



El aparato, llamado jammer, también impidió el funcionamiento de las cámaras corporales de los agentes

Arrestan a chileno en Estados Unidos por usar dispositivo que bloquea comunicaciones de la policía

El joven de 22 años fue detenido en Texas cuando intentaba robar una vivienda. Llevaba pocos meses en el país y residía en un hotel.

IGNACIO MOLINA

La detención del chileno Ignacio Castillo en Houston, Texas, presenta un giro poco común en los delitos de robo residencial. A diferencia de los asaltantes tradicionales, el joven de 22 años fue arrestado no solo por irrumpir en una vivienda, sino por emplear un dispositivo de interferencia de radiofrecuencia que afectó las comunicaciones policiales, llamado jammer.

El incidente ocurrió en Sewanee Avenue, una zona residencial donde, según el Houston Police Department, Castillo ejecutó el robo con tecnología que bloqueó las señales de radio de los oficiales que respondieron a la emergencia. Este dispositivo también impidió el funcionamiento de las cámaras corporales de los agentes y sus radios portátiles, según el reporte de Fox News (disponible, en inglés, en este enlace: <http://bit.ly/4k6xlq8>).

El uso de un inhibidor de frecuencia representó un problema grave para la policía, ya que afectó su capacidad de respuesta. Kim Ogg, exfiscal del condado de Harris, señaló a los medios que la posibilidad de que un delincuente interfiriera con las comunicaciones oficiales "es extremadamente preocupante". Aunque el acceso a estos dispositivos está restringido en Estados Unidos, su uso en actividades criminales ha sido documentado en otros estados, principalmente en robos de autos.

Castillo compareció ante la corte para una audiencia de causa probable, donde reconoció no ser ciudadano estadounidense y haber estado en Houston durante los últimos meses, con residencia en un hotel. Quedó bajo custodia mientras las autoridades investigan el caso



La imagen, difundida por Fox News, muestra al chileno de 22 años arrestado en Houston.



Un aparato similar a éste tenía en su poder el chileno, de 22 años.

Cómo funciona

Gabriel Bergel, máster en Ciberseguridad y CEO de la 8.8 Computer Security Conference, explica que un dispositivo de interferencia de radiofrecuencia, conocido como jammer, interrumpe las comunicaciones al interferir con las frecuencias utilizadas por los sistemas de comunicación. "Generan ruido electromagnético en las bandas de frecuencia utilizadas por las redes celulares (GSM, 3G, 4G, 5G). Este ruido satura el espectro radioeléctrico, impidiendo la comunicación efectiva", detalla.

Nicolás Silva, máster en Tecnologías de la Información, lo sintetiza así: "Es como si en una conversación normal alguien empezara a gritar muy fuerte para que nadie más pueda escucharse".

Estos dispositivos cuentan con varios elementos técnicos que les

permiten operar, entre ellos un oscilador de frecuencia; un amplificador de radiofrecuencia (RF) y un generador de ruido. Cada uno cumple funciones específicas en la interceptación.

Vulnerabilidad

Según Nicolás Silva, director de Tecnología de Asimov Consultores, algunas frecuencias resultan más sensibles a este tipo de interferencia que otras. "Las más vulnerables suelen ser las frecuencias utilizadas por sistemas de seguridad y comunicación crítica, como las bandas de VHF y UHF, que usan los servicios de emergencia y las fuerzas de seguridad. Estas bandas resultan especialmente vulnerables porque suelen operar con señales de baja potencia y sin cifrado fuerte, lo que facilita su interferencia. Además, las antenas y dispositivos que usan estas frecuencias suelen estar diseñados para captar señales débiles en entornos urbanos, lo que los hace sensibles a transmisiones más fuertes o deliberadamente disruptiva", detalla.