Se ha observado un nuevo troyano bancario para Android con más de 50 mil instalaciones, distribuido a través de la tienda oficial de Google Play con el objetivo de apuntar a 56 bancos europeos y llevar a cabo la recopilación de información confidencial de los dispositivos comprometidos.

Apodado como Xenomorph por la compañía de seguridad holandesa ThreatFabric, se dice que el malware en desarrollo comparte superposiciones con otro troyano bancario rastreado bajo el nombre de Alien, y al mismo tiempo, es *«radicalmente diferente»* de su predecesor en términos de las funcionalidades que ofrece.

> *«A pesar de ser un trabajo en progreso, Xenomorph ya luce superposiciones efectivas y se distribuye activamente en las tiendas de aplicaciones oficiales. Además, cuenta con un motor modular muy detallado para abusar de los servicios de accesibilidad, que en el futuro podría potenciar capacidades muy avanzadas, como ATS»,* dijo el fundador y director ejecutivo de ThreatFabric, Han Sahin.

Alien, un troyano de acceso remoto (RAT) con detección de notificaciones y funciones de robo 2FA basadas en autenticadores, surgió poco después de la desaparición del malware Cerberus en agosto de 2020. Desde entonces, se han detectado otras bifurcaciones de Cerberus, incluyendo ERMAC en septiembre de 2021.

Xenomorph, como Alien y ERMAC, es otro ejemplo más de un troyano bancario para Android que se enfoca en eludir las protecciones de seguridad de Google Play Store, haciéndose pasar por aplicaciones de productividad como *«Fast Cleaner»* para engañar a las víctimas desprevenidas para que instalen el malware.

Cabe mencionar que una aplicación cuentagotas de entrenamiento físico con más de 10 mil instalaciones, denominada GymDrop, se encontró entregando la carga útil del troyano bancario Alien en noviembre al enmascararlo como *«un nuevo paquete de ejercicios de entrenamiento».*

Fast Cleaner, que tiene el nombre de paquete *«vizeeva.fast.cleaner»* y sigue disponible en la tienda de aplicaciones, ha sido más popular en Portugal y España, según revelan los datos de la firma de inteligencia de mercado de aplicaciones móviles Sensor Tower, con la aplicación haciendo su primera aparición en Play Store a fines de enero de 2022.

Además, las reseñas de la aplicación por parte de los usuarios incluyen advertencias de que *«esta aplicación tiene malware y solicita una actualización que se confirme continuamente».*

Otro usuario dijo: *«Mete malware en el dispositivo y aparte tiene un sistema de autoprotección para que no lo puedas desinstalar».*

Xenomorph también utiliza la táctica comprobada de pedir a las víctimas que le otorguen privilegios del servicio de Accesibilidad y abusen de los permisos para realizar ataques superpuestos, en los que el malware inyecta pantallas de inicio de sesión no autorizadas sobre aplicaciones específicas de España, Portugal, Italia y Bélgica, para desviar credenciales y otra información personal.

Además, está equipado con una función de interceptación de notificaciones para extraer tokens de autenticación de dos factores recibidos a través de SMS y obtener la lista de aplicaciones instaladas, cuyos resultados se filtran a un servidor remoto de comando y control.

> *«La aparición de Xenomorph muestra, una vez más, que los actores de amenazas están centrando su atención en las aplicaciones de aterrizaje en los mercados oficiales. El malware de la banca moderna está evolucionando a un ritmo muy rápido y los delincuentes están comenzando a adoptar prácticas de desarrollo más refinadas para respaldar futuras actualizaciones»,* dijeron los investigadores.