Una nueva variante del troyano bancario para Android, llamado Xenomorph, apareció en estado salvaje, según revelan los últimos hallazgos de ThreatFabric.

Nombrada como Xenomorph 3rd generation, por Hadoken Security Group, el grupo de hackers detrás de la operación, la versión ecualizada cuenta con nuevas características que permiten realizar fraudes financieros de forma transparente.

> *«Esta nueva versión del malware agrega muchas capacidades nuevas a un banco de Android ya rico en funciones, sobre todo la introducción de un motor de tiempo de ejecución muy extenso impulsado por los servicios de accesibilidad, que los hackers usan para implementar un marco ATS completo»*, dijo la compañía de seguridad cibernética holandesa.

Xenomorph salió a la luz por primera vez hace un año, en febrero de 2022, cuando se descubrió que apuntaba a 56 bancos europeos por medio de aplicaciones cuentagotas publicadas en Google Play Store.

Por el contrario, la última versión del banco, que tiene un sitio web dedicad que anuncia sus características, está diseñada para apuntar a más de 400 instituciones bancarias y financieras, incluyendo varias billeteras de criptomonedas.

ThreatFabric dijo que detectó muestras del malware distribuido a través de la Red de Entrega de Contenido (CDN) de Discord, una técnica que ha experimentado un aumento desde 2020. Dos de las aplicaciones asociadas a Xenomorph se enumeran a continuación:

- Play Protect (com.great.calm)
- Play Protect (meritoriousness.mollah.presser)

> *«Xenomorph v3 se implementa mediante una aplicación Zombinder vinculada a un convertidor de moneda legítimo, que descarga como una 'actualización' una*

> *aplicación que se hace pasar por Google Protect»,* explicó ThreatFabric.

Zombinder se refiere a un servicio de vinculación de APK anunciado en la web oscura que permite a los ciberdelincuentes entregar malware por medio de versiones troyanizadas de aplicaciones legítimas. Desde entonces, la oferta se ha cerrado.

Los objetivos de la última campaña van más allá de su enfoque europeo (es decir, España, Italia y Portugal) para incluir entidades financieras belgas y canadienses.

Se sabe que Xenomorph, al igual que otros programas maliciosos bancarios, abusa de los servicios de accesibilidad para realizar fraudes mediante ataques superpuestos. También incluye capacidades para completar de forma automática transacciones fraudulentas en dispositivos infectados, una técnica llamada Sistema de Transferencia Automatizada (ATS).

Debido a que los bancos están pasando de los SMS para la autenticación de dos factores (2FA) a las aplicaciones de autenticación, el troyano Xenomorph incorpora un módulo ATS que le permite iniciar la aplicación y extraer los códigos de autenticación.

El malware de Android se jacta además de las funciones de robo de cookies, lo que permite a los hackers realizar ataques de apropiación de cuentas.

> *«Con estas nuevas características, Xenomorph ahora puede automatizar por completo toda la cadena de fraude, desde la infección hasta la exfiltración de fondos, lo que lo convierte en uno de los troyanos Android más avanzados y peligrosos en circulación»*, dijo la compañía.