Según ThreatFabric, Crocodilus no es una simple copia de otros troyanos bancarios, sino una amenaza avanzada desde el principio. Está equipado con técnicas modernas como:

- Control remoto del dispositivo
- Superposición de pantalla negra (para ocultar actividades maliciosas)
- Robo avanzado de datos mediante el abuso de los servicios de accesibilidad de Android

Como otros troyanos bancarios, Crocodilus facilita el control total del dispositivo (DTO, por sus siglas en inglés) para realizar transacciones fraudulentas. Un análisis del código fuente y los mensajes de depuración indica que el autor del malware habla turco.

¿Cómo se Propaga Crocodilus?

El malware se disfraza como una aplicación de Google Chrome con el nombre de paquete `"quizzical.washbowl.calamity"`, actuando como un dropper que evade las restricciones de Android 13 o superior.

Método de Infección:

1. Instalación y ejecución: Una vez que la víctima instala la aplicación falsa y la abre, esta solicita acceso a los servicios de accesibilidad de Android.
2. Conexión con un servidor remoto: El malware recibe instrucciones para atacar aplicaciones financieras específicas y aplicar superposiciones en pantalla para robar credenciales.

Ataques Contra Carteras de Criptomonedas

Además de bancos, Crocodilus también apunta a monederos de criptomonedas. En lugar de falsificar páginas de inicio de sesión, muestra un mensaje de advertencia falso, instando a la víctima a guardar su frase semilla en 12 horas para evitar perder acceso a su monedero.

Este truco de ingeniería social obliga a los usuarios a navegar hasta su frase semilla, la cual

es capturada mediante el abuso de accesibilidad, permitiendo a los atacantes robar fondos.

Funcionalidades Claves del Malware

- Monitorea el uso de aplicaciones y muestra superposiciones para interceptar credenciales.
- Captura eventos de accesibilidad, registrando todas las interacciones del usuario.
- Realiza capturas de pantalla, incluyendo contenido de Google Authenticator.
- Oculta sus actividades con una pantalla negra y silenciamiento de sonidos.

Otras capacidades incluyen:

 Lanzar aplicaciones específicas
 Autoeliminarse del dispositivo
 Enviar notificaciones push
 Enviar SMS masivos
 Extraer listas de contactos y aplicaciones instaladas
 Leer mensajes SMS
 Solicitar permisos de Administrador del Dispositivo
 Configurar el servidor C2
 Habilitar/deshabilitar keylogging
 Convertirse en el gestor predeterminado de SMS

Un Malware Altamente Sofisticado

ThreatFabric destaca que Crocodilus representa una nueva escalada en la evolución del malware bancario, mostrando una madurez poco común en amenazas recién descubiertas.

Mientras tanto, la empresa Forcepoint ha identificado una campaña de phishing que usa cebos relacionados con impuestos para distribuir el troyano bancario Grandoreiro. Este malware, dirigido a usuarios de Windows en México, Argentina y España, se propaga mediante un script de Visual Basic ofuscado.