Después de que algunos troyanos populares para Android como Anubis, Red Alert 2.0, GM bot y Exobot, abandonaron sus negocios, ha surgido un nuevo peligro en Internet con capacidades similares, que ofrece alquiler de bot de Android.

Apodado como Cerberus, el nuevo troyano de acceso remoto permite a los hackers tomar el control total sobre los dispositivos Android infectados y también viene con capacidades bancarias de troyanos como el uso de ataques de superposición, control de SMS y recolección de listas de contactos.

Según el autor del malware, que es sorprendentemente social en Twitter y se ha burlado abiertamente de los investigadores de seguridad y la industria antivirus, Cerberus ha sido codificado desde cero y no reutiliza ningún código de otros troyanos bancarios existentes.

El autor también afirmó que utiliza el troyano para operaciones privadas desde al menos dos años antes de alquilarlo para cualquier persona interesada en los últimos dos meses, a cambio de 2000 dólares por un mes de uso, 7000 dólares por 6 meses y hasta 12 mil dólares por 12 meses.

Según los investigadores de seguridad de ThreatFabric que analizaron una muestra de Cerberus, el malware cuenta con una lista muy común de características como:

- Tomar capturas de pantalla
- Grabar audio
- Grabar pulsaciones de teclado
- Enviar, recibir y borrar SMS
- Robar la lista de contactos
- Reenviar llamadas
- Recolectar información del dispositivo
- Rastrear la ubicación del dispositivo
- Robar credenciales de cuentas
- Deshabilitar Play Protect
- Descargar aplicaciones y cargas adicionales

- Desinstalar aplicaciones
- Notificaciones push
- Bloquear la pantalla del dispositivo

Una vez infectado, Cerberus primero oculta su icono del cajón de la aplicación y luego solicita el permiso de accesibilidad haciéndose pasar por Flash Player Service. Si se otorga, el malware registra de forma automática el dispositivo comprometido en su servidor de comando y control, lo que permite al comprador/atacante controlar el dispositivo de forma remota.

Para robar los números de tarjeta de crédito de los usuarios, las credenciales bancarias y las contraseñas para otras cuentas en línea, Cerberus permite a los atacantes lanzar ataques de superposición de pantalla desde su tablero remoto.

En el ataque de superposición de pantalla, el troyano muestra una superposición sobre las aplicaciones de banca móvil legítimas y engaña a los usuarios de Android para que ingresen sus credenciales bancarias en la pantalla de inicio de sesión falsa, como un ataque de phishing.

> *«El bot abusa del privilegio del servicio de accesibilidad para obtener el nombre del paquete de la aplicación en primer plano y determinar si mostrar o no una ventana de superposición de phishing»*, dijeron los investigadores.

Según los investigadores, Cerberus ya contiene plantillas de ataque superpuesto para un total de 30 objetivos únicos, que incluyen:

- 7 aplicaciones bancarias francesas
- 7 aplicaciones bancarias de Estados Unidos
- 1 aplicación bancaria japonesa
- 15 aplicaciones no bancarias

Cerberus utiliza táctica de evasión basada en movimiento

Cerberus también utiliza algunas técnicas interesantes para evadir la detección de soluciones antivirus y evitar su análisis, como usar el sensor del acelerómetro del dispositivo para medir los movimientos de la víctima.

A medida que el usuario se mueve, tu dispositivo Android generalmente crea cierta cantidad de datos del sensor de movimiento. El malware monitorea los pasos del usuario por medio del sensor de movimiento del dispositivo para verificar si se está ejecutando en un dispositivo Android real.

> *«El troyano usa este contador para activar el bot; si el contador de pasos mencionado anteriormente alcanza el umbral preconfigurado, considera que la ejecución en el dispositivo es segura. Esta simple medida evita que el troyano se ejecute y se analice en entornos de análisis dinámico y en los dispositivos de prueba de analistas de malware»,* dicen los investigadores.

Si el dispositivo del usuario carece de datos del sensor, el malware asume que sandox para escanear malware es un emulador sin sensores de movimiento y no ejecutará el código malicioso.

Sin embargo, esta técnica tampoco es única y ha sido implementada previamente por el popular troyano bancario para Android, Anubis.

Cabe mencionar que el malware Cerberus no aprovecha ninguna vulnerabilidad para instalarse automáticamente en un dispositivo de destino en primer lugar. En cambio, la instalación de malware se basa en tácticas de ingeniería social.

Por lo tanto, para protegerse de estas amenazas de malware, se recomienda tener cuidado con lo que descarga en tu teléfono y que definitivamente se piense muchas veces antes de descargas cosas de fuentes desconocidas.