Varias aplicaciones de Android no autorizadas que se han instalado acumulativamente desde la tienda oficial de Google Play más de 50,000 veces se utilizan para apuntar a bancos y otras entidades financieras.

El troyano bancario de alquiler, denominado Octo, es un cambio de marca de otro malware de Android llamado ExobotCompacto, que a su vez, es un reemplazo *«ligero»* de su predecesor Exobot, según dijo la empresa holandesa de seguridad móvil, ThreatFabric.

Es probable que también Exobot allanó el camino para un descendiente separado llamado Coper, que se descubrió inicialmente dirigido a usuarios colombianos alrededor de julio de 2021, con infecciones más nuevas dirigidas a usuarios de Android en distintos países europeos.

> *«Las aplicaciones de malware de Coper tienen un diseño modular e incluyen un método de infección de múltiples etapas y muchas tácticas defensivas para sobrevivir a los intentos de eliminación»,* dijo la compañía de ciberseguridad Cyble.

Al igual que otros troyanos bancarios de Android, las aplicaciones no autorizadas no son más que cuentagotas, cuya función principal es desplegar la carga maliciosa incrustada en ellas. La lista de cuentagotas Octo y Coper utilizados por múltiples actores de amenazas se encuentra a continuación:

- Creador de pantalla de bolsillo (com.moh.screen)
- Limpiador rápido 2021 (vizeeva.fast.cleaner)
- Tienda de juegos (com.restthe71)
- Seguridad del banco postal (com.carbuildz)
- Creador de pantalla de bolsillo (com.cutthousandjs)
- BAWAG PSK Security (com.frontwonder2)
- Instalación de la aplicación Play Store (com.theseeye5)

Estas aplicaciones, que se hacen pasar por el instalador de aplicaciones PlayStore, grabación

de pantalla y aplicaciones financieras, están *«impulsadas por esquemas de distribución de incentivos»,* que se distribuyen a través de la tienda Google Play por medio de páginas de destino fraudulentas que supuestamente alertan a los usuarios para que descarguen una actualización del navegador.

Los goteros, una vez instalados, actúan como un conducto para lanzar los troyanos, no sin antes solicitar a los usuarios que habiliten los Servicios de Accesibilidad que permiten una amplia gama de filtrar información confidencial de los teléfonos comprometidos.

Octo, la versión revisada de ExobotCompact, también está equipada para realizar fraudes en el dispositivo al obtener el control remoto de los dispositivos aprovechando los permisos de accesibilidad, así como la API Media Projection de Android para capturar el contenido de la pantalla en tiempo real.

El objetivo final, según ThreatFabric, es activar el *«inicio automático de transacciones fraudulentas y su autorización sin esfuerzos manuales por parte del operador, lo que permite el fraude a una escala significativamente mayor».*

Otras características notables de Octo incluyen el registro de pulsaciones de teclas, la realización de ataques de superposición en aplicaciones bancarias para capturar credenciales, la recopilación de información de contacto y medidas de persistencia para evitar la desinstalación y evadir los motores antivirus.

> *«El cambio de marca a Octo borra los vínculos anteriores con la filtración del código fuente de Exobot, invitando a múltiples actores de amenazas que buscan la oportunidad de alquilar un troyano supuestamente nuevo y original»,* dijo ThreatFabric.

> *«Sus capacidades ponen en riesgo no solo las aplicaciones dirigidas explícitamente que son objeto de un ataque de superposición, sino que cualquier aplicación instalada en el dispositivo infectado, como ExobotCompact/Octo, puede leer el contenido de cualquier aplicación que se muestra en la pantalla y proporcionar al actor información suficiente para interactuar de forma remota con él y realizar fraude en el dispositivo (ODF)»*, agregó.

Los hallazgos llegan poco después del descubrimiento de un robot bancario de Android distinto llamado GodFather, que comparte superposiciones con los troyanos bancarios Cerberus y Medusa, que se ha observado apuntando a usuarios bancarios en Europa bajo la apariencia de la aplicación Configuración predeterminada para transferir fondos y robar mensajes SMS, entre otros.

Además, un nuevo análisis publicado por AppCensus, encontró 11 aplicaciones con más de 46 millones de instalaciones que se implantaron con un SDK de terceros llamado Coelib, que hizo posible capturar contenido del portapapeles, datos de GPS, direcciones de correo electrónico, números de teléfono e incluso la dirección MAC del enrutador del módem del usuario y el SSID de la red.