Investigadores de seguridad cibernética descubrieron una nueva vulnerabilidad no parcheada en el sistema operativo Android, que muchas aplicaciones maliciosas ya están explotando en la naturaleza para robar las credenciales de inicio de sesión bancarias y otras credenciales de los usuarios.

Strandhogg, es el nombre que se le brindó a la vulnerabilidad, que reside en la función multitarea de Android que puede ser explotada por una aplicación maliciosa instalada en un dispositivo para enmascararse como cualquier otra aplicación, incluida cualquier aplicación de sistema privilegiada.

Cuando un usuario toca el icono de una aplicación legítima, el malware que explota la vulnerabilidad Strandhogg puede interceptar y secuestrar esta tarea para mostrar una interfaz falsa al usuario en lugar de iniciar la aplicación legítima.

Al engañar a los usuarios para que piensen que están usando una aplicación legítima, la vulnerabilidad hace posible que las aplicaciones maliciosas roben convenientemente las credenciales de los usuarios utilizando pantallas de inicio de sesión falsas, como se muestra en el video.

> *«La vulnerabilidad permite a un atacante enmascararse como casi cualquier aplicación de una forma altamente creíble»,* dijeron los investigadores.
>
> *«En este ejemplo, el atacante engaña con éxito al sistema e inicia la interfaz de usuario de suplantación de identidad al abusar de algunas condiciones de transición del estado de la tarea, es decir, taskAffinity y allowTaskReparenting».*
>
> *«Cuando la víctima ingresa sus credenciales de inicio de sesión dentro de esta interfaz, los detalles confidenciales se envían inmediatamente al atacante, que luego puede iniciar sesión y controlar las aplicaciones sensibles a la seguridad».*

Además de las credenciales de inicio de sesión de phishing, una aplicación maliciosas también puede aumentar significativamente sus capacidades engañando a los usuarios para que otorguen permisos de dispositivos confidenciales mientras se hace pasar por una aplicación legítima.

> *«Un atacante puede solicitar acceso a cualquier permiso, incluidos SMS, fotos, micrófono y GPS, lo que le permite leer mensajes, ver fotos, escuchar y rastrear los movimientos de la víctima».*

Descubiertos por investigadores de la empresa de seguridad noruega Promon, los ataques de secuestro de tareas de Strandhogg son potencialmente peligrosos debido a lo siguiente:

- Es casi imposible que los usuarios seleccionados detecten el ataque
- Se puede usar para secuestrar la tarea de cualquier aplicación instalada en un dispositivo
- Se puede usar para solicitar cualquier permiso de dispositivo de forma fraudulenta
- Se puede explotar sin acceso de root
- Funciona en todas las versiones de Android
- No necesita ningún permiso especial en el dispositivo

Promon detectó la vulnerabilidad luego de analizar una aplicación troyana bancaria maliciosa que secuestró cuentas bancarias de distintos clientes en la República Checa y les robó su dinero.

Según los investigadores, algunas de las aplicaciones maliciosas identificadas, también se distribuían a través de varios cuentagotas y aplicaciones de descarga hostiles disponibles en Goole Play Store.

La compañía de seguridad móvil Lookout, también analizó la muestra maliciosa y confirmó que habían identificado al menos 36 aplicaciones maliciosas en la naturaleza, que están explotando la vulnerabilidad Strandhogg.

> *«Estas aplicaciones ahora se han eliminado, pero a pesar de la suite de seguridad Play Protect de Google, las aplicaciones cuentagotas siguen siendo publicadas y frecuentemente pasan desapercibidas, y algunas se descargan millones de veces antes de ser detectadas y eliminadas»,* dijeron los investigadores.

Promon informó la vulnerabilidad de Strandhogg al equipo de seguridad de Google este verano y reveló detalles cuando el Google no pudo solucionar el problema incluso después de un plazo de divulgación de 90 días.

Aunque no existe una forma efectiva y confiable de bloquear o detectar ataques de secuestro de tareas, los usuarios aún pueden detectar estos ataques al vigilar discrepancias como:

- Una aplicación en la que ya has iniciado sesión, solicita un nuevo inicio de sesión
- Ventanas emergentes de permisos que no contienen el nombre de una aplicación
- Permisos solicitados desde una aplicación que no debería requerir o necesitar los permisos que solicita
- Los botones y enlaces en la interfaz de usuario no hacen nada cuando se hace clic en ellos
- El botón de retroceso no funciona como se esperaba