Investigadores en seguridad cibernética han registrado una innovadora técnica de persistencia post-explotación en iOS 16 que podría ser aprovechada para pasar desapercibida y mantener el acceso a un dispositivo de Apple, incluso cuando la víctima cree que está fuera de línea.

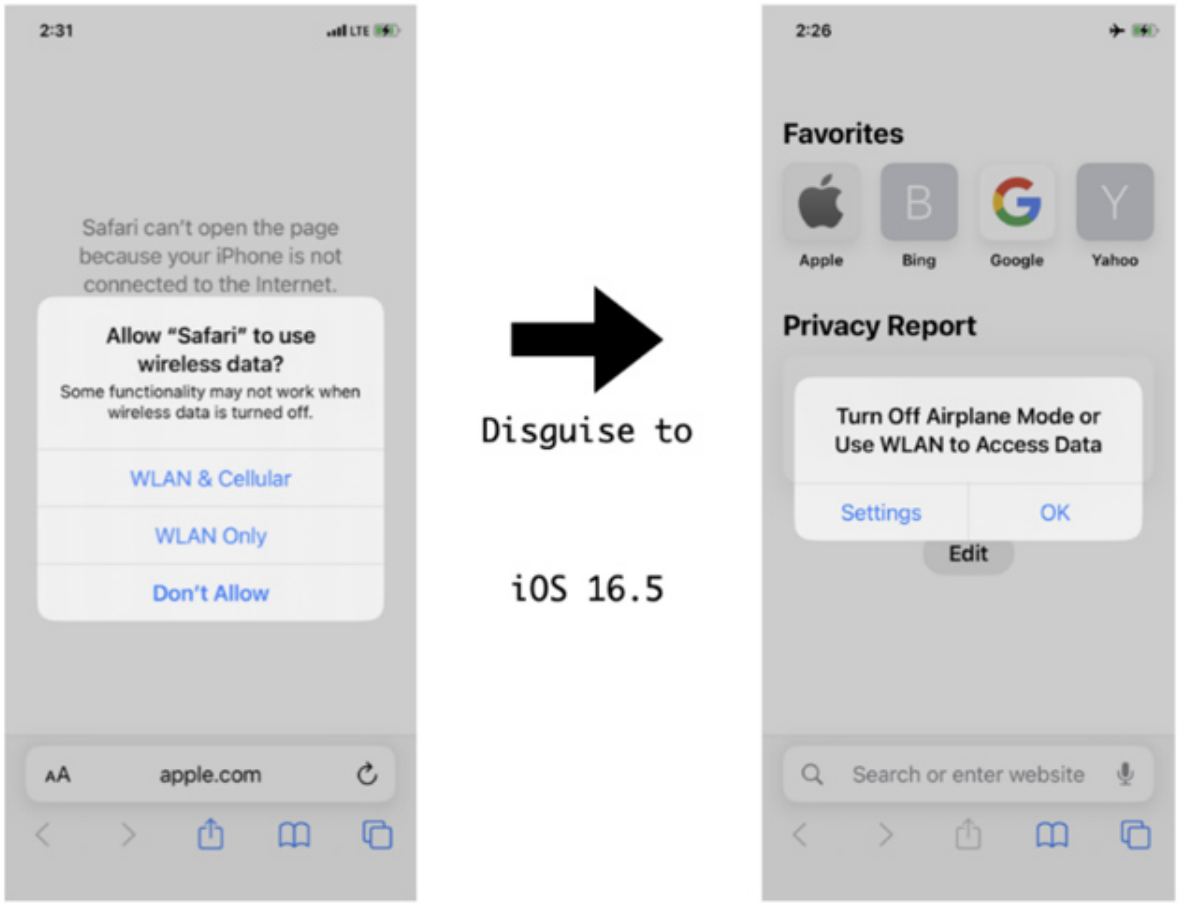
«El enfoque engaña al afectado haciéndole creer que el Modo Avión de su dispositivo funciona cuando en realidad el atacante (tras una exitosa explotación del dispositivo) ha implantado un Modo Avión falso que modifica la interfaz de usuario para mostrar el ícono del Modo Avión y corta la conexión a internet para todas las aplicaciones excepto la aplicación del atacante», señalaron los expertos de Jamf Threat Labs, Hu Ke y Nir Avraham.

El Modo Avión, como su nombre indica, permite a los usuarios desactivar las características inalámbricas de sus dispositivos, bloqueando efectivamente la conexión a redes Wi-Fi, datos celulares y Bluetooth, así como la realización de llamadas y el envío o recepción de mensajes de texto.

El método ideado por Jamf, en resumen, crea una ilusión para el usuario de que el Modo Avión está activado, al mismo tiempo que permite a un actor malicioso mantener en secreto una conexión a la red celular para una aplicación fraudulenta.

> *«Cuando el usuario activa el Modo Avión, la interfaz de red pdp_ip0 (datos celulares) ya no mostrará direcciones IP ipv4/ipv6. La red celular queda desconectada e inutilizable, al menos en el nivel del espacio de usuario»,* explicaron los investigadores.

Aunque los cambios subyacentes son realizados por CommCenter, las modificaciones en la interfaz de usuario (UI), como las transiciones de los iconos, son gestionadas por SpringBoard.



El objetivo del ataque, por lo tanto, es crear un Modo Avión ficticio que mantenga los cambios en la interfaz de usuario pero conserve la conectividad celular para una carga maliciosa instalada en el dispositivo mediante otros medios.

> *«Después de habilitar el Modo Avión sin conexión Wi-Fi, los usuarios esperarían que al abrir Safari no haya conexión a Internet. La experiencia habitual es una ventana emergente que insta al usuario a 'Desactivar el Modo Avión'»,* comentaron los investigadores.

Para llevar a cabo el engaño, se utiliza el daemon CommCenter para bloquear el acceso a los datos celulares de aplicaciones específicas y simular el Modo Avión mediante una función modificada que altera la ventana de alerta para que parezca que se ha activado la configuración.

Es importante señalar que el núcleo del sistema operativo notifica al CommCenter a través de una rutina de llamada de retorno, que a su vez notifica a SpringBoard para mostrar el mensaje emergente.

Un análisis más profundo del daemon CommCenter también ha revelado la existencia de una base de datos SQL que se emplea para registrar el estado de acceso a los datos celulares de cada aplicación (conocida como ID de paquete), con una señal configurada en el valor «8» si se bloquea el acceso de una aplicación.

> *«Utilizando esta base de datos de IDs de paquete de aplicaciones instaladas, ahora podemos bloquear o permitir selectivamente que una aplicación acceda a Wi-Fi o datos celulares utilizando el siguiente código»,* indicaron los investigadores.

> *«Cuando se combina con las otras técnicas descritas anteriormente, el Modo Avión falso ahora parece funcionar de manera idéntica al real, excepto que la prohibición de acceso a internet no se aplica a procesos que no son aplicaciones, como un troyano de puerta trasera».*