Tipos de Amenazas

Sala 4

**Tipo de virus:** Adwares

Son muy similares a los troyanos, cuyo objetivo es bombardear nuestro dispositivo con publicidad. No son dañinos y usualmente vienen dentro de troyanos.

**Link noticia**: <https://thehackernews.com/2019/10/42-adware-apps-with-8-million-downloads.html>

La amenaza comienza cuando se instala la app en el celular, los investigadores de ciberseguridad 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 anuncios maliciosos en pantalla completa a sus usuarios.

El desarrollador de este malware fue un estudiante universitario vietnamita, fue sencillo rastrearlo ya que no se tomo la molestia de ocultar su identidad. Los detalles de registro disponibles públicamente de un dominio asociado con las aplicaciones de adware ayudaron a encontrar la identidad del desarrollador, incluido su nombre real, dirección y número de teléfono, lo que finalmente llevó al investigador a sus cuentas personales en **Facebook, GitHub y YouTube.**

## Apps

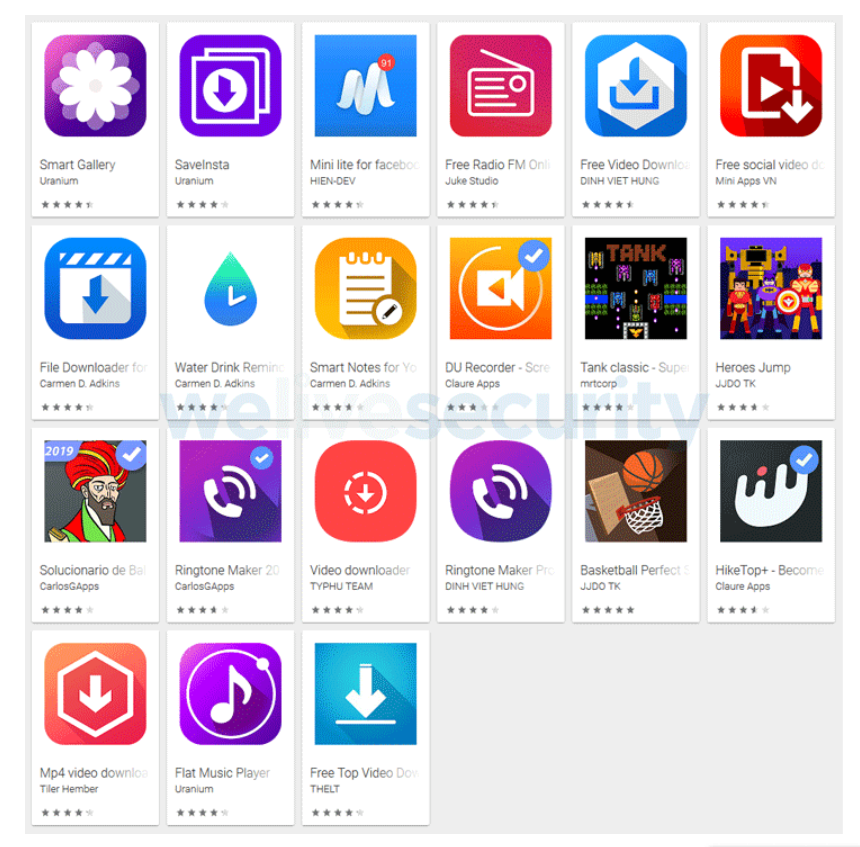
Apodado la familia de programas publicitarios "Ashas", el componente malicioso se conecta a un servidor de comando y control remoto operado por el desarrollador y envía automáticamente información básica sobre el dispositivo Android con una de las aplicaciones publicitarias instaladas.

Luego, la aplicación recibe datos de configuración del servidor responsable de mostrar anuncios según la elección del atacante.

Para ocultar su funcionalidad maliciosa del mecanismo de seguridad de Google Play, las aplicaciones primero verifican 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 útil del adware.

Para evitar que los usuarios asocien inmediatamente los anuncios no deseados con su aplicación, 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.



**¿Qué es interesante?** Si el usuario afectado se dirige al botón "Aplicaciones recientes" para verificar qué aplicación está publicando anuncios, el adware muestra el ícono de Facebook o Google para parecer legítimo y evitar sospechas, engañando a los usuarios haciéndoles creer que los anuncios están siendo mostrados por un servicio legítimo.