Expertos en seguridad de Threat Fabric han identificado una versión renovada del troyano bancario para Android conocido como Chameleon. Esta variante avanzada posee habilidades para asumir el control de dispositivos, incluida la capacidad de esquivar verificaciones biométricas.

Chameleon surgió como amenaza a principios de 2023. Se propagaba usando diversos medios para infiltrar smartphones y tablets Android. Sus principales objetivos iniciales eran usuarios en Polonia y la región australiana.

El modus operandi de este troyano se centraba en apps bancarias, distribuyéndose a través de sitios fraudulentos que simulaban ser aplicaciones legítimas. En Polonia, se camuflaba como apps bancarias auténticas, mientras que en Australia se presentaba como una herramienta oficial del Departamento de Impuestos.

La versión actualizada de Chameleon intensifica sus tácticas. Además de afectar a usuarios en el Reino Unido e Italia, incorpora funciones avanzadas que lo hacen más astuto y peligroso.

Threat Fabric destaca que esta nueva versión se presenta bajo la apariencia de Google Chrome, el navegador más utilizado globalmente. Esta versión incluye dos atributos innovadores.

Primero, utiliza una interfaz HTML para solicitar la activación del servicio de accesibilidad, adaptándose especialmente a dispositivos Android 13 con ciertas limitaciones. Esta interfaz guía al usuario hacia la activación de servicios esenciales que Chameleon utiliza para sus maniobras.

> Los expertos detallan: «*Cuando se detecta la configuración restringida de Android 13 en el dispositivo afectado, el troyano inicia una carga de una interfaz HTML. Esta guía al usuario en un proceso detallado para activar el Servicio de Accesibilidad en versiones Android 13 y superiores. La ilustración siguiente muestra cómo*

> *Chameleon se adapta a los entornos Android 13».*

Segundo, esta variante posee la habilidad de interferir con sistemas biométricos en dispositivos comprometidos, dirigiendo al usuario hacia autenticaciones mediante PIN en lugar de métodos biométricos.

Otra mejora notable es su capacidad para gestionar tareas mediante la API AlarmManager. Esto permite al troyano identificar aplicaciones activas, información crucial para sus operaciones.

Los analistas subrayan que la estrategia del troyano se basa en la distribución de archivos APK de Android a través de medios no oficiales. Es vital recordar que descargar aplicaciones como Google Chrome de fuentes no confiables representa un riesgo.

Aunque este troyano pueda focalizarse en ciertas áreas específicas inicialmente, es evidente que sus operaciones podrían extenderse a otras geografías en el futuro.