Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°204	Fecha: 30-08-2023
		Página: 4 de 7

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El troyano MMRat para Android ejecuta un fraude financiero remoto mediante una función de accesibilidad		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES:**

   Se ha observado que un troyano bancario para Android, previamente indocumentado, denominado MMRat, se dirige a usuarios móviles en el Sudeste Asiático desde finales de junio de 2023 para controlar de forma remota los dispositivos y realizar fraudes financieros.

2. **DETALLES:**

   "El malware, llamado así por el nombre distintivo de su paquete com.mm.user, puede capturar la entrada del usuario y el contenido de la pantalla, y también puede controlar de forma remota los dispositivos de la víctima a través de diversas técnicas, lo que permite a sus operadores llevar a cabo fraude bancario en el dispositivo de la víctima", dijo Trend Micro.

   Lo que distingue a MMRat de otros de su tipo es el uso de un protocolo personalizado de comando y control (C2) basado en buffers de protocolo (también conocido como protobuf) para transferir eficientemente grandes volúmenes de datos desde teléfonos comprometidos, lo que demuestra la creciente sofisticación del malware.

   El punto de entrada de los ataques es una red de sitios de phishing que imitan las tiendas de aplicaciones oficiales, aunque actualmente se desconoce cómo se dirige a las víctimas a estos enlaces. MMRat normalmente se hace pasar por un gobierno oficial o una aplicación de citas. Una vez instalada, la aplicación se apoya en gran medida en el servicio de accesibilidad de Android y en la API MediaProjection, los cuales han sido aprovechados por otro troyano financiero de Android llamado SpyNote, para llevar a cabo sus actividades. El malware también es capaz de abusar de sus permisos de accesibilidad para concederse otros permisos y modificar configuraciones.

   Además, configura la persistencia para sobrevivir entre reinicios e inicia comunicaciones con un servidor remoto para esperar instrucciones y filtrar los resultados de la ejecución de esos comandos. El troyano emplea diferentes combinaciones de puertos y protocolos para funciones como exfiltración de datos, transmisión de video y control C2.

   MMRat posee la capacidad de recopilar una amplia gama de datos del dispositivo e información personal, incluida la intensidad de la señal, el estado de la pantalla y las estadísticas de la batería, las aplicaciones instaladas y las listas de contactos. Se sospecha que el actor de la amenaza utiliza los detalles para realizar algún tipo de perfilado de la víctima antes de pasar a la siguiente etapa.

   Algunas de las otras características de MMRat incluyen la grabación del contenido de la pantalla en tiempo real y la captura del patrón de la pantalla de bloqueo para permitir que el actor de la amenaza obtenga acceso remoto al dispositivo de la víctima cuando está bloqueado y no está en uso activo.

   "El malware MMRat abusa del servicio de Accesibilidad para controlar remotamente el dispositivo de la víctima, realizando acciones como gestos, desbloquear pantallas e ingresar texto, entre otras", dijo Trend Micro. "Esto puede ser utilizado por actores de amenazas, junto con credenciales robadas, para realizar fraude bancario".

   Los ataques terminan con MMRat eliminándose al recibir el comando C2 UNINSTALL_APP, que generalmente ocurre después de una transacción fraudulenta exitosa, eliminando efectivamente todos los rastros de infección del dispositivo.

3. **RECOMENDACIONES:**

   - Descargar aplicaciones sólo de fuentes oficiales.
   - Examinar las revisiones de las aplicaciones y verificar los permisos a los que una aplicación debe solicitar acceso antes de su uso.

Fuente de Información:	• hxxps://thehackernews.com/2023/08/mmrat-android-trojan-executes-remote.html