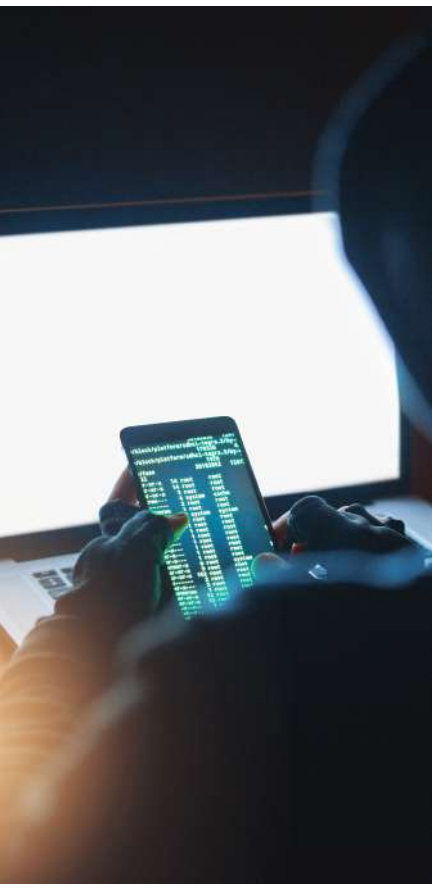
www.mexis.net

MALWARE CHAMELEON

BLOQUEA TU HUELLA DIGITAL Y ROBA INFORMACIÓN BANCARIA



Gracias a esta capacidad, el troyano puede desbloquear el terminal a voluntad sin autorización de las víctimas.

Una nueva variante del troyano identificado como Chameleon es capaz de bloquear el registro biométrico de dispositivos Android y, más concretamente el de la huella dactilar, para obligar a los usuarios a introducir su número PIN o contraseña y acceder a sus cuentas sin autorización.

Chameleon es un 'malware' identificado en enero de 2023 por la compañía de ciberseguridad ThreatFabric, **que tiene por objetivo principal las aplicaciones móviles bancarias y que se distribuye a través de páginas de 'phishing' fraudulentas de servicios legítimos.**

En el momento de su descubrimiento, este troyano se encontraba en su fase de desarrollo inicial, esto es, persentaba funcionalidades maliciosas limitadas, aunque "insinuaba un claro potencial para una mayor evolución e impacto", según ha explicado esta firma en su blog.

Este troyano, además, mostró una capacidad distintiva para manipular el dispositivo afectado, al ejecutar acciones en su nombre a través de una función de proxy, que **permite llevar a cabo ataques de apropiación de cuentas (ATO) y de apropiación de dispositivos (DTO).**

Según los investigadores, **estos ataques estaban dirigidos tanto a aplicaciones bancarias como a servicios de criptomonedas** y eran capaces de abusar de los privilegios del Servicio de Accesibilidad.

Para poder distribuir este 'malware', los agentes maliciosos lo disfrazaban de servicios legítimos, como la Oficina de Impuestos de Australia (ATO) a través de páginas de 'phishing', por lo que las víctimas podían creer que se trataba de enlaces confiables.

En base a sus investigaciones, los expertos en ciberseguridad han adelantado ahora que **ha surgido una iteración refinada de este troyano, que conserva características de su predecesor y que ha ampliado su línea de ataque a usuarios de Android en Reino Unido e Italia.**

Esta nueva variante se distribuye a través de la plataforma maliciosa Zombinder e introduce funciones avanzadas. Asimismo, ha logrado sumar más víctimas al hacerse pasar por aplicaciones de Google Chrome y también porque ha incorporado la capacidad de omitir indicaciones biométricas.

Esto quiere decir que **Chameleon es capaz de interrumpir el reconocimiento de la huella dactilar del dispositivo al bloquearlo, de modo que obliga a los usuarios a indicar el patrón, PIN o contraseña de acceso a la aplicación bancaria.**

Gracias a esta capacidad, **el troyano puede desbloquear el terminal a voluntad sin autorización de las víctimas** y sin la protección correspondiente a los sistemas de autenticación biométrica, ya que roba dichas credenciales.

Por otra parte, desde ThreatFabric han matizado que **este troyano también puede hacerse con el control del sistema y programar tareas empleando la interfaz de programación de aplicaciones (API) AlarmManager**, una habilidad con la que no contaba en su desarrollo inicial.

Por otra parte, esta variante más sofisticada también muestra una página HTML en dispositivos Android con la versión 13 y versiones posteriores del sistema operativo afectados, a quienes solicita que habiliten el servicio de Accesibilidad. Gracias a ello, puede ejecutar ataques DTO.

La compañía de ciberseguridad ha señalado finalmente que **la aparición del nuevo troyano bancario Chameleon es otro ejemplo del panorama de amenazas sofisticado y adaptable dentro del ecosistema Android** y que esta variante demuestra una mayor resistencia, al emplear múltiples métodos de distribución. **Esto es, a través de Zombinder y aplicaciones legítimas de Chrome.**

Fuente de información: publimetro.com.mx