Han salido a la luz detalles sobre una *«gran operación de fraude publicitario»* que utiliza cientos de aplicaciones en la Google Play Store para llevar a cabo diversas actividades maliciosas.

La campaña ha sido bautizada como Konfety – la palabra rusa para caramelo – debido a su uso indebido de un kit de desarrollo de software (SDK) de publicidad móvil vinculado a una red publicitaria con sede en Rusia llamada CaramelAds.

> *«Konfety representa una nueva forma de fraude y ofuscación, en la que los actores de amenazas operan versiones 'malévolas' de aplicaciones 'señuelo' disponibles en los principales mercados»,* dijo el equipo de inteligencia de amenazas Satori de HUMAN en un informe técnico.

Mientras que las aplicaciones señuelo, que suman más de 250, son inofensivas y se distribuyen a través de la Google Play Store, sus versiones «*malévolas*» se difunden mediante una campaña de publicidad maliciosa diseñada para facilitar el fraude publicitario, monitorear búsquedas web, instalar extensiones de navegador y cargar archivos APK en los dispositivos de los usuarios.

El aspecto más notable de la campaña es que la versión malévola se hace pasar por la versión señuelo falsificando el ID de la aplicación y los IDs de los publicistas de anuncios de esta última. Tanto las aplicaciones señuelo como las malévolas operan en la misma infraestructura, permitiendo a los actores de amenazas escalar sus operaciones exponencialmente según sea necesario.

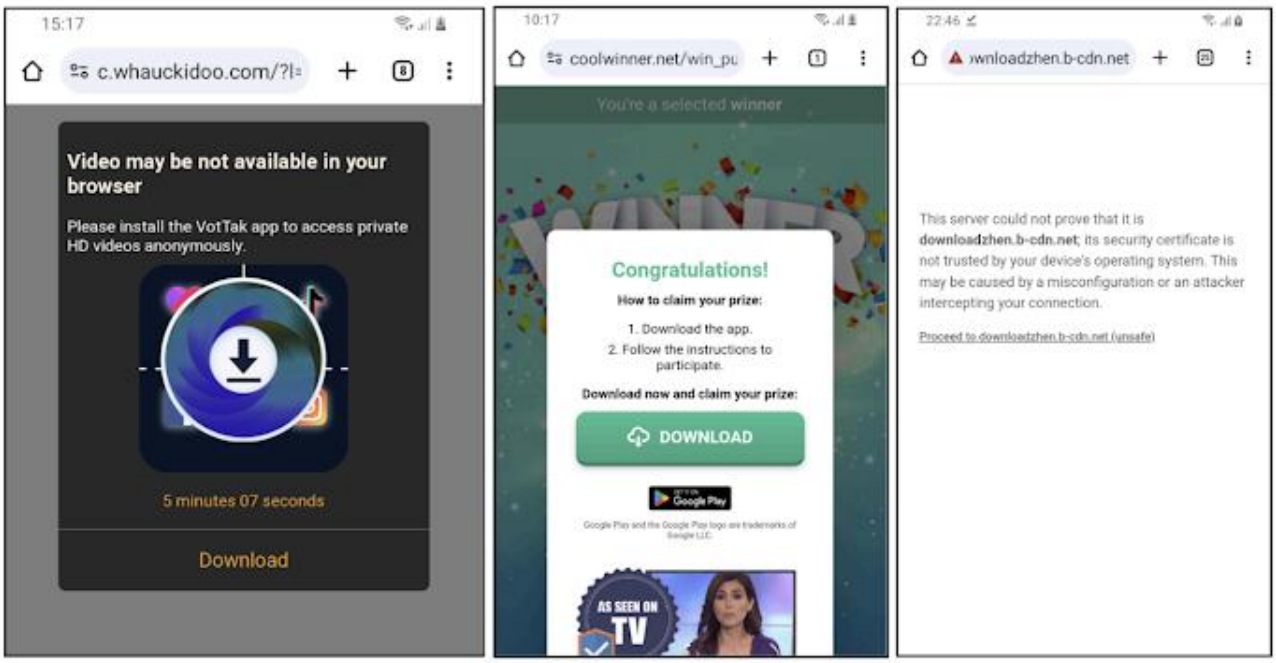
Dicho esto, no solo las aplicaciones señuelo se comportan normalmente, sino que la mayoría de ellas ni siquiera muestran anuncios. También incorporan un aviso de consentimiento de GDPR.

> *«Este mecanismo de 'señuelo/malévola' para la ofuscación es una forma novedosa*

> *para que los actores de amenazas representen el tráfico fraudulento como legítimo. En su pico, el volumen programático relacionado con Konfety alcanzó los 10 mil millones de solicitudes por día»,* dijeron los investigadores de HUMAN.

En otras palabras, Konfety aprovecha las capacidades de renderización de anuncios del SDK para cometer fraude publicitario, haciendo que sea mucho más difícil distinguir el tráfico malicioso del tráfico legítimo.

Se dice que las aplicaciones malévolas de Konfety se propagan a través de una campaña de publicidad maliciosa que promociona mods de APK y otros programas como Letasoft Sound Booster, con las URL trampa alojadas en dominios controlados por los atacantes, sitios de WordPress comprometidos y otras plataformas que permiten la carga de contenido, incluidos Docker Hub, Facebook, Google Sites y OpenSea.



Los usuarios que terminan haciendo clic en estas URL son redirigidos a un dominio que los

engaña para que descarguen la aplicación maliciosa, que, a su vez, actúa como un dropper para una primera etapa que se descifra desde los activos del archivo APK y se utiliza para configurar comunicaciones de comando y control (C2).

La etapa inicial también intenta ocultar el ícono de la aplicación de la pantalla de inicio del dispositivo y ejecuta una carga útil DEX de segunda etapa que realiza fraude al servir anuncios de video a pantalla completa fuera de contexto cuando el usuario está en su pantalla de inicio o usando otra aplicación.

> *«La clave de la operación Konfety radica en las aplicaciones malévolas. Estas aplicaciones imitan a sus correspondientes aplicaciones señuelo copiando sus ID de aplicación/nombres de paquete y IDs de publicistas de las aplicaciones señuelo»,* dijeron los investigadores.
>
> *«El tráfico de red derivado de las aplicaciones malévolas es funcionalmente idéntico al tráfico de red derivado de las aplicaciones señuelo; las impresiones de anuncios renderizadas por las aplicaciones malévolas usan el nombre del paquete de las aplicaciones señuelo en la solicitud.»*

Otras capacidades del malware incluyen aprovechar el SDK de CaramelAds para visitar sitios web usando el navegador web predeterminado, atraer a los usuarios enviando notificaciones que los incitan a hacer clic en los enlaces falsos, o cargar versiones modificadas de otros SDK de publicidad.

Eso no es todo. A los usuarios que instalan las aplicaciones malévolas se les insta a agregar un widget de barra de búsqueda a la pantalla de inicio del dispositivo, que monitorea subrepticiamente sus búsquedas enviando los datos a dominios nombrados vptrackme[.]com y youaresearching[.]com.

> *«Los actores de amenazas entienden que alojar aplicaciones maliciosas en las tiendas no es una técnica estable, y están encontrando formas creativas e ingeniosas de evadir la detección y cometer fraude a largo plazo. Los actores que configuran empresas de mediación de SDK y difunden el SDK para abusar de editores de alta calidad es una técnica en crecimiento»,* concluyeron los investigadores.