Investigadores de seguridad detectaron las aplicaciones para Android Camero, FileCrypt y CallCam, como maliciosas y se cree que están vinculadas a Sidewinder APT, un sofisticado grupo de piratería especializado en ataques de espionaje cibernético.

Según los investigadores de Trend Micro, estas aplicaciones estaban explotando una vulnerabilidad crítica de uso libre después de Android al menos desde marzo del año pasado, lo que significa que funcionan desde 7 meses antes de que se descubriera la misma vulnerabilidad de día cero cuando un investigador de Google analizó un ataque separado desarrollado por el proveedor israelí de vigilancia, NSO Group.

> *«Especulamos que estas aplicaciones han estado activas desde marzo de 2019 en función de la información del certificado en una de las aplicaciones»,* dijeron los investigadores.

Rastreada como CVE-2019-2215, la vulnerabilidad es un problema de escalada de privilegios locales que permite el compromiso total de la raíz de un dispositivo vulnerable, y también podría explotarse remotamente al combinarse con un defecto de representación del navegador separado.

Según Trend Micro, FileCrypt Manager y Camero actúan como cuentagotas y se conectan a un servidor de comando y control remoto para descargar un archivo DEX, que luego descarga la aplicación callCam e intenta instalarla aprovechando las vulnerabilidades de escalada de privilegios o abusando de la función de accesibilidad.

> *«Todo esto se realiza sin la conciencia o intervención del usuario. Para evadir la detección, utiliza muchas técnicas como la ofuscación, el cifrado de datos y la invocación de código dinámico»,* dijeron los investigadores.

Una vez instalada, CallCam oculta su ícono del menú, recopila información del dispositivo

comprometido y la envía al servidor de C&C del atacante en segundo plano. Entre la información recopilada se encuentra:

- Ubicación
- Estado de la batería
- Archivos en el dispositivo
- Lista de aplicaciones instaladas
- Información del dispositivo
- Información del sensor
- Información de la cámara
- Captura de pantalla
- Cuenta
- Información de WiFi
- Datos de WeChat, Outlook, Twitter, Yahoo Mail, Facebook, Gmail y Chrome

Además de la vulnerabilidad CVE-2019-2215, las aplicaciones maliciosas también intentan aprovechar una vulnerabilidad separada en el controlador MediaTek-SU para obtener privilegios de root y permanecer persistente en una amplia gama de teléfonos Android.

Sobre la base de la superposición en la ubicación de los sensores de comando y control, los investigadores atribuyeron la campaña a SideWinder, que se cree que es un grupo de espionaje indio que históricamente apuntó a organizaciones vinculadas con el ejército paquistaní.

Google ya se encargó de eliminar todas las aplicaciones maliciosas mencionadas de Play Store, pero debido a que los sistemas de Google no son suficientes para mantener las aplicaciones maliciosas fuera de la tienda oficial, se debe tener mucho cuidado al descargar apps.

Para verificar si tu dispositivo está infectado con el malware, puedes acceder a la configuración del sistema, en el administrador de aplicaciones buscar los nombres de paquete enumerados y desinstalarlos.