Se ha detectado un nuevo malware para Android llamado SoumniBot en circulación, dirigido a usuarios en Corea del Sur aprovechando fallos en el procedimiento de extracción y análisis del manifiesto.

El software malicioso destaca por su enfoque poco convencional para eludir la detección y análisis, particularmente mediante la ofuscación del manifiesto de Android, según señaló el investigador de Kaspersky, Dmitry Kalinin, en un análisis técnico.

Cada aplicación de Android viene acompañada de un archivo XML de manifiesto («AndroidManifest.xml») que reside en el directorio principal y declara los distintos componentes de la aplicación, así como los permisos y las características de hardware y software que requiere.

Dado que los investigadores de amenazas suelen iniciar su análisis examinando el archivo de manifiesto de la aplicación para comprender su funcionamiento, los perpetradores detrás de este malware han utilizado tres métodos distintos para dificultar este proceso.

En primer lugar, se emplea un método inválido de compresión al desempaquetar el archivo de manifiesto del APK utilizando la biblioteca libziparchive, que considera como no comprimido cualquier valor distinto de 0x0000 o 0x0008.

> *«Esto permite a los desarrolladores de aplicaciones utilizar cualquier valor, excepto 8, en el método de compresión y escribir datos sin comprimir»,* explicó Kalinin.
>
> *«Aunque cualquier herramienta de desempaquetado que implemente la validación correcta del método de compresión consideraría inválido un manifiesto así, el analizador de APK de Android lo reconoce correctamente y permite la instalación de la aplicación».*

Es importante destacar que este método ha sido adoptado por perpetradores asociados con

varios troyanos bancarios para Android desde abril de 2023.

En segundo lugar, SoumniBot altera el tamaño del archivo de manifiesto archivado, proporcionando un valor superior al real, lo que resulta en que el archivo «descomprimido» se copie directamente, y el analizador de manifiestos ignora el resto de los datos «superpuestos» que ocupan el resto del espacio disponible.

> *«Los analizadores de manifiesto más estrictos no podrían leer un archivo así, mientras que el analizador de Android maneja el manifiesto inválido sin errores»,* dijo Kalinin.

La última técnica consiste en utilizar nombres de espacio de nombres XML largos en el archivo de manifiesto, lo que dificulta que las herramientas de análisis asignen suficiente memoria para procesarlos. Sin embargo, el analizador de manifiestos está diseñado para pasar por alto los espacios de nombres, y como resultado, no se generan errores al procesar el archivo.

Una vez activado, SoumniBot solicita su configuración desde una dirección de servidor codificada, para obtener los servidores utilizados para enviar los datos recopilados y recibir comandos mediante el protocolo de mensajería MQTT, respectivamente.

Está diseñado para iniciar un servicio malicioso que se reinicia cada 16 minutos si se detiene por alguna razón, y carga la información cada 15 segundos. Esto incluye metadatos del dispositivo, listas de contactos, mensajes SMS, fotos, videos y una lista de aplicaciones instaladas.

Además, el malware es capaz de agregar y eliminar contactos, enviar mensajes SMS, cambiar al modo silencioso y activar el modo de depuración de Android, además de ocultar el ícono de la aplicación para dificultar su desinstalación del dispositivo.

Una característica destacada de SoumniBot es su capacidad para buscar archivos .key y .der

en el almacenamiento externo, que contienen rutas a «/NPKI/yessign», relacionado con el servicio de certificado de firma digital ofrecido por Corea del Sur para gobiernos (GPKI), bancos e intercambios de acciones en línea (NPKI).

> *«Estos archivos son certificados digitales emitidos por bancos coreanos a sus clientes y se utilizan para iniciar sesión en servicios bancarios en línea o confirmar transacciones bancarias. Esta táctica es bastante inusual para el malware bancario de Android»,* explicó Kalinin.

A principios de este año, la firma de ciberseguridad S2W reveló detalles de una campaña de malware llevada a cabo por el grupo Kimusuky, vinculado a Corea del Norte, que utilizaba un ladrón de información basado en Golang llamado Troll Stealer para extraer certificados GPKI de sistemas Windows.

> *«Los creadores de malware buscan maximizar la cantidad de dispositivos infectados sin llamar la atención. Esto los motiva a buscar nuevas formas de complicar la detección. Los desarrolladores de SoumniBot lamentablemente tuvieron éxito debido a la falta de validaciones estrictas en el código del analizador de manifiestos de Android».*

Cuando se contactó para hacer comentarios, Google informó que no encontró aplicaciones que contengan SoumniBot en la tienda Google Play Store para Android.

> *«Los usuarios de Android están protegidos automáticamente contra las versiones conocidas de este malware por Google Play Protect, que está habilitado de forma predeterminada en los dispositivos Android con Google Play Services. Google Play Protect puede advertir a los usuarios o bloquear aplicaciones conocidas por mostrar comportamiento malicioso, incluso cuando esas aplicaciones provienen de fuentes*

> *externas a Play»,* agregó.