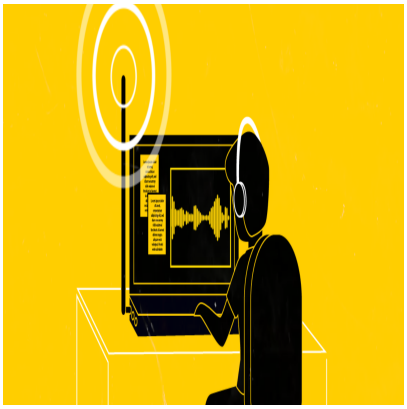

En estos puntos rojos tu celular es un libro abierto

Descripción

En su crecimiento irregular y desordenado, Caracas se ha transformado de varias formas. Una de ellas se nota directamente en el verdor de los cerros que la rodean, rasgado por arañazos marrones y grisáceos en los que despuntan unas enormes estructuras metálicas que concentran la transmisión de las señales de todos los teléfonos celulares en un radio de 35 kilómetros en esta capital que es, a la vez, hogar de cuatro millones de personas.

Este semillero de antenas telefónicas se extiende por el resto del país indicando que existe algún progreso tecnológico, aunque irregular, en un circuito sobrecargado. Pero no todas son de la envergadura de las torres metálicas ni actúan de la misma forma. Existen dispositivos muy discretos llamados IMSI Catchers -también conocidos como Stingrays o Triggerfish- muy difíciles de detectar a simple vista y que trabajan como antenas portátiles que pueden llegar a ocultarse en el clóset de una casa o en la parte trasera de un camión, con un botón de encendido y apagado tan accesible que pueden pasar fácilmente inadvertidas.

Desde luego, estos aparatos sirven para la vigilancia electrónica. Tienen la capacidad de actuar como pequeñas repetidoras, como si fueran una operadora telefónica, interceptando la señal móvil de los teléfonos que se encuentran en un área de un kilómetro a la redonda o de un solo aparato específico si conocen sus detalles. Lo demás es invisible: esta tecnología permite la lectura de los mensajes que llegan a los móviles, escuchar las llamadas y localizar exactamente su ubicación. Los datos personales que se cuidan con tanto celo quedan expuestos.

Armando.info tuvo acceso a un informe elaborado por la organización South Lighthouse -dedicada a investigar tecnologías al servicio de los derechos humanos- en un estudio denominado FADe Project, por sus siglas en inglés (*Fake Antenna Detection Project*). En julio de 2020 publicaron los primeros hallazgos luego de un monitoreo continuo llevado a cabo en Caracas, entre marzo y mayo de 2019, al que luego sumaron otros casos. Estos evidencian la actividad de, al menos, 80 antenas irregulares en Venezuela, algunas de ellas sospechosas, por su comportamiento y ubicación, de ser en realidad IMSI Catchers.

El informe de FADe Project no solo muestra lo que puede constituir una puerta trasera a las

comunicaciones venezolanas, sino un peligro latente por el que quedan en riesgo la privacidad y seguridad de los ciudadanos en el marco de un Estado con vocación de fisgón. El envejecimiento de la red de telefonía, la escasa oferta de empresas proveedoras, las restricciones estatales, la falta de una ley que regule el uso indebido de información, y la casi segura adquisición de tecnología para espiar, pintan un escenario ideal de riesgos para la información privada.

Aunque todas las compañías que ofrecen servicios de telefonía celular en Venezuela fueron consultadas para este reportaje, solo Digitel aseguró a través de su oficina de Comunicación Externa que no tienen información y desconocen "la existencia de antenas repetidoras falsas". "Sin embargo", prosiguen, "puede haber enlaces de terceros que operan en la banda asignada a Digitel, representando así interferencia para nuestra red, lo cual afecta la calidad del servicio que prestamos. Cuando detectamos esto recurrimos al ente regulador Conatel (Comisión Nacional de Telecomunicaciones) para que este organismo realice las gestiones correspondientes con terceros y se proceda al retiro de estos enlaces".

Conatel es quien asigna las bandas, otorga las licencias y supervisa todo cuanto ocurre en el espectro eléctrico.

La antena "loca"

La icónica Plaza Venezuela, ubicada en el centro geográfico de la capital venezolana es, por eso mismo, una encrucijada de caminos con acceso a distintos puntos de la ciudad. Además de la fuente con luces multicolores que se encienden en sus múltiples reinauguraciones -y quizás en alguna festividad decembrina-, también es el sitio de una de las antenas que más suspicacias despierta entre los investigadores del estudio.

"Algunas mediciones encajan en la hipótesis de que se trata de un equipo de vigilancia con una configuración errónea por un período breve de tiempo", explican Andrés Alärkhon-Schiavi, coordinador de FADe Project y, Carlos Guerra, encargado técnico del proyecto. Ambos aclaran que revisan unos 340 parámetros técnicos para determinar las anomalías y que, cuando consiguen una que sale de la norma, sin justificación aparente, la antena se marca como sospechosa.

En este caso, la precisión del monitoreo ubicó el dispositivo en la Zona Rental, a unos 350 metros de distancia de la fuente de Plaza Venezuela. Fue avistada una sola vez durante los tres meses de barrido constante por el lugar, y su repentina aparición a las 9:03 de la noche, del 11 de mayo de 2019, fue más que sorpresiva: su señal no estaba asociada a ninguna de las tres proveedoras telefónicas que existen en el país -las privadas Movistar y Digitel, o la estatal Movilnet- y no tenía registrado un código de país válido. Una verdadera antena fantasma.

Como mínimo, estas dos variables (asociación con una teleoperadora y un código de discado directo) deben estar presentes para que una torre telefónica funcione de manera normal. Si presenta un error en la transmisión de los datos, lo esperado es que sean valores que existen en la realidad.

“El punto de interés potencial, según el mapa, podría ser las instalaciones del Servicio Bolivariano de Inteligencia”, o Sebin (policía política del chavismo), cuya sede se encuentra en las cercanías de la Plaza Venezuela, según explican los expertos de FADe Project. Sin embargo, esto no es concluyente, ni se pudo comprobar la existencia de estos dispositivos en manos de los agentes de inteligencia.

De acuerdo con los cálculos de los expertos, un dispositivo IMSI Catcher en esta zona abarcaría como máximo unos 800 metros alrededor del punto de medición, un radio que incluye las instalaciones del Sebin. Sería una inmensa ola invisible que arroparía todo: hoteles, edificios con más de 20 pisos (residenciales y comerciales), oficinas gubernamentales, despachos de abogados, estaciones de metro, centros financieros, restaurantes, centros comerciales, consultorios médicos. Un solo IMSI Catcher podría recoger y capturar los datos de todos los teléfonos celulares de gran parte del bulevar de Sabana Grande en dirección noreste, aquellos que están casi llegando a la principal de la avenida Maripérez en dirección noroeste y alcanzar una parte de Colinas de Bello Monte, en el sureste.


armando.info

Tanto el Servicio Bolivariano de Inteligencia Nacional (Sebin), como la DGCIM, cuentan con equipos para hacer seguimiento e intervención telefónica, asegura Iván Simonovis. Crédito: Ronaldo Schemidt / AFP

El experto tecnológico Cooper Quintin, de la organización Electronic Frontier Foundation (EFF), que ha trabajado varios años en la detección de IMSI Catcher, comenta a Armando.info que estos dispositivos “podrían ser capaces de alcanzar precisión solamente con información del número de teléfono y a través de la operadora telefónica rastrear en el área de una cuadra”. Esto es posible porque las compañías telefónicas en todo el mundo, y en Venezuela es una exigencia obligatoria, deben registrar los datos de las personas que compran una línea móvil y anotar el código IMSI, por sus siglas en inglés (*International Mobile Subscriber Identify*) que está asociada a la SIM card.

Aunque sin entrar en especificaciones técnicas, al ser consultado sobre la posible vigilancia a través de estos equipos, Iván Simonovis, comisionado de Seguridad e Inteligencia del gobierno interino de Juan Guaidó, alertó que las oficinas dependientes del Sebin y de la Dirección de Contrainteligencia Militar (Dgcim), en manos de Nicolás Maduro, “tienen la tecnología y hacen trabajo de seguimiento e intervención de teléfonos”. Puntualiza diciendo que “el monitoreo de celulares es de los objetivos que consideran, según el caso”, que casi siempre son figuras de la actividad política.

Simonovis explica que “cuando existe una investigación abierta que amerita información sobre un número o suscriptor, las operadoras telefónicas están obligadas a facilitar los datos a los órganos jurisdiccionales: a quién pertenece, las torres donde ha abierto, el movimiento que ha tenido”. El ex preso político, que escapó del Sebin mientras cumplía arresto domiciliario, precisa que el problema principal es lo que terminan haciendo con esa información.

Digitel respondió sobre este particular señalando que “se manejan de acuerdo a la normativa legal vigente y bajo un lineamiento de confidencialidad. Todas las empresas que operan en Venezuela deben colaborar y dar respuesta a cualquier solicitud de su ente regulador (Conatel), siempre que sea solicitada dentro de una investigación penal, por Fiscalía y Tribunales, y se cumplan con los extremos de ley”.

Autopista por el hombrillo

Uno de los hallazgos más recientes de FADe Project fue la identificación de 26 antenas sospechosas a la vera de la autopista El Valle-Coche. Es uno de los accesos más importantes a Caracas desde los estados industriales del centro del país (Miranda, Aragua y Carabobo) y es una vía rápida de 16 kilómetros, con seis canales (ida y vuelta) que se conecta en distintos puntos con las alcabalas militares que dan acceso al complejo militar Fuerte Tiuna y al Paseo Los Próceres.

La mitad de estas antenas sospechosas fueron asociadas con la operadora Movistar y la otra mitad con la estatal Movilnet, y cambiaron de valores de manera irregular durante cinco de los 29 días que fueron monitoreadas. Aunque se registraron parámetros fuera de lo normal por varios días, el 24 de abril de 2019 fue una jornada que rompió completamente los estándares. El reporte de actividad parecía un sismógrafo haciendo pulsaciones a la máquina de monitoreo que registró, entre las 8:53 hasta las 11:43 de la noche de ese miércoles, 21 antenas con irregularidades, algunas conactividades tan breves como un minuto y otras con valores fuera de lo común por períodos de hastados horas.

Al día siguiente, vino la calma y solo se pudieron comprobar seis antenas sospechosas. Durante el tercer día de ese sismógrafo irregular, viernes 26 de abril, prácticamente cesó todo y solo se registraron dos antenas con irregularidades.

Hasta la fecha no hay evidencia que vincule estas actividades sospechosas que tuvieron las antenas con lo que ocurrió cuatro días después, el martes 30 de abril de 2019 en horas de la madrugada, cuando el líder opositor Juan Guaidó llegó al distribuidor Altamira en Caracas, frente a la Base Aérea Francisco de Miranda de La Carlota y, acompañado por su compañero de partido y hasta ese día bajo prisión domiciliaria, Leopoldo López, fundador de Voluntad Popular y preso político desde 2014. Fue el inicio de un intento de levantamiento cívico-militar que a las pocas horas quedó sofocado.

A diferencia de la antena *loca* de Plaza Venezuela, las torres telefónicas irregulares de la autopista El Valle-Coche sí tenían identificación de país y de operadoras, pero las “órdenes” que le daban a los celulares eran otras. Por ejemplo, la torre sospechosa le indicaba a los teléfonos cercanos que podían "usar conexiones GPRS” porque no había redes más veloces disponibles, aunque en realidad sí las hubiera. En términos sencillos, era como decirle a un Maserati o a un Porsche que circulara por el hombrillo, mientras los otros canales de la autopista estaban libres. Los celulares eran engañados por la torre para pegarse a una red 2G, cuya posibilidad de vulneración es aún mayor.

A los expertos de FADe Project les llamó la atención que estas antenas sospechosas de los alrededores de Fuerte Tiuna “forzaran a los teléfonos” a que usaran redes 2G cuando existe disponibilidad de 3G y 4G para la navegación. Esta es uno de los indicios típicos de la acción de los IMSI Catchers, porque mientras más vulnerable la red, mayor acceso se tiene a la información disponible en el celular.

Se le consultó a la empresa Telefónica de Venezuela sobre la existencia de antenas sospechosas que operan como Movistar, pero no dio respuesta a la solicitud de información. El equipo de expertos de FADe Project observó, entre otras irregularidades, que antenas de Movistar Venezuela aparecieron como ubicadas en Cúcuta, Colombia.

Nicolás Maduro suscribió nuevas alianzas con Xi Jinping en 2019 para ampliar las redes de telefonía en Venezuela. Crédito: Andy Wong / POOL / AFP

La Comisión Nacional de Telecomunicaciones (Conatel) es quien otorga las licencias y supervisa todo cuanto ocurre en el espectro eléctrico. Crédito: Andrew Álvarez / AFP

La estatal Comisión Nacional de Telecomunicaciones (Conatel) registraba, para 2018, más de 16 millones de usuarios de telefonía móvil en Venezuela, que se conectaban por GSM (redes lentas), y solo 2,5 millones por LTE (redes 4G). A mediados de 2019, Nicolás Maduro sorprendió con sus declaraciones de expandir “de manera experimental” las redes 5G para la telefonía móvil apoyándose en sus aliados chinos. Pocos meses antes, en mayo de ese año, había invitado a las empresas rusas para que “hicieran realidad una red 4G” en el país.

Los años de congelamiento de las tarifas celulares y el control del Estado sobre las telecomunicaciones han impactado el funcionamiento de las redes instaladas. La red 4G en

Venezuela solo está disponible de manera limitada para centros urbanos del interior del país y Caracas. A pesar de ello, tanto Movistar, marca del gigante empresarial español Telefónica -que recientemente anunció su intención de vender todo su negocio en América Latina, con la excepción de Brasil y en México, donde alcanzó una alianza estratégica con la estadounidense AT&T- y que controla más del 40% del mercado venezolano de suscriptores de telefonía móvil, como Digitel, la otra operadora privada, que tiene un poco más de 10%, han tratado de hacer algunas inversiones para mejorar su tecnología y expandir sus redes en el país. La estatal Movilnet, que tiene un poco más de 35% del mercado, también ha hecho lo suyo.

De acuerdo a la información suministrada por Digitel, sigue atendiendo las necesidades de comunicación de sus clientes en redes 2G y 3G, que son las más vulnerables, y estiman una expansión 4G para finales de 2020. En Caracas tiene 100% de cobertura 3G y han expandido la red 4G, sobretodo hacia la zona sureste de la ciudad, aunque las antenas todavía pueden conectarse en 2G.

Sin plan de vuelo

Los 90 días de monitoreo permitieron identificar también antenas sospechosas fuera de Caracas. Las singularidades se fueron haciendo más grandes y, entre marzo y mayo de 2019, el estudio detalló presencia de torres telefónicas con actividad irregular en los principales aeropuertos que sirven a la capital de Venezuela: el internacional de Maiquetía, ubicado en el litoral central de La Guaira; el Caracas Oscar Machado Zuloaga, en Charallave, que se encuentra a unos 40 kilómetros de la capital y el Metropolitano, en Ocumare del Tuy, que está a casi 70 kilómetros.

Particularmente en los dos últimos, las antenas sospechosas estaban en las entradas de las instalaciones. De acuerdo con las observaciones del equipo de FADe Project, “aunque la mayoría de los parámetros anómalos no resultan decisivos en la ejecución de vigilancia telefónica, son sospechosamente diferente al resto de la red, aún más en Movistar”. Aún cuando no se puede afirmar la existencia de un dispositivo IMSI Catcher, las operaciones de la antena detectada son irregulares y, por lo tanto, arriesgan a quien se conecte con esa red.

El Aeropuerto Metropolitano, en los valles del Tuy, recibe vuelos privados y tiene un ingrediente extra del cóctel de anomalías. La antena sospechosa que se encuentra en ese lugar da instrucciones a todos los celulares cercanos de que está inhabilitada o bloqueada para conectarse, aún cuando existen las redes. Es tanto como decir que la misma operadora telefónica, interesada en atender a sus suscriptores, emite la instrucción de cancelar el servicio. Este caso fue único en el país y, particularmente poco común en los otros países, México y Bolivia, donde se realizó el estudio. El registro ubicó la anomalía el 15 y 24 mayo, así como el 16 de julio del año pasado.

Para cerciorarse, los expertos de FADe Project consultaron a los investigadores de seguridad de SeaGlass, de la Universidad de Washington -creadores de la metodología de monitoreo-, quienes advirtieron las incongruencias y su hipótesis es que esta actividad de la antena busca aislar a las personas.

Tanto el Aeropuerto Caracas como el Metropolitano, ambos en el estado Miranda, están bajo el control administrativo y operacional de la administración de Maduro. Tal vez no fuera coincidencia que en mayo de 2019 -el mes de la actividad inusual de la antena a la entrada del Aeropuerto

Metropolitano-, efectivos de los distintos cuerpos de seguridad del Estado tomaron las instalaciones, evaluaron los hangares y los talleres, así como los sistemas de control para la salida de aeronaves, pilotos y pasajeros, de acuerdo con la información oficial difundida en el momento.

El peso omnipresente

Hablar de IMSI Catchers es como “tratar de describir a un fantasma, que te asusta porque te abre y cierra la puerta, pero es difícil de explicar”, describe el experto Cooper Quintin, de Electronic Frontier Foundation (EFF). “Mi sospecha es que sí son usados frecuentemente”, enfatiza.

La organización con sede en Estados Unidos es reconocida mundialmente por el prestigioso trabajo que ha desarrollado en la defensa de las libertades civiles relacionadas con el uso de la tecnología. En su país de origen, EFF ganó litigios civiles vinculados con dispositivos de vigilancia como los IMSI Catchers, usados por agentes de seguridad para tratar de identificar sospechosos por delitos mayores o menores, sin discriminación. El objetivo podía ser desde un secuestrador hasta un inmigrante, o también manifestantes.

“En una protesta, se capturan todos los identificadores de teléfonos y con esto se consiguen más datos con las operadoras”, precisa Quintin. Al preguntarle sobre el procesamiento de la información, señaló que usan softwares específicos para big data. En la página de la EFF tienen publicado un catálogo de tecnología que podría ser usada en espionaje.

De acuerdo con Rocío San Miguel, presidenta de la organización venezolana Control Ciudadano, hay un riesgo creciente de vulneración del derecho a la privacidad por parte de organismos de inteligencia y contrainteligencia. Señala el peligroso camino que experimenta el país si no hay una ley que señale procedimientos, alcances y proteja los derechos de los ciudadanos. Al final todos están expuestos, aún más cuando existen arbitrariedades para conducir investigaciones.

Los intentos de EFF porque no se extienda de manera ilegal el uso de los dispositivos IMSI Catchers han resultado una tarea titánica, en la que se han enfrentado con el Departamento de Justicia estadounidense y las grandes corporaciones que venden estos equipos. Una de las más conocidas es Harris Corporation -hoy conocida como L3 Harris luego de su fusión con L3 Tecnologies, otro gigante de la tecnología- y fue la mencionada por dos periodistas mexicanos sobre la presencia de antenas sospechosas en el Distrito Federal, según un artículo del Washington Post.

Venezuela es uno de los 130 países del mundo en el que Harris Corporation tiene una subsidiaria y lleva por nombre Harris International Venezuela C.A. Según el Registro de Contrataciones Públicos del Estado se encarga de manejar los negocios de la corporación y cualquier otra sociedad relacionada, y para 2003 mostraba en su cartera de clientes al Ministerio de Defensa y componentes de los distintos cuerpos militares (Armada, Ejército, Guardia Nacional Bolivariana). Su oficina estaba en el sector de Las Mercedes, barrio de tiendas de lujo y sitios nocturnos del sureste de Caracas, y en su junta directiva aparecía para entonces el ciudadano libanés Mohamad Kannan Zuhdi El Haffar.

El Haffar figura además en la sociedad Venconsul Ingeniería, constituida en 1998 y parte del grupo de empresas aliadas que lideraron la creación de la operadora de telefonía celular Digitel. En 2007, una mención en una demanda civil lo señala como Director Ejecutivo de la operadora. En la junta directiva de Venconsul Ingeniería también estuvo Ibrahim El Hibri, empresario que invirtió en el proyecto de

telefonía privada Digitel que empezó a operar en 1999. Tanto Veneconsul como Harris International Venezuela tuvieron de clientes a los mismos organismos militares venezolanos, según las fichas del Registro Nacional de Contratistas de 2003.

Aunque Harris Corporation es el principal proveedor de IMSI Catchers, no es el único. Su catálogo de productos es muy variado, enfocado en tecnología para comunicaciones y, de acuerdo con la precisión de Quintin de la EFF, esta corporación se ha dedicado a venderle al sector militar, no a fuerzas del orden civil.

Hasta la fecha, no hay evidencia de que la administración de Nicolás Maduro haya comprado dispositivos de vigilancia para Venezuela, como sí la hubo en 2008 con respecto al gobierno de Hugo Chávez, cuando la primera filtración masiva de documentos de Wikileaks liberó una comunicación firmada por la unidad de Desarrollo Tecnológico de la Dirección de Inteligencia Militar (DIM), fechada en el año 2000. En ese documento se detalla la compra de unos Triggerfish, modelo 4080 (IMSI Catchers), cuyo proveedor fue Phoenix Worldwide Industries. En 2001, Phoenix Worlwide Industries entregó 225.256 dólares en equipos a la policía secreta de Venezuela y, según registros de la corte federal citados en la filtración, hubo contratos hasta 2004.


RECEIVER 1
PHONES
VOLUME
HARRIS
TF-4000
RECEIVER 2
HARRIS
RECEIVER 3
HARRIS
HARRIS
TriggerFish™ 4000
3 2 1 NET
RECEIVER ACTIVITY
RECORDER OUT
COMPUTER
RECEIVER 1
RECEIVER 2
RECEIVER 3

Un equipo similar a este fue ofrecido al gobierno de Hugo Chávez, en 2008. Es un Triggerfish modelo 4000.

Un equipo similar a este fue ofrecido al gobierno de Hugo Chávez, en 2008. Es un Triggerfish modelo 4000.

Con Maduro en el poder, el cortejo con las empresas proveedoras de equipos espías pasó de correos a las visitas en casa. Uno de los antecedentes más certeros está registrado en otra filtración que hicieron a la empresa italiana Hacking Team, especializada en la venta de software para *piratear* computadoras y teléfonos celulares. Al igual que los IMSI Catchers, este software permitía tener acceso a la mensajería de texto, la geolocalización y grabar las llamadas, además de interceptar los correos electrónicos del objetivo escogido.

El episodio que rodeó las negociaciones con Caracas está publicado en **Armando.info**. En el reportaje se cuenta cómo el equipo de ventas de Hacking Team y uno de sus aliados, la empresa estadounidense DTXT Corporation, especializada en aplicaciones de seguridad, mantuvieron conversaciones con altos funcionarios del gobierno y presentaron las nuevas soluciones de intercepción móvil.

Entre sus potenciales clientes estaban el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (Cicpc), División de Inteligencia Militar (DIM), Dirección General de Contrainteligencia Militar (Dgcim) y la Dirección de Comunicaciones de la Fuerza Armada Nacional Bolivariana. Aunque tenían pautada la reunión el 6 de marzo de 2013, a menos de 24 horas después del anuncio de la muerte del presidente Hugo Chávez, finalmente lo lograron dos días después. El sucesor no detendría los objetivos estratégicos; en su nombre asistió un general del Ejército venezolano y el coqueteo seguiría, al menos, por dos años más.

El interés ha seguido latente. Hace menos de un año, a mediados de noviembre de 2019, Maduro aprobó la compra de unidades Cellebrite UFED Toch2 por un costo de 51.000 euros. Este dispositivo es usado para extraer los datos de un teléfono celular y, según lo anunciado, sería empleado en investigaciones criminales legítimas. La reacción de 25 organizaciones no gubernamentales de Venezuela no se hizo esperar y solicitaron a la empresa israelí evitar la venta de cualquier tecnología de extracción de datos.

(*) *Los mapas interactivos que acompañan a esta historia fueron realizados por el equipo de FADe Project.*

Fecha de creación
2020/09/06