Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°307	Fecha: 27-12-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Malware De Android Que Infecta Activamente Dispositivos Para Tomar El Control Total		
Tipo de Ataque	Malware	Abreviatura	Malware
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:

El malware de Android infecta dispositivos para tomar el control total con diversos fines ilícitos como:

- Robar información confidencial.
- Generar transacciones financieras no autorizadas.
- Habilitar ataques remotos.

Al obtener un control total, los actores de amenazas pueden explotar el dispositivo para sus actividades ilícitas, lo que representa amenazas importantes para la privacidad y seguridad del usuario.

2. DETALLES:

Los analistas de ciberseguridad de McAfee Mobile Research encontraron recientemente una puerta trasera de Android, "Android/Xamalicious", que utiliza el marco Xamarin para infectar dispositivos y tomar el control total.

Emplea ingeniería social para obtener privilegios de accesibilidad y se comunica con el servidor C2

En la segunda etapa, la carga útil inyectada dinámicamente como DLL de ensamblaje, toma el control total para generar:

- Fraude publicitario
- Instalaciones de aplicaciones
- Acciones motivadas financieramente

Los investigadores identificaron el vínculo con la aplicación de fraude publicitario “Cash Magnet”, lo que revela una motivación financiera. El uso de Xamarin permite una actividad a largo plazo, ocultando código malicioso en el proceso de compilación del APK.

Se utilizaron técnicas de cifrado personalizado y ofuscación para la comunicación y la filtración de datos. Alrededor de 25 aplicaciones maliciosas conllevan la amenaza, en las cuales, algunas están en Google Play desde mediados de 2020.

Las medidas proactivas de McAfee y Google Play Protect tienen como objetivo mitigar las aplicaciones potencialmente dañinas. Android/Xamalicious, detectado en al menos 327.000 dispositivos, permanece muy activo.

Los troyanos de Android/Xamalicious se disfrazan de aplicaciones de las siguientes categorías que están disponibles en mercados de terceros:

- Salud
- Juego
- Horóscopo
- Productividad

A diferencia del malware anterior basado en Xamarin, Xamalicious se distingue por su implementación. La arquitectura Xamarin permite la interpretación de código .NET en Android a través de Mono.

Una aplicación de ejemplo, "Numerology", solicita a las víctimas que habiliten servicios de accesibilidad para funciones engañosas.

Todos los servicios de accesibilidad deben activarse manualmente después de varias advertencias del sistema operativo.

Después de adquirir permisos de accesibilidad, el malware se pone en contacto con el servidor para realizar la carga útil de la segunda etapa.

El malware Xamalicious verifica la información del dispositivo de la víctima, como las aplicaciones y el estado de enraizamiento, mediante comandos del sistema. Si está rooteado o conectado a través de ADB, omite la descarga de carga útil de la segunda etapa.

A continuación, mencionamos los tipos de información que recopila el malware:

Método/Comando	Descripción
DevInfo	Información de hardware y dispositivo que incluye: • ID de Android • Marca, CPU, modelo, huella digital, Número de Serie • Versión del sistema operativo, liberación de actualización, SDK • Idioma • Estado de la opción de desarrollador • Información SIM (operador, estado, tipo de red, etc.) • Firmware, versión de firmware
GeoInfo	Ubicación del dispositivo según la dirección IP, el malware contacta servicios como api.myip.com para verificar la ubicación del dispositivo y los datos del ISP. • Nombre del proveedor de servicios de Internet • Organización • Servicios Puntuación de Fraude: Autoprotección para identificar si el dispositivo no es un usuario real
EmuInfo	Enumera todas las adbProperties que en un dispositivo real tienen alrededor de 640 propiedades. Esta lista está codificada como un parámetro de cadena en formato codificado en URL. Estos datos pueden usarse para determinar si el cliente afectado es un dispositivo real o un emulador ya que contiene parámetros como: • CPU • Memoria • Sensores • Configuración USB • Estado del BAD
RootInfo	Después de intentar identificar si el dispositivo está rooteado o no con múltiples técnicas, el resultado se consolida en este comando
Packages	Utiliza los comandos del sistema "pm list packages -s" y "pm list packages -3" para enumerar el sistema y las aplicaciones instaladas en el dispositivo.
Accessibillity	Proporciona el estado si se otorgan o no permisos de servicios de accesibilidad
GetURL	Este comando sólo proporciona el ID de Android y es una solicitud para la carga útil de la segunda etapa. El C2 evalúa la solicitud proporcionada del cliente y devuelve un estado y una DLL de ensamblaje cifrada.

Con la ayuda de RSA-OAEP y HTTPS, Xamalicious cifra todos los datos para evadir la detección. Sin embargo, si la infraestructura C2 está disponible, las claves RSA codificadas en la DLL permiten el descifrado.

La función Enviar() cifra los datos con un JWT y los envía a "/Updater" a través de HTTP POST. La función decrypt() utiliza una clave privada RSA codificada para las respuestas C2, que posiblemente contenga una carga útil de segunda etapa.

Los datos enviados al servidor C&C que decide la entrega de la carga útil de la segunda etapa y la autoprotección del malware incluyen:

- Enraizamiento
- BAsD
- Comprobaciones de SIM

El C&C cifra la DLL con AES y una clave específica del dispositivo, el dispositivo descifra el token y luego el parámetro 'URL' con una clave AES personalizada única para los detalles del dispositivo.

3. RECOMENDACIONES:

- Evitar abrir o descargar archivos adjuntos o enlaces sospechosos en correos no solicitados o mensajes de redes sociales.
- Verificar la fuente de información de tus correos entrantes.
- Utilizar una aplicación de seguridad que le proporcione una capa adicional de protección escaneando e identificando aplicaciones potencialmente dañinas, detectando malware y advirtiendo a los usuarios sobre actividades sospechosas.
- Instalar y mantener actualizados los últimos parches de seguridad de su software, tanto en el sistema operativo como en su antivirus.

Fuente de Información:	• hxxps://gbhackers.com/android-malware-actively-infecting-devices/