Masterhacks – A inicios del año se informó sobre el troyano bancario para Android denominado BankBot, ahora volvió a infiltrarse en Google Play.

Este peligroso troyano ha estado evolucionando a lo largo del año y esta nueva versión presenta avances como la ofuscación de código mejorada, funcionalidad más sofisticada para descargar el payload y un mecanismo de infección muy sigiloso.

BankBot logró entrar a la tienda oficial de Google haciéndose pasar por un juego llamado Jewls Star Classic. Los piratas informáticos utilizaron el nombre de la saga Jewels Star, desarrollada por ITREEGAMER, misma que no está relacionada a la camapaña maliciosa.

Una vez que el usuario descarga el supuesto juego, desarrollado por GameDevTony, aparece un juego que sí funciona, pero cuenta con elementos escondidos, el malware bancario entre los recursos del juego y un servicio malicioso que espera por ser ejecutado luego de una ventana de tiempo.

El servicio malicioso se ejecuta luego de 20 minutos desde la primera ejecución de Jewels Star Classic. El dispositivo infectado muestra una alerta para que el usuario habilite «Google Service».

Cuando el usuario acepta, haciendo mención de que no hay forma de negarse, aparece el menú de accesibilidad de Android, donde se gestionan los servicios con esta función. Entre los servicios reales aparece uno nuevo llamado «Google Service», que fue creado por el malware.

Al intentar activar el servicio, aparece una lista de permisos requeridos:

- Observar tus acciones
- Recuperar contenido de ventana
- Prender Explore by Touch
- Activar la accesibilidad web mejorada
- Ejecutar acciones

Cuando se acepta todo, se otorgan permisos de accesibilidad reales al servicio propio del malware. Entonces el malware ya tiene permiso para ejecutar cualquier acción que necesite.

Luego, el malware realiza acciones como habilitar la instalación de aplicaciones de fuentes desconocidas, instalar BankBot desde los recursos y ejecutarlo, activar el administrador de dispositivos para BankBot, establecer BankBot como aplicación de SMS por defecto y obtener permiso para sobreescribir apps.

Al ejecutarse estas tareas, el malware comienza a trabajar en robar los detalles de la tarjeta de crédito de la víctima. Esta variante se enfoca principalmente en Google Play.

Cuando el usuario abre Google Play, BakBot se ejecuta y superpone a la app legítima un formulario falso, donde se le pide los datos de su tarjeta de crédito.

En caso de que el usuario ingrese los datos, BankBot tendría acceso a los recursos de la tarjeta, pues al interceptar los mensajes SMS, el malware puede evadir la doble autenticación que algunos bancos ofrecen a sus clientes.