó las vulnerabilidades antes de llevar a la víctima a un sitio auténtico.

> *«Las campañas fueron limitadas, en cada caso, evaluamos que la cantidad de objetivos era de decenas de usuarios. Si el enlace no estaba activo, el usuario era redirigido directamente a un sitio web legítimo»,* dijeron Lecigne y Resell.

El objetivo final de la operación, según los investigadores, era distribuir un malware llamado Alien, que actúa como un precursor para cargar Predator en dispositivos Android infectados.

El malware *«simple»,* que recibe comandos de Predator a través de un mecanismo de comunicación entre procesos (IPC), está diseñado para grabar audio, agregar certificados de CA y ocultar aplicaciones para evadir la detección.

La primera de las tres campañas tuvo lugar en agosto de 2021. Usó Google Chrome como punto de partida en un dispositivo Samsung Galaxy S21 para obligar al navegador web a cargar otra URL en el navegador de Internet de Samsung sin necesidad de la interacción del usuario mediante la explotación de CVE-2021-38000.

Otra intrusión, que ocurrió un mes después y se entregó a un Samsung Galaxy S10 actualizado, involucró una cadena de exploits que usaba CVE-2021-37973 y CVE-2021-37976 para escapar del sandbox de Chrome, aprovechándolo para eliminar un segundo exploit para escalar privilegios e implementar la backdoor.

La tercera campaña, un exploit de día cero completo de Android, se detectó en octubre de 2021 en un teléfono Samsung actualizado que ejecutaba la última versión de Chrome. Enlazó dos vulnerabilidades, CVE-2021-38003 y CVE-2021-1048, para escapar de la zona de pruebas y comprometer el sistema al inyectar código malicioso en procesos privilegiados.

Google TAG dijo que, si bien CVE-2021-1048 se solucionó en el kernel de Linux en septiembre de 2020, no se reportó a Android hasta el año pasado, ya que la solución no se marcó como un problema de seguridad.

> *«Los atacantes buscan activamente y se benefician de vulnerabilidades que se solucionan lentamente»,* dijeron los investigadores.

> *«Hacer frente a las prácticas nocivas de la industria de la vigilancia comercial requerirá un enfoque sólido e integral que incluya la cooperación entre los equipos de inteligencia de amenazas, los defensores de la red, los investigadores académicos y las plataformas tecnológicas».*