El troyano bancario SOVA para Android sigue desarrollándose activamente con capacidades mejoradas para apuntar a no menos de 200 aplicaciones móviles, incluyendo aplicaciones bancarias y criptobolsas y billeteras frente a las 90 aplicaciones cuando comenzó.

Estos hallazgos fueron informados por la compañía italiana de seguridad cibernética Cleafy, que encontró versiones más nuevas de la funcionalidad deportiva de malware para interceptar códigos de autenticación de dos factores (2FA), robar cookies y expandir su objetivo para cubrir Australia, Brasil, China, India, Filipinas y el Reino Unido.

SOVA, que significa Búho en ruso, salió a la luz en septiembre de 2021 cuando se observaron aplicaciones financieras y de compras sorprendentes de Estados Unidos y España para recolectar credenciales por medio de ataques de superposición aprovechando los servicios de accesibilidad de Android.

En menos de un año, el troyano también actuó como base para otro malware de Android llamado MaliBot, que está diseñado para apuntar a clientes de banca en línea y billeteras de criptomonedas en España e Italia.

La última variante de SOVA, denominada v4 por Cleafy, se oculta dentro de aplicaciones falsas que presentan logotipos de aplicaciones legítimas como Amazon y Google Chrome, con el fin de engañar a los usuarios para que las instalen. Otras mejoras notables incluyen la captura de pantalla y la grabación de las pantallas del dispositivo.

> *«Estas características, combinadas con los servicios de accesibilidad, permiten realizar gestos, y en consecuencia, actividades fraudulentas desde el dispositivo infectado, como ya hemos visto en otros troyanos bancarios de Android (por ejemplo, Oscorp o BRATA)»,* dijeron los investigadores de Cleafy, Francesco Lubatti y Federico Valentini.

SOVA v4 también se destaca por su esfuerzo para recopilar información confidencial de Binance y Trust Wallet, como saldos de cuentas y frases iniciales. Además, las 13

aplicaciones bancarias rusas y ucranianas que fueron atacadas por el malware se eliminaron de la versión.

Aparte de esto, la actualización permite que el malware aproveche sus amplios permisos para desviar los intentos de desinstalación al redirigir a la víctima a la pantalla de inicio y mostrar el mensaje *«Esta aplicación está protegida».*

También se espera que el troyano bancario, a pesar de su gran cantidad de funciones, incorpore un componente de ransomware en la próxima iteración, que actualmente se encuentra en desarrollo y tiene como objetivo cifrar todos los archivos almacenados en el dispositivo infectado usando AES y renombrarlos con la extensión «.enc».

También es probable que la mejora haga de SOVA una amenaza formidable en el panorama de amenazas móviles.

> *«La función de ransomware es bastante interesante, ya que aún no es común en el panorama de los troyanos bancarios de Android. Aprovecha fuertemente la oportunidad que ha surgido en los últimos años, ya que los dispositivos móviles se convirtieron para la mayoría de las personas en el almacenamiento central de datos personales y comerciales»,* dijeron los investigadores.