StrandHogg, una vulnerabilidad de seguridad que afecta a Android, hace que las aplicaciones maliciosas puedan explotarla para enmascararse como cualquier otra aplicación instalada en un dispositivo objetivo para mostrar interfaces a los usuarios, engañándolos para que brinden información confidencial.

A finales del año pasado, en el momento de la divulgación pública, los investigadores también confirmaron que algunos atacantes ya estaban explotando la falla en la naturaleza para robar las credenciales de inicio de sesión de los usuarios y otras credenciales, así como para espiar sus actividades.

El mismo equipo de investigadores noruegos de seguridad cibernética reveló hoy los detalles de una nueva vulnerabilidad crítica (CVE-2020-0096), que afecta al sistema operativo Android que podría permitir a los atacantes llevar a cabo una versión más sofisticada del ataque Strandhogg.

Apodada como «Strandhogg 2.0», la nueva vulnerabilidad afecta a todos los dispositivos Android, excepto a los que ejecutan la última versión de Android Q (10), que, desafortunadamente, solo se ejecuta en el 15-2’% de todos los dispositivos Android.

Strandhogg 1.0 residía en la función multitarea de Android, mientras que la nueva falla es básicamente una vulnerabilidad de elevación de privilegios que permite a los hackers acceder a casi todas las aplicaciones.

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

Sin embargo, a diferencia de Strandhogg 1.0, que solo puede atacar aplicaciones de una en una, la última falla podría permitir a los hackers *«atacar dinámicamente casi cualquier aplicación en un dispositivo dado simultáneamente con solo tocar un botón»,* todo esto sin requerir una preconfiguración para cada aplicación objetivo.

Los defectos de StrandHogg son potencialmente peligrosos y preocupantes, ya que entre sus características se encuentran:

- Es casi imposible que los usuarios seleccionados detecten el ataque
- Se puede utilizar para secuestrar la interfaz de cualquier aplicación instalada en un dispositivo específico sin requerir configuración
- 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, excepto Q
- No necesita ningún permiso especial para trabajar en el dispositivo

Además de robar credenciales de inicio de sesión por medio de una pantalla falsa convincente, la aplicación de malware también puede aumentar de forma significativa sus capacidades engañando a los usuarios para que otorguen permisos de dispositivos sensibles mientras se hace pasar por una aplicación legítima.

> *«Utilizando StrandHogg 2.0, los atacantes pueden, una vez que se instala una aplicación maliciosa en el dispositivo, obtener acceso a mensajes de texto privados y fotos, robar las credenciales de inicio de sesión de las víctimas, rastrear movimientos de GPS, hacer y/o grabar conversaciones telefónicas y espiar a través de la cámara y micrófono»*, dijeron los investigadores.
>
> *«El malware que explota StrandHogg 2.0 también será más difícil de detectar para los antivirus y los escáneres de seguridad, y como tal, representa un peligro significativo para el usuario final»*, agregaron.

Los investigadores informaron de forma responsable la nueva vulnerabilidad a Google en diciembre del año pasado.

Luego de eso, Google preparó un parche y lo compartió con las empresas de fabricación de

teléfonos inteligentes en abril de 2020, que ahora comenzaron a implementar actualizaciones de software para sus respectivos usuarios a partir de este mes.

Aunque no existe una forma efectiva y confiable de bloquear o detectar ataques de secuestro de tareas, los usuarios todavía pueden detectar los ataques al vigilar las discrepancias que se compartieron al informar sobre StrandHogg 1.0, como:

- Una aplicación en la que ya se ha iniciado sesión, solicita otro 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