Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°239	Fecha: 09-10-2023
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los dispositivos chinos basados en Android vienen preinstalados con una puerta trasera de firmware		
Tipo de Ataque	Backdoors	Abreviatura	Backdoors
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C04
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El equipo de investigadores de ciberseguridad de la compañía Human Security ha hecho pública una trama de ciberdelincuencia de gran envergadura.

La empresa está revelando nuevos detalles sobre el alcance de los dispositivos infectados y la red oculta e interconectada de esquemas de fraude vinculados a las cajas de streaming, tablets y apps para iOS y Android.

La investigación de Human Security se divide en dos áreas: Badbox, que involucra los dispositivos Android comprometidos y las formas en que están involucrados en fraude y cibercrimen. Y el segundo, denominado Peachpit, es una operación de fraude publicitario relacionada que involucra al menos 39 aplicaciones de Android y iOS.

Actualmente no está claro cómo los dispositivos Android se ven comprometidos con una puerta trasera de firmware, pero la evidencia apunta a un ataque a la cadena de suministro de hardware.

2. DETALLES:

Esta primera operación, bautizada con el nombre de BADBOX, se basa en la introducción de malware en la cadena de suministro de diversos dispositivos Android fabricados en China — televisiones conectadas (CTV), smartphones y tablets — que luego se distribuyen a través de importantes plataformas de comercio minorista, lo que hace que los usuarios no desconfíen de sus dispositivos.

BADBOX es una red mundial de productos de consumo que oculta puertas traseras de firmware en las cadenas de suministro de hardware. También se infiltran en hogares y oficinas, vinculándose a un servidor de comando y control, lo que lleva a diversas actividades fraudulentas.

BADBOX ha dejado una huella significativa, infectando más de 74.000 dispositivos Android en todo el mundo, incluidas escuelas públicas de EE. UU.

Los investigadores confirmaron ocho dispositivos con puertas traseras instaladas: siete Android TV Box: T95, T95Z, T95MAX, X88, Q9, X12PLUS y MXQ Pro 5G, y una tablet: J5-W.

BADBOX utiliza el malware Triada a modo de "puerta trasera". Aunque este malware se descubrió por primera vez en 2016 por la empresa de seguridad Kaspersky, sigue siendo una amenaza relevante hoy en día, pues modifica un elemento del sistema operativo Android, permitiéndose acceder a las aplicaciones instaladas en los dispositivos, y a todo tipo de información personal en ellos.

Incluso después de realizar una restauración a la configuración de fábrica, los dispositivos infectados siguen comprometidos, ya que el malware (instalado en la propia fábrica) se conecta a un servidor de comando y control ya desde el primer arranque, descargando un conjunto de instrucciones y comienza a hacer un montón de cosas malas.

Algunos ejemplos mencionados en el reporte de seguridad incluyen fraude publicitario; servicios de proxy residencial, donde el grupo detrás del plan vende acceso a tu red doméstica; la creación de cuentas falsas de Gmail y WhatsApp utilizando tus conexiones e instalación remota de código.

Por otra parte, la botnet de fraude publicitario denominada PEACHPIT aprovechó un ejército de cientos de miles de dispositivos Android y iOS para generar ganancias ilícitas para los actores de amenazas detrás del plan.

Se dice que las infecciones se realizaron a través de una colección de 39 aplicaciones que se instalaron más de 15 millones de veces. Algunos ejemplos de aplicaciones infectadas eran sobre cómo desarrollar abdominales y registrar la cantidad de agua que bebe una persona.

Dentro de las aplicaciones de Android hay un módulo responsable de crear WebViews ocultos que luego se utilizan para solicitar, representar y hacer clic en anuncios, y disfrazar las solicitudes de anuncios como si se originaran en aplicaciones legítimas, una técnica observada previamente en el caso de VASTFLUX .

Los dispositivos equipados con malware permitieron a los operadores robar datos confidenciales, crear nodos proxy residenciales y cometer fraude publicitario a través de aplicaciones falsas.

"Los actores de amenazas también pueden utilizar los dispositivos con puerta trasera para crear cuentas de mensajería de WhatsApp robando contraseñas de un solo uso de los dispositivos", dijo la compañía.

"Además, los actores de amenazas pueden usar los dispositivos para crear cuentas de Gmail, evadiendo la típica detección de bots porque la cuenta parece haber sido creada desde una tableta o teléfono inteligente normal, por una persona real".

La investigación dice que si bien los que están detrás de Peachpit parecen diferentes de los que están detrás de Badbox, es probable que estén trabajando juntos de alguna manera.

La firma de prevención de fraude señaló que trabajó con Apple y Google (desarrollador de Android y, al mismo tiempo, propietario del mayor ecosistema de publicidad online) para interrumpir la operación, y agregó que "el resto de BADBOX debe considerarse inactivo: los servidores C2 que alimentan la infección de puerta trasera del firmware BADBOX han sido eliminados por los actores de amenazas". Eso no significa que los dispositivos hayan sido 'limpiados' de la puerta trasera, sólo que habrían dejado de recibir instrucciones (y enviar datos) desde de la misma.

Dicho esto, se sospecha que los atacantes están ajustando sus tácticas en un probable intento de eludir las defensas.

3. RECOMENDACIONES:

- Evite los dispositivos que no sean de marca oficial, ya que carecen de la certificación Play Protect.
- Los usuarios deben verificar el estado de certificación de su dispositivo.
- Tenga cuidado con las aplicaciones de clonación y conozca el origen de sus descargas.
- Si su dispositivo actúa de manera extraña, considere realizar un restablecimiento de fábrica para eliminar las aplicaciones comprometidas.

Fuente de Información:	• hxxps://gbhackers.com/badbox-firmware-backdoors/ • hxxps://www.genbeta.com/seguridad/sale-a-luz-venta-cientos-miles-dispositivos-android-malware-que-actuaba-como-puerta-trasera • hxxps://www.adslzone.net/noticias/seguridad/malware-badbox-android-tv-box-puerta-trasera/ • hxxps://thehackernews.com/2023/10/peachpit-massive-ad-fraud-botnet.html