EL MERCURIO

Fecha: 28/08/2025 Audiencia: 320.543 Sección: ECONOMIA
Vpe: $6.606.292 Tirada: 126.654 Frecuencia: SEMANAL
Vpe pág: $20.570.976 Difusión: 126.654
Vpe portada: $20.570.976 Ocupación: 32,11%

Gran Bretaña: Fabricantes versus delincuentes

Cómo los ladrones pueden entrar a su auto

Bandas piratean sistemas electrónicos con equipos cada vez más sofisticados.

Imagine encontrarse con un ladrón de autos británico experimentado en 2013. Probablemente habría dado lástima. Cada año de su carrera, el oficio se había vuelto más difícil. Las herramientas de su trabajo —como una percha o un "slim jim" (una lámina metálica plana) para forzar cerraduras, y los pelacables para manipular los conductores de encendido— habían quedado obsoletas, poco a poco, gracias a la mejora de la tecnología de seguridad. El negocio estaba extinto.

Ya no. El reciente auge del robo de autos muestra un campo de batalla en constante cambio. De un lado están los fabricantes, que producen y venden autos. Del otro, los ladrones, que intentan robárselos. A medida que la tecnología para brindar seguridad (y vulnerarla) se ha vuelto más eficaz y barata, la lucha se ha acelerado.

Los autos modernos a veces se llaman "computadores sobre ruedas". Eso trajo beneficios, pero también vulnerabilidades que los fabricantes tardaron en dimensionar. La primera fue el "*relay attack*" o ataque de retransmisión, que se hizo popular en Gran Bretaña en 2016, tras la introducción del encendido sin llave. Un ladrón se coloca en la calle y usa un dispositivo para "rebotar" la señal electrónica desde la casa hasta el auto.

Los fabricantes ya diseñaron soluciones contra eso en modelos más nuevos. Hoy los ladrones suelen entrar conectando un dispositivo directamente a uno de los componentes electrónicos del vehículo, engañándolo para que crea que lo contacta una llave inteligente. Adam Gibson, policía en el puerto de Felixstowe, señala varios autos recuperados que fueron vulnerados con esta técnica: uno a través de la luz trasera y otro mediante una pieza junto al pestillo del capó.

EFE.

El reciente auge del robo de autos muestra un campo de batalla en constante cambio. De un lado están los fabricantes, que producen y venden autos. Del otro, los ladrones, que intentan robárselos.

The Economist
DERECHOS EXCLUSIVOS

El equipo necesario se puede comprar fácilmente en línea. Incluso hay videos en YouTube que explican cómo usarlo. La mayoría de los robos son obra de grupos criminales organizados, dispuestos a invertir hasta £20.000 (US$ 27.000) en un solo aparato. Una fuerza policial contó que, cuando confiscó uno de estos dispositivos, solo consiguió un par de semanas en paz.

Un desafío para los fabricantes es la rapidez de la innovación criminal. El diseño y la producción de un auto toman años; una vez que los grupos descubren un punto de entrada, pueden tener años de negocio fácil. Otro obstáculo es el costo. En la gama alta, las marcas invierten fuerte en corregir vulnerabilidades, en parte porque temen que una ola de robos dañe su prestigio. En los autos de gama media, la competencia de precios es más feroz y los conductores son menos propensos a culpar al fabricante si les roban el vehículo.

Los criminales también han debido adaptar sus técnicas en el caso de los teléfonos. La introducción del bloqueo biométrico y del reconocimiento facial dificultó el acceso a aparatos bloqueados, volviéndolos menos valiosos. La respuesta fue un aumento de los "robos por arrebato": los ladrones arrancan de la mano un teléfono desbloqueado y deshabilitan el rastreo antes de que la víctima pueda reportarlo.

Los fabricantes, a su vez, han desarrollado medidas de detección basadas en movimiento (el teléfono se bloquea ante un tirón brusco) y protección de dispositivos robados (exige un código al moverse a un lugar desconocido). Sin embargo, la seguridad de cualquier sistema depende de usted. Muchos usuarios no activan esas funciones. Los delincuentes se han hecho expertos en *phishing* para conseguir la información personal necesaria para desbloquear un teléfono. Y, si todo falla, siempre se puede vender un aparato bloqueado por partes.

A los fabricantes a menudo se les acusa de lentitud. Parlamentarios británicos han sostenido, por ejemplo, que Apple podría socavar con facilidad el modelo de negocio de los ladrones de celulares introduciendo un "*kill switch*" (interruptor de apagado total), pero que no lo hace por "fuertes incentivos comerciales". Eso simplifica demasiado las cosas. Los fabricantes diseñan la seguridad en torno a contraseñas y bloqueos, y ya permiten a los usuarios "matar" su teléfono de forma remota cuando está bloqueado. Introducir un *kill switch* para un equipo que parece haberse transferido legítimamente a un nuevo usuario abriría una serie de problemas. Un vendedor de segunda mano, por ejemplo, podría intentar extorsionar a un comprador amenazando con desactivar el celular después de la venta. Los fabricantes tendrían serias dificultades para diseñar un proceso infalible que distinguiera entre robos y ventas legales.

Una conclusión más justa es que —como sus costos se socializan a través de primas de seguro más altas— el robo es a menudo un problema que nadie tiene un incentivo fuerte para resolver.

Artículo traducido por Economía y Negocios de "El Mercurio".