Investigadores de seguridad cibernética revelaron una nueva familia de malware de Android que abusa de los servicios de accesibilidad en el dispositivo para secuestrar las credenciales del usuario y grabar audio y video.

Nombrado como Oscorp por el CERT-AGID de Italia y detectado por AddressIntel, el malware *«induce al usuario a instalar un servicio de accesibilidad con el que los atacante pueden leer lo que está presente y lo que se escribe en la pantalla».*

Llamado así por el título de la página de inicio de sesión de su servidor de comando y control (C2), el APK malicioso (llamado «*Assistenzaclienti.apk*» o «*Protección del cliente*«) se distribuye a través de un dominio llamado «*supportoapp[.]com*«, que *«tras la instalación, solicita permisos intrusivos para habilitar el servicio de accesibilidad y establece comunicaciones con un servidor C2 para recuperar comandos adicionales».*

Además, el malware vuelve a abrir repetidamente la pantalla Configuración cada ocho segundos hasta que el usuario activa los permisos para la accesibilidad y las estadísticas de uso del dispositivo, lo que presiona al usuario para que otorgue privilegios adicionales.

Una vez que se proporciona el acceso, el malware explota los permisos para registrar pulsaciones de teclas, desinstalar aplicaciones en el dispositivo, realizar llamadas, enviar mensajes SMS, robar criptomonedas al redirigir los pagos realizados a través de la aplicación Blockchain.com Wallet y acceder a códigos de autenticación de dos factores de Google.

La billetera controlada por el atacante tenía $584 dólares el 9 de enero, según los investigadores.

En el último paso, el malware extrae los datos capturados, junto con la información del sistema, como aplicaciones instaladas, modelo del teléfono, operador, entre otros, al servidor C2 y además obtiene comandos del servidor que le permiten iniciar la aplicación Google Authenticator, robar mensajes SMS, desinstalar aplicaciones, iniciar URL específicas y grabar audio y video de la pantalla por medio de WebRTC.

Además, a los usuarios que abren las aplicaciones objetivo del malware, se les muestra una página de phishing que solicita su nombre de usuario y contraseña, dijo CERT, agregando que el estilo de la pantalla varía de una aplicación a otra y que está diseñada con la intención de engañar a la víctima para proporcionar la información.

Aún no está claro el tipo exacto de aplicaciones señaladas por el malware, pero los investigadores afirmaron que podría ser cualquier app que trate con datos confidenciales, como bancarias y de mensajería.

> *«Las protecciones de Android evitan que el malware cause algún tipo de daño hasta que el usuario habilite el servicio de accesibilidad. Una vez habilitado, sin embargo, se abre una 'represa'. De hecho, Android siempre ha tenido una política muy permisiva hacia los desarrolladores de aplicaciones, dejando la decisión final de confiar o no en una aplicación al usuario final»,* dijo el CERT-AGID.