

iPhone, cómo secuestrar un iPhone en tres pasos

La seguridad de los dispositivos móviles está en entredicho, y mucho se ha hablado de las carencias de los teléfonos móviles de Apple en este aspecto.

Dos investigadores del Mobile Security Lab acaban de demostrar lo sencillo que es secuestrar un iPhone. Se trata de Roberto Gassira y Roberto Piccirillo. Todo lo que hace falta es el número del teléfono móvil de la víctima, una pieza de software gratuita denominada iPhone Configuration Utility, y un servidor proxy con software Apache. El número de teléfono del móvil de la víctima sirve para averiguar a qué operador pertenece. Esto es necesario porque cada operador utiliza unos parámetros de red específicos que el atacante debe conocer. El segundo paso es crear un fichero .mobileconfig (para reconfigurar la terminal) utilizando la utilidad gratuita antes mencionada, disponible en el sitio web de Apple. La misión de ese fichero es desviar el tráfico de navegación HTTP y HTTPS a un servidor proxy malicioso que controla el hacker. En tercer lugar, hay que conseguir engañar al usuario para que lo instale en su propia terminal, evitando que se disparen las alertas. Los investigadores Gassira y Piccirillo han descubierto un método para lograrlo: enviar un mensaje corto (SMS). El atacante simula que el mensaje procede de la compañía de móviles o de un empleado para convencer al usuario de que descargue e instale el nuevo fichero .mobileconfig. Estos dos investigadores demostraron que es posible evitar el proceso de verificación, e instalar la nueva configuración sin que salte ningún aviso de falta de autenticidad. Este método de secuestrar conexiones móviles de datos no sólo funciona con el iPhone, sino que también es aplicable a otros dispositivos de Apple como iPod e iPad, e incluso a dispositivos con sistema operativo Android. El modo de evitar un ataque como éste es instalar la última versión del sistema operativo para iPhone, el iOS 4; además hay que bloquear el perfil de la configuración del teléfono para que no pueda ser sustituido por otro malicioso. PUBLICADO: 16 de julio, 2010 / FUENTE: tuexperto.com / FOTOS: tuexperto.com