Un malware de Android que se observó abusando de los servicios de accesibilidad en dispositivos para secuestrar las credenciales de usuario de las aplicaciones bancarias europeas, se ha transformado en una botnet completamente nueva como parte de una campaña renovada que comenzó en mayo de 2021.

El CERT-AGID de Italia, a finales de enero, reveló detalles sobre Oscorp, un malware móvil desarrollado para atacar múltiples objetivos financieros con el objetivo de robar fondos de víctimas desprevenidas.

Sus características incluyen la capacidad de interceptar mensajes SMS y realizar llamadas telefónicas, y realzar ataques de superposición para más de 150 aplicaciones móviles mediante el uso de pantallas de inicio de sesión similares para desviar datos valiosos.

El malware se distribuyó por medio de mensajes SMS maliciosos, y los ataques por lo general se realizaban en tiempo real haciéndose pasar por operadores bancarios para engañar a los objetivos por teléfono y obtener acceso subrepticiamente al dispositivo infectado por medio del protocolo WebRTC y, finalmente, realizar transferencias bancarias no autorizadas.

Aunque no se informaron nuevas actividades desde entonces, parece que Oscorp pudo haber realizado un regreso luego de una pausa temporal en la forma de una botnet de Android conocida como UBEL.

> *«Al analizar algunas muestras relacionadas, encontramos varios indicadores que vinculan a Oscorp y UBEL con la misma base de código malicioso, lo que sugiere una bifurcación del mismo proyecto original o simplemente un cambio de marca por parte de otros afiliados, ya que su código fuente parece ser compartido entre múltiples actores»,* dijo Cleafy.

Anunciado en foros clandestinos por 980 dólares, UBEL solicita permisos intrusivos que permiten leer y enviar mensajes SMS, grabar audio, instalar y eliminar aplicaciones, iniciarse automáticamente luego del inicio del sistema y abusar de los servicios de accesibilidad en

Android para acumular información confidencial del dispositivo, como credenciales de inicio de sesión y códigos de autenticación de dos factores, cuyos resultados se exfiltran a un servidor remoto.

Una vez descargado en el dispositivo, el malware intenta instalarse como un servicio y ocultar su presencia al objetivo, logrando de este modo la persistencia durante largos períodos de tiempo.

El uso de WebRTC para interactuar con el teléfono Android comprometido en tiempo real, evita la necesidad de inscribir un nuevo dispositivo y hacerse cargo de una cuenta para realizar actividades fraudulentas.

> *«El objetivo principal de este actor de amenazas al utilizar esta función es evitar una inscripción de un nuevo dispositivo, lo que reduce drásticamente la posibilidad de ser marcado como sospechoso, ya que los indicadores de huellas dactilares del dispositivo son bien reconocidos desde la perspectiva del banco»,* dijeron los investigadores.

La distribución geográfica de los bancos y otras aplicaciones a las que apunta Oscorp se compone de España, Polonia, Alemania, Turquía, Estados Unidos, Italia, Japón, Australia, Francia e India, entre otros.