GIRONA NOTICIES.COM
+ Periodisme

Cómo evitar el ‘juice jacking’, el ciberataque del verano

Comunicados | 27/07/2023 | 00:00

La empresa S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, ha destacado que el ‘juice jacking’ se ha convertido en uno de los problemas de ciberseguridad más notorio en los últimos meses y, por eso, es necesario extremar las precauciones para evitar caer en este ciberdelito durante las vacaciones

/COMUNICAE/

La empresa S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, ha destacado que el ‘juice jacking’ se ha convertido en uno de los problemas de ciberseguridad más notorio en los últimos meses y, por eso, es necesario extremar las precauciones para evitar caer en este ciberdelito durante las vacaciones

Según ha informado la compañía española en un comunicado, el juice jacking es una técnica maliciosa que supone la manipulación de puertos USB públicos para robar datos y afectar a la seguridad de los dispositivos electrónicos de los usuarios que los utilizan. En este caso, los ciberdelincuentes instalan hardware o software en estos puertos con el objetivo de acceder a la información privada de los dispositivos conectados.

"Cuando nos conectamos a estos puertos USB que han sido manipulados, se produce una transferencia de datos no autorizada. El malware instalado en el puerto puede robar información personal, como contraseñas, números de tarjetas de crédito o datos bancarios y, junto a esto, también puede permitir a los atacantes controlar el dispositivo de la víctima de forma remota", ha afirmado Miguel A. Juan, socio-director de S2 Grupo.

Como han explicado desde la compañía, una escena muy común en vacaciones puede ser quedarse sin batería mientras se espera un vuelo en un aeropuerto. Entonces, no se encuentra ningún enchufe para cargar el smartphone, pero sí unos puertos USB disponibles. Lo que parece la solución al problema porque por fin se tendrá batería, puede suponer el inicio de un problema mayor.

Desde S2 Grupo se ha insistido en que, si bien no hay que tener miedo en el uso de las nuevas tecnologías a pesar de los ciberpeligros que aparecen, es importante conocerlos para poder protegernos adecuadamente.

En este sentido y en relación al juicie jacking, han detallado que existen 4 formas de operar:

Instalación de dispositivos fraudulentos (como un cable USB) en puertos públicos. Éstos están diseñados para extraer datos de los dispositivos conectados.

Instalación de software malicioso que infecta el dispositivo que se conecta a él. Además, este malware puede robar información o controlar el dispositivo de forma remota.

Otra forma, es con estaciones de carga falsas. Éstas parecen que están habilitadas correctamente para únicamente cargar los dispositivos pero, en realidad, están transfiriendo datos.

Por último, este tipo de ciberdelitos también están operando a través de cargadores inalámbricos.

Consejos para evitar el ‘juicie jacking" este verano:

Utilizar un cargador propio y evitar los USB públicos.

Utilizar baterías portátiles o power banks, que podrán ayudar a cargar los dispositivos en caso de emergencia.

Si se usan USB públicos, activar sólo la opción de carga y desactivar la transferencia de datos del dispositivo.

Si al conectar el dispositivo al USB, aparece en la pantalla un mensaje que pregunta si se confía en ese dispositivo, hay que contestar siempre que "NO".

Es esencial actualizar el software y antivirus de los dispositivos tecnológicos, porque actúan como escudos digitales contra las amenazas, detectando y bloqueando cualquier intento de infiltrarse en ellos.

Fuente Comunicae

Autor: Redacció

https://gironanoticies.com/comunicado/212801-como-evitar-el-juice-jacking-el-ciberataque-del-verano.htm