Miles de millones de usuarios de Android pueden ser fácilmente engañados para cambiar la configuración de red crítica de sus dispositivos con solo un ataque de phishing basado en SMS.

Al insertar una nueva SIM en un teléfono y conectarse a la red celular por primera vez, el servicio de operador configura de forma automática o envía un mensaje con la configuración específica de la red requerida para conectarse a los servicios de datos.

Al instalarlo de forma manual en el dispositivo, la mayoría de los usuarios nunca se molestan en revisar qué configuraciones se están realizando en los mensajes conocidos como OMA CP.

Ahora, es necesario preocuparse por estas configuraciones, pues la instalación de configuraciones no confiables podría poner en riesgo la privacidad de tus datos, permitiendo que hackers remotos espíen tus comunicaciones de datos, según informó un equipo de investigadores.

Los operadores de telefonía móvil envían mensajes OMA CP (Open Mobile Alliance Client Provisioning), que contienen configuraciones APN y otras de dispositivos que el teléfono necesita para poder establecer una conexión a la puerta de enlace entre la red móvil del operador y los servicios públicos de Internet.

Para la configuración APN, se incluye un campo opcional para configurar el proxy HTTP que puede enrutar el tráfico web a través de él, pero muchos operadores utilizan servidores proxy transparentes que no requieren una configuración.

Además de la configuración de proxy, los mensajes de aprovisionamiento de OMA CP también pueden incluir configuraciones para cambiar lo siguiente:

- Servidor de mensajes MMS
- Dirección proxy
- Página de inicio del navegador y marcadores
- Servidor de correo

- Servidores de directorio para sincronizar contactos y calendario, entre otros

Según un nuevo informe de Check Point, los nuevos mensajes de aprovisionamiento débilmente auteticados implementados por algunos fabricantes de dispositios, incluyendo Samsung, Huawei, LG y Sony, pueden permitir que los piratas informáticos remotos engañen a los usuarios para actualizar su configuración de dispositivos con servidores proxy controlados por el atacante.

A su vez, esto podría permitir a los hackers interceptar fácilmente algunas conexiones de red que un dispositivo objetivo realiza a través de su servicio de soporte de datos, incluidos los navegadores web y los clientes de correo electrónico integrados.

> *«Solo se necesita un único mensaje SMS para obtener acceso completo a sus correos electrónicos. En estos ataques, un agente remoto puede engañar a los usuarios para que acepten nuevas configuraciones del teléfono que, por ejemplo, enruten todo su tráfico de Internet para robar correos electrónicos por medio de un proxy controlado por el atacante»,* dijeron los investigadores.
>
> *«Además, cualquier persona conectada a una red celular puede ser el objetivo de esta clase de ataques de phishing, lo que significa que no tiene que estar conectado a una red WiFi para obtener sus datos privados de correo electrónico extraídos maliciosamente por ciberatacantes»*.

Sin embargo, al igual que en el caso de configurar un proxy para una conexión WiFi, no todas las aplicaciones instaladas en un dispositivo de destino utilizan la configuración de proxy para la red de datos móviles. En cambio, depende de qué aplicación se haya diseñado para aceptar el proxy configurado por el usuario.

Además, el servidor proxy no podría descifrar las conexiones HTTPS, por lo tanto, esta técnica es adecuada solo para interceptar conexiones inseguras.

> *«Esta es una clasificación completamente nueva de ataques de phishing en nuestros correos electrónicos. Al principio fue difícil clasificar la vulnerabilidad porque es un problema de especificidad profunda. Probablemente sea el ataque de phishing más avanzado en nuestros correos electrónicos que he visto hasta la fecha»*, dijo Slava Makkaveev, investigador de Chek Point, a THN.

Volviendo a las debilidades que los investigadores de Check Point identificaron en la autenticación de los mensajes de aprovisionamiento, las especificaciones que el estándar de la industria recomienda para que el aprovisionamiento de OTA sea seguro no obliga a los operadores a autenticar de forma adecuada los mensajes de CP utilizando USERPIN, NETWPIN y otros métodos.

Como resultado, un destinatario del mensaje no puede verificar si el mensaje OMA CP con la nueva configuración se originó en su operador de red o en un impostor, lo que brinda a los atacantes la oportunidad de explotar dicha debilidad.

> *«Más peligrosamente, cualquiera puede comprar un dongle USB de $10 y ejecutar un ataque de phishing a gran escala. No se requiere equipo especial para llevar a cabo el ataque. Los mensajes de CP de suplantación de identidad pueden ser dirigidos de forma restringida, por ejemplo, precedidos de un mensaje de texto personalizado diseñado para engañar a un destinatario en particular, o enviados a granel, suponiendo que al menos algunos de los destinatarios sean lo suficientemente crédulos como para aceptar un CP sin cuestionar su autenticidad»*, agregaron los investigadores.

Los investigadores informaron sus hallazgos a los vendedores de teléfonos Android afectados en marzo de 2019. Samsung y LG abordaron el problema en su versión de mantenimiento de seguridad para mayo y julio.

Huawei planea solucionar el problema en la siguiente generación de teléfonos inteligentes de

la serie Mate o de la serie P, mientras que Sony no quiso reconocer el problema, afirmando que sus dispositivos móviles siguen la especificación OMA CP.

Aún después de recibir parches, los investigadores recomendaron a los usuarios que no confíen ciegamente en los mensajes de sus operadores de telefonía móvil o en las configuraciones de APN disponibles en Internet.