Investigadores de seguridad cibernética identificaron 42 aplicaciones en Google Play Store, con un total de más de 8 millones de descargas, que inicialmente se distribuyeron como aplicaciones legítimas pero luego se actualizaron para mostrar de forma maliciosa, anuncios de pantalla completa a sus usuarios.

Descubierto por el investigador de seguridad de ESET, Lukas Stefanko, estas apps de adware para Android fueron desarrolladas por un estudiante universitario vietnamita, que fue rastreado fácilmente porque nunca ocultó su identidad.

Los detalles de registro disponibles públicamente de un dominio asociado con las aplicaciones de adware, ayudaron a encontrar la identidad del desarrollador deshonesto, incluyendo su nombre real, dirección y número de teléfono, lo que finalmente reveló sus cuentas personales en Facebook, GitHub y YouTube.

> *«Al ver que el desarrollador no tomó ninguna medida para proteger su identidad, parece probable que sus intenciones no fueron deshonestas. En algún momento de su carrera en Google Play, aparentemente decidió aumentar sus ingresos publicitarios mediante la implementación de la funcionalidad de adware en el código de sus aplicaciones»,* dijo Stefanko en una publicación.

Debido a que las 42 aplicaciones de adware brindan las funcionalidades originales que prometieron, como Radio FM, descargador de video o juegos, es bastante difícil para la mayoría de los usuarios detectar aplicaciones maliciosas o encontrar algo sospechoso.

Implementación del adware

La familia de malware ha sido nombrada como *«Ashas»*, el componente malicioso se conecta a un servidor remoto de comando y control operado por el desarrollador y envía de forma automática información básica sobre el dispositivo Android con una de las aplicaciones de adware instaladas.

Después, la aplicación recibe datos de configuración del servidor de Comando y Control responsable de mostrar anuncios según la elección del atacante y aplicar una serie de trucos para el sigilo y la resistencia, algunos de los cuales se mencionan a continuación.

Para ocultar su funcionalidad maliciosa del mecanismo de seguridad de Google Play, las aplicaciones primero comprueban la dirección IP del dispositivo infectado, y si se encuentra dentro del rango de direcciones IP conocidas para los servidores de Google, la aplicación no activará la carga de adware.

Con el fin de evitar que los usuarios asocien inmediatamente los anuncios no deseados con las aplicaciones, el desarrollador también agregó una funcionalidad para establecer un retraso personalizado entre la visualización de anuncios y la instalación de la aplicación.

Además, las aplicaciones también ocultan sus iconos en el menú del teléfono Android y crean un acceso directo en un intento de evitar la desinstalación.

> *«Si un usuario típico intenta deshacerse de la aplicación maliciosa, es probable que solo se elimine el acceso directo. La aplicación sigue ejecutándose en segundo plano sin el conocimiento del usuario»,* dijo Stefanko.

Si el usuario afectado se dirige al botón «Aplicaciones recientes» para verificar qué aplicación está publicando anuncios, el adware muestra el icono de Facebook o Google para parecer legítimo y evitar sospechas, engañando a los usuarios para que crean que un servicio legítimo está mostrando los anuncios.

Aunque Stefanko no habló mucho sobre el tipo de anuncios que este adware sirve a los usuarios infectados, el adware por lo general bombardea a los dispositivos infectados con anuncios, principalmente llevando a sitios web fraudulentos, maliciosos y de phishing.

El investigador informó al equipo de seguridad de Google sobre sus hallazgos, y la compañía ya eliminó las aplicaciones en cuestión de su plataforma Play Store.

Si has descargado alguna de estas aplicaciones, debes eliminarlas inmediatamente de tu dispositivo.