BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
Agencia de Sistemas

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

BLUEJACKING:
OTRA FORMA DE ENVIAR SPAM

BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
Agencia de Sistemas

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

¿QUÉ SIGNIFICA "BLUEJACKING"?

Es un método que **permite enviar mensajes dañinos, anónimos y no deseados entre equipos conectados a través de la red Bluetooth** (como pueden ser los teléfonos celulares, computadoras portátiles, PDAs, etc.), dentro de un radio determinado.

El término nace de una anécdota que cuenta que, en una oportunidad, un hombre llamado "Jack" se encontraba en un banco con un dispositivo móvil intentando comunicarse con otros que dispusieran de Bluetooth. En sus intentos, finalmente logró entablar comunicación con un móvil de marca Nokia modelo 7650, al cual le envió un mensaje que decía: "Buy Ericsson" ("Comprate un Ericsson"). Este humorístico episodio fue definido por Jack como "Bluejacking" y, a partir de allí, se implementó tal denominación para referirse a este tipo de actividad.

Si bien suele ser tomado como un hecho inofensivo, ya que **las personas que realizan Bluejacking no pueden acceder a la información personal de sus víctimas**, lo cierto es que puede convertirse en un evento dañino si mediante el mensaje enviado se introduce un virus en el dispositivo.

No hay que confundir "*Bluejacking*" con "*Bluesnarfing*". Éste último, va más allá de un simple envío de mensajes entre dispositivos, dado que permite a un atacante descargarse (e incluso eliminar) los contactos, el listado de llamadas recibidas/ realizadas, los SMS enviados, etc., sin dejar rastro alguno.

Recordá desactivar siempre el Bluetooth cuando no esté siendo utilizado.

BLUEJACKING GENERALMENTE ES INOFENSIVO, PERO LAS PERSONAS QUE SUFRIERON UN BLUEJACKED NO SABEN MUY BIEN QUÉ OCURRIÓ EN SU CELULAR Y PIENSAN QUE EL TELÉFONO ESTA FUNCIONANDO MAL.

¿QUÉ ES BLUETOOTH?

Se denomina Bluetooth al protocolo de comunicaciones diseñado especialmente para dispositivos de bajo consumo que requieren corto alcance de emisión y se basan en transceptores de bajo costo. Los dispositivos que incorporan este protocolo pueden comunicarse entre sí cuando se encuentran dentro de su rango de alcance y las comunicaciones establecidas se realizan por radiofrecuencia.

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

¿CÓMO FUNCIONA?

La tecnología Bluetooth opera usando ondas de radio de baja potencia que se comunican en una frecuencia de 2.4 gigaherzios. Dicha frecuencia especial es también conocida como banda ISM, una banda sin licencia apartada de los dispositivos médicos, industriales o científicos. Cuando un número de dispositivos de bluetooth son encendidos en la misma área, comparten la misma banda ISM y pueden localizarse y comunicarse entre ellos como si fueran radios comunicadores sintonizados en la misma frecuencia.

1. Poniendo un dispositivo bluetooth en modo de descubrir otros equipos, los usuarios pueden encontrarse y contactarse.

2. Los atacantes se aprovechan de esta habilidad para interactuar con otros teléfonos y enviar mensajes de texto, tarjetas de negocios, etc.

3. El atacante explora su entorno con un dispositivo compatible con la red Bluetooth a la búsqueda de otros dispositivos conectados en la misma red.

4. Luego, éste envía un mensaje no solicitado a los dispositivos conectados.

Si bien el límite de la tecnología Bluetooth permite una comunicación limitada de sólo 10 metros entre los dispositivos (normalmente en dispositivos pequeños como son los teléfonos celulares), en ciertos casos, como sucede con las computadoras portátiles (transmisores más potentes), puede alcanzar los 100 metros.

Sin embargo, el bluejacking es impreciso. Buscar otros dispositivos hardware con bluetooth puede mostrar una lista de dispositivos etiquetados con una serie de nombres y letras. A menos que el dispositivo objetivo haya elegido dejar mostrar su identidad o sea el único dispositivo en toda el área, puede ser complicado saber a quién mandar el mensaje con tantos códigos difíciles de identificar.

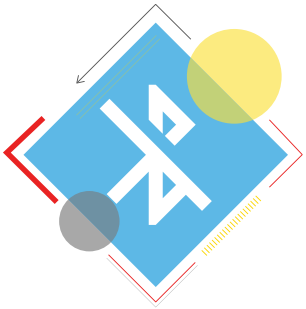
+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

¿CÓMO PREVENIRLO?

Para realizar Bluejacking, aquellos usuarios malintencionados se valen de una serie de herramientas de software que han sido desarrolladas para ello, como: Bluetooth Messenger o el famoso Mobiluck.

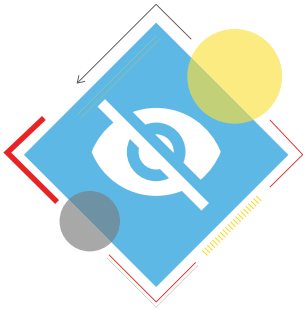
En el caso de los teléfonos celulares, que suelen ser los dispositivos más vulnerables, pueden prevenirse este tipo de ataques de manera sencilla.

EJEMPLOS:



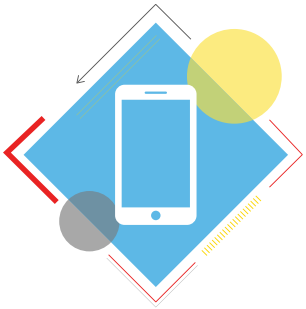
APAGAR

Recordar siempre **desactivar** la funcionalidad de Bluetooth **cuando no esté siendo utilizada**.



CONFIGURAR

Configurar el dispositivo en **"modo oculto"** con el objetivo de que, al activar Bluetooth, no sea visible para otros equipos que se encuentren cerca.



PROTEGERSE

Cuando compramos un nuevo dispositivo, tratar de que trabaje con seguridad de **Bluetooth del Modo 2** que es una seguridad reforzada a nivel de servicio; a los fines de estar protegido de forma automática.

REFERENCIAS:

1. https://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Bluejacking-el-gran-peligro-de-Bluetooth.php
2. https://eduardoarea.blogspot.com.ar/2013/02/que-es-el-bluejacking.html
3. http://www.ordenadores-y-portatiles.com/bluejacking.html