MÉXICO

Panorama de Amenazas Digitales: Sociedad Civil y Medios de Comunicación

Internews
Local voices. Global change.

SOCIALTIC
Digital technology for social change

Índice

Contexto

En el mundo de la seguridad digital, México se ha hecho un nombre como el más prolífico y uno de los primeros clientes reportados del spyware Pegasus, siendo la sociedad civil y los medios de comunicación su objetivo principal. Si bien Pegasus a menudo es noticia, la sociedad civil mexicana y las organizaciones de medios de comunicación se enfrentan a ataques digitales menos sofisticados en múltiples frentes. Este informe fue preparado por el equipo de Libertad y Resiliencia en Internet de Internews bajo una corriente de trabajo que fortalece la capacidad de las organizaciones de la sociedad civil (OSC), los periodistas y otros defensores de los derechos humanos (DDH) para detectar, analizar y desarrollar la resiliencia a los ataques digitales a través de la experiencia localizada en el análisis de amenazas y la respuesta a incidentes. Este informe tiene como objetivo proporcionar una visión general de las amenazas digitales que enfrentan la sociedad civil y las organizaciones de medios de comunicación en México y una guía para los expertos en seguridad digital que apoyan a esta comunidad. También tiene la intención de proporcionar un contexto para la industria de la ciberseguridad, que puede necesitar analizar los incidentes de seguridad que afectan a la sociedad civil y los medios de comunicación mexicanos. Concluimos con una discusión sobre las medidas de mitigación que los expertos en seguridad digital pueden proponer a las organizaciones con las que trabajan, así como a la sociedad civil y las organizaciones de medios de comunicación para que las implementen.

Este informe fue escrito en estrecha colaboración con SocialTIC, una organización sin fines de lucro dedicada a la investigación, capacitación, apoyo y promoción de la tecnología digital y la información con fines sociales. SocialTIC existe para empoderar de manera segura a los actores del cambio en América Latina mediante el fortalecimiento de sus acciones de análisis, comunicación social e incidencia a través del uso estratégico de tecnologías y datos digitales.

Las amenazas, tendencias y estudios de casos destacados en este informe se identificaron a través del apoyo directo de seguridad digital para las comunidades en riesgo (proporcionado por Internews y SocialTIC), la investigación documental y las conversaciones con miembros de confianza de la comunidad de Internet Freedom. Este informe agrega datos del trabajo de respuesta a incidentes y documenta patrones de ataque específicos de México.

Octubre de 2023

Escrito y editado: Martijn Grooten, Ashley Fowler, Marc Shaffer y Skyler Sallick
Edición, diseño y maquetación: Skyler Sallick

Panorama de Amenazas Digitales

Contexto Político, Sociedad Civil y Medios de Comunicación

El actual gobierno de México bajo el presidente Andrés Manuel López Obrador (a menudo denominado AMLO) está acusado de socavar la democracia y reprimir la libertad de los medios de comunicación y la sociedad civil. AMLO ha estigmatizado a los periodistas en la prensa y acosa a los medios de comunicación que van en contra de las narrativas oficiales del gobierno. Los periodistas enfrentan amenazas significativas a su seguridad física, principalmente por parte de redes del crimen organizado que trabajan en colaboración con funcionarios gubernamentales. Casi 150 periodistas han sido asesinados en México desde el año 2000, cuatro de los cuales ocurrieron en 2023. Reporteros sin Fronteras clasifica a México en el puesto 128 de los 180 países incluidos en su índice de libertad de prensa, que analiza el contexto político, económico, legislativo, social y de seguridad del periodismo en un país. Reporteros sin Fronteras enfatiza que las amenazas físicas en México se encuentran entre las más altas del mundo.[1] Las luchas experimentadas por los periodistas son particularmente severas para las mujeres y otras comunidades marginadas, ya que a menudo experimentan mayores impactos mentales y enfrentan amenazas más agresivas que adquieren un carácter más personal.[2]

Aunque la sociedad civil mexicana sigue activa, se enfrenta a importantes obstáculos para operar libremente. La administración de AMLO no ha cumplido con las promesas de campaña de apoyar los derechos humanos.[3] La administración a menudo está en conflicto con la sociedad civil; haciendo caso omiso de las críticas e insultando a los opositores. En marzo de 2022, los legisladores de MORENA, el partido gobernante, introdujeron una ley que "prohibiría a las organizaciones sin fines de lucro tratar de influir o cambiar las leyes ya sea a través del cabildeo o mediante litigios estratégicos si reciben fondos, directa o indirectamente, de gobiernos o corporaciones extranjeras."[4] Amnistía Internacional argumenta que habrá un efecto disuasorio en la capacidad de la sociedad civil para criticar al gobierno si esta ley entra en vigor. Existen leyes similares en Nicaragua y Guatemala, y aunque El Salvador intentó seguir su ejemplo con su ley de "agente extranjero", los grupos de derechos humanos tuvieron éxito en oponerse a la aprobación de la ley.[5]

El ejército de México ha seguido ganando poder sin dejar de ser el brazo menos transparente del gobierno.

El ejército de México ha seguido ganando poder sin dejar de ser el brazo más opaco en su operación del gobierno. En particular, la administración de AMLO transfirió el control de la Guardia Nacional dirigida por civiles de México a los militares en 2022. En 2021, los militares tomaron el control del desarrollo, construcción y de todas las ganancias futuras del "Tren Maya", uno de los mega proyectos estrella de AMLO. El proyecto tiene la intención de conectar destinos turísticos populares en la costa de Yucatán como Cancún y Tulum con el interior de la península y la costa caribeña a través del tren. Muchos grupos ambientalistas e indígenas se oponen a la construcción de este tren, puesto que ya ha causado daños al ecosistema y a los sitios históricos de Yucatán. Los grupos de derechos humanos también han acusado al gobierno de no lograr la

aceptación pública y critican la falta de transparencia gubernamental sobre el proyecto. Al transferir el control del proyecto a los militares, la administración fortalece aún más a las fuerzas armadas al tiempo que valida las preocupaciones sobre la falta de transparencia.[6]

Los miembros de la sociedad civil, incluidos los que se oponen a la eliminación del control civil de la Guardia Nacional y la toma militar del proyecto Tren Maya, enfrentan represalias violentas por parte de los militares y grupos delictivos organizados. El gobierno ha sido acusado de no investigar los abusos criminales cometidos por miembros de las fuerzas armadas. Con un sentido de impunidad, los delincuentes atacan a los defensores de los derechos humanos, a menudo hasta el punto en que los activistas se ven en la necesidad de requerir seguridad física.[7]

Aunque el país ha mejorado significativamente los derechos legislativos de la comunidad LGBTQIA+, México sigue siendo el país con la segunda tasa más alta de delitos de odio relacionados con LGBTQIA+ en la región.

México es el hogar de varias comunidades vulnerables que enfrentan discriminación y violencia. Aunque existen leyes contra la discriminación, los pueblos indígenas y los afromexicanos siguen estando subrepresentados.[8] El 77% de los indígenas mexicanos viven por debajo de la línea de pobreza y los estados con mayor población indígena generalmente reciben menos recursos y servicios.[9] La comunidad LGBTQIA+ de México enfrenta una "paradoja del progreso". Aunque el país ha mejorado significativamente los derechos legislativos de la comunidad LGBTQIA+, México sigue siendo el país con la segunda tasa más alta de delitos de odio relacionados con personas LGBTQIA+ en la región.10 En el papel, México es un líder regional con respecto a la comunidad LGBTQIA+. En la práctica, el país no protege los derechos y la seguridad física de la comunidad.[11]

Ciberseguridad en México

México ha experimentado tasas significativamente más altas de actividad cibernética maliciosa en la última década. El país no ha evitado el reciente aumento global en el uso de ransomware por parte de los ciberdelincuentes, con actores de amenazas que despliegan varias familias de malware bancario para atacar a los usuarios. Destacados objetivos de tales ciberataques incluyen al proveedor de petróleo Pemex y una fábrica local del gigante manufacturero Foxconn.[12]

Si bien los ataques de Pemex y Foxconn fueron oportunistas, los ciberdelincuentes organizados también están activos en el país. Un grupo denominado por la empresa de seguridad Mandiant como "FIN13" llevó a cabo una campaña financiera más específica en el país.[13] Activo desde aproximadamente 2016, "FIN13" se centra particularmente en México y se dirige a grandes organizaciones en los sectores financiero, minorista y hotelero mediante el uso de malware estándar y personalizado. Además, una reciente publicación de la empresa de seguridad SentinelOne informa que el capo de una operación global de ciberdelincuencia dirigida a usuarios de bancos españoles y chilenos reside en México.[14]

Un grupo de skimmers de cajeros automáticos rumanos también ha estado activo en el país. Según informes de los medios locales, el grupo recibe protección legal por sus delitos

cibernéticos por motivos financieros de un alto funcionario anticorrupción de la Fiscalía General del país.[15]

En respuesta a la prevalencia de la ciberdelincuencia, el gobierno mexicano publicó una iniciativa de "Ley de Ciberseguridad" el 25 de abril de 2023, el primer intento de una ley integral de este tipo. La ley contiene cuatro enfoques centrales para la ciberseguridad: defender el espacio digital para salvaguardar la seguridad nacional, crear un nuevo marco legal para abordar los ciberataques, pruebas anuales de penetración de instituciones públicas y privadas y la creación de una Agencia Nacional de Ciberseguridad. La Agencia Nacional de Ciberseguridad será controlada por el poder ejecutivo de México y se inspira en agencias similares en la Unión Europea, Estados Unidos y Brasil.[16]

Los activistas de derechos humanos han criticado intensamente la nueva ley. Article19 México y Centroamérica, la sección local de la organización internacional defensora de derechos humanos enfocada en promover la libertad de expresión y la libertad de información, ha planteado varias preocupaciones. En primer lugar, señala que la ley militariza la ciberseguridad al tratar la defensa del espacio digital como un problema de seguridad nacional.[17] Los expertos en el sector privado de México coinciden en que la ley se centra demasiado en la ciberseguridad como un asunto de seguridad nacional sin considerar el alcance del problema en todos los aspectos de la vida. Existe la preocupación de que el posicionamiento de la ciberseguridad bajo un marco de seguridad nacional podría crear una cobertura legal para la vigilancia generalizada de la actividad digital en México.[18] Este enfoque estrecho en la ciberseguridad como un problema de seguridad nacional proporciona vías para el abuso de los derechos civiles. Además, los tipos y definiciones de delito cibernético incluidos en la ley tienen el potencial de criminalizar la conducta legítima o hacer que la actividad delictiva sea demasiado difícil de procesar. Como ejemplo, Article19 sugiere que la criminalización del contenido que incita a la hostilidad puede servir como justificación para reprimir la libertad de expresión. Article19 también señala que la ley está mal redactada, lo que dificulta su implementación y no aborda los abusos cometidos por el gobierno mexicano.[19]

El Estado de la Ciberseguridad de la Sociedad Civil y los Medios de Comunicación

México es un objetivo del grupo hacker activista anónimo "Guacamaya", o hacktivista, que ha estado activo en varios países de América Latina desde principios de 2022. Los hackeos perpretados por este grupono solo son relevantes por su actividad cibernética, sino también por lo que revelaron. En el caso de México, el grupo hacktivista "Guacamaya" reveló vínculos entre el ejército y las organizaciones criminales, así como el uso por parte del ejército del spyware Pegasus para atacar a periodistas, defensores de los derechos humanos y funcionarios gubernamentales.[20]

El spyware Pegasus de NSO Group se ha utilizado en México contra una amplia gama de objetivos, incluidos abogados de las familias de mujeres asesinadas, periodistas que investigan cárteles criminales y la esposa de un periodista asesinado por cárteles.

El uso de Pegasus por parte de los funcionarios mexicanos no es nuevo. El primer informe público sobre el ahora notorio spyware se publicó en 2016 y nombró al periodista mexicano Rafael Cabrera como uno de los objetivos.[21] Desde entonces, el spyware Pegasus de NSO Group se ha utilizado en México contra una amplia gama de objetivos, incluidos abogados de las familias de mujeres asesinadas, [22] periodistas que investigan cárteles criminales[23] y la esposa de un periodista asesinado por cárteles.[24] De los 50.000 números de teléfono descubiertos en una investigación de 2021 por Forbidden Stories y Amnistía Internacional sobre posibles teléfonos atacados por Pegasus, aproximadamente 15.000 eran números de teléfono mexicanos, más número que en cualquier otro país.[25]

Los hallazgos iniciales del uso de spyware en México llevaron a organizaciones de la sociedad civil como SocialTIC, R3D y Article19 a retirarse de un grupo de trabajo de spyware en 2017 en Open Government Partnership, una organización multilateral que promueve la transparencia y la reforma del gobierno. En su retirada, estas OSC citaron una falta de confianza en el gobierno mexicano dado su uso de spyware. Tras la elección de AMLO a principios de 2019, estas organizaciones se reincorporaron al grupo de trabajo con base a su promesa de campaña de respetar los derechos humanos. Sin embargo, las acusaciones de uso continuo de Pegasus por parte del gobierno y los militares han agregado complicaciones adicionales.

Además de Pegasus, la sociedad civil mexicana y los medios de comunicación se han enfrentado al uso de los spywares Hacking Team[26], Finfisher[27] y QuaDream[28]. Algunos medios de comunicación y organizaciones de la sociedad civil ahora perciben la prevalencia de la tecnología de vigilancia como la mayor amenaza para su trabajo. Otro riesgo prevalente es la frecuencia con la que el hackeo resulta en el robo de cuentas personales e institucionales y la pérdida de información.

El uso generalizado de spyware por parte de las autoridades mexicanas tiene un efecto importante en la sociedad civil y las organizaciones de medios de comunicación: la percepción de ser espiado, incluso cuando ese pueda no ser el caso. Debido al miedo a la vigilancia, los eventos inexplicables en cuentas y dispositivos, como el retraso en las velocidades de conectividad o los reinicios frecuentes de dispositivos, hacen que estas personas teman que el spyware pueda haber infectado su dispositivo, lo que aumenta la paranoia y el estrés cuando la explicación puede ser más mundana.

Además, muchos miembros de la sociedad civil y los medios de comunicación se enfrentan al acoso en línea por parte de personas con opiniones opuestas. Este acoso puede implicar 'doxeo', la publicación de información personal, lo que puede llevar a amenazas de violencia física y/o muerte. Las mujeres y las minorías de género son un objetivo particular de este tipo de acoso.

Debido al miedo a la vigilancia, los eventos inexplicables en cuentas y dispositivos, como el retraso en las velocidades de conectividad o los reinicios frecuentes de dispositivos, hacen que estas personas teman que el spyware pueda haber infectado su dispositivo, lo que aumenta la paranoia y el estrés cuando la explicación puede ser más mundana.

Las amenazas a la sociedad civil y los medios de comunicación en México son significativas, y estas organizaciones requieren el apoyo de la comunidad de ciberseguridad para garantizar que puedan continuar llevando a cabo su trabajo necesario.

Medidas de Mitigación

La seguridad de las cuentas en líneaes importante para cualquier persona en México, pero crucial para los miembros de la sociedad civil en particular. **La autenticación de dos factores es imprescindible** y mitiga el uso de contraseñas débiles y/o reutilizadas. Aunque es mejor que ninguna autenticación de dos factores, la autenticación a través de SMS no debe considerarse lo suficientemente segura, especialmente para los usuarios de alto riesgo, ya que hay algunas pruebas de que los SMS pueden ser interceptados a través de proveedores de telecomunicaciones corruptos o pirateables. El uso de una aplicación de autenticación es mejor que los SMS, y el uso de un token de hardware generalmente proporciona la mejor seguridad, aunque esto requiere equipo adicional.

Algunas aplicaciones de mensajería como Telegram, WhatsApp y Signal requieren el uso de un número de teléfono para activar la cuenta. Habilitar la autenticación de dos factores implica **agregar un código de acceso** además de usar SMS para acceder a la cuenta, proporcionando mayor seguridad en casos de compromiso de SMS.

Cuando esta función está habilitada, la aplicación le pedirá periódicamente al usuario que ingrese su código de acceso para asegurarse de que nadie más que el propietario de la cuenta tenga acceda a los mensajes. Esto evita la toma de posesión de la cuenta a través de la interceptación de SMS.

Los spyware avanzados como Pegasus y Quadream suelen utilizar vulnerabilidades de día cero y, especialmente en el primer caso, infecciones de clic cero. Este tipo de spyware avanzado puede infectar un dispositivo sin hacer clic en un enlace o abrir un archivo adjunto. Como los usuarios no pueden prevenir este tipo de infección, aquellos en riesgo de este tipo de spyware deben tener esto en cuenta.

Se insta a los objetivos potenciales a **usar mensajes que desaparecen** en aplicaciones de mensajería donde los mensajes se eliminan automáticamente después de un período de tiempo fijo, ya que esto puede limitar el daño si la cuenta llegara a estar comprometida. La compartimentación, como el **uso de dispositivos separados para el trabajo y el uso personal**, o incluso un **dispositivo separado para trabajos de alto riesgo**, también limita el daño potencial, pero conlleva costos e inconvenientes adicionales.

Los puntos finales, como las computadoras portátiles y los teléfonos móviles, deben mantenerse actualizados aplicando parches de seguridad a los sistemas operativos y otro software siempre que estén disponibles. **El software solo debe adquirirse de fuentes oficiales.** En muchos casos, esto requiere un pago. Las ONGs no deben ser tímidas para discutir esto con los financiadores, o para buscar alternativas gratuitas, como software de código abierto y programas que proporcionen software de forma gratuita o a precios reducidos a las ONGs elegibles.

Mantener los dispositivos actualizados es muy importante, y para los iPhones, **reiniciar regularmente el dispositivo** – idealmente una vez al día - y usar el **modo hermético de Apple** también mitiga la probabilidad de ataques.

Se sabe mucho menos sobre el spyware dirigido a dispositivos Android, aunque eso no significa que los usuarios de Android corran menos riesgo. Los dispositivos Android más caros, incluidos los dispositivos Pixel de Google, son más seguros y generalmente tienen soluciones para las vulnerabilidades disponibles más rápidamente que los dispositivos Android más baratos. El reinicio regular de los dispositivos probablemente mitigará el daño, ya que el spyware generalmente se elimina de los dispositivos después de un reinicio.[i] Hay que tomar en cuenta que el reinicio de un dispositivo Android puede eliminar la evidencia de una infección anterior, lo que puede ser una preocupación para algunos usuarios.

Estudios de Casos

Doxeo de una Activista Contra la Trata

Una mujer mexicana defensora de los derechos humanos y aboga por las víctimas de la trata de personas ha sido durante mucho tiempo el blanco de los gobiernos locales corruptos y el crimen organizado. Ambos grupos se oponen a su trabajo por sacar a la luz su actividad delictiva y el abuso de los derechos humanos que cometen, lo que anteriormente la llevó a abandonar el país por algún tiempo.

En el otoño de 2022, experimentó una campaña de acoso. Su información personal se publicó en un sitio web mexicano similar a 4Chan que se usa comúnmente para el acoso. Se instó a las personas en el sitio a ponerse en contacto con ella para obtener fotografías de desnudos y servicios sexuales.

La mujer se acercó a SocialTIC. El contenido se eliminó del sitio web y SocialTIC ayudó a proteger sus cuentas y dispositivos online. SocialTIC realizó una verificación remota de sus dispositivos para cerciorarse que no estuvieran infectados. Por suerte, no se encontró ninguno lo estaban.

Para las comunidades en riesgo, cualquier forma de acoso tiene un impacto. Sin embargo, el impacto a menudo es mucho peor para las mujeres y las minorías sexuales, ya que a menudo implica acoso de naturaleza sexual.

En este caso, la mujer cesó sus actividades durante varios meses como consecuencia de las amenazas a su seguridad, antes de finalmente retomarlas cuando el contenido había sido retirado. El doxeo puede llegar a ser muy pernicioso y puede traer riesgos a la seguridad personal.

[i] Este es el caso de todos los spywares conocidos para iPhone y probablemente también para spywares de Android, especialmente el tipo que "rootea" el dispositivo.

La enredada telaraña de Pegasus en México

Pegasus fue descubierto por primera vez en México en el teléfono del periodista Rafael Cabrera en 2016. En su libro, Pegasus, los periodistas de investigación Laurent Richard y Sandrine Rigaud revelan que el gobierno mexicano compró Pegasus por primera vez en 2011. Los autores sugieren que México fue el primer cliente crucial de NSO Group, lo que les permitió convertirse en un negocio exitoso.

Cuando asumió el cargo en 2018, el presidente mexicano Andrés Manuel López Obrador ("AMLO") disolvió la policía federal y reformó la agencia de inteligencia del país.[29] Ambas instituciones habían utilizado previamente Pegasus para atacar a los individuos que investigan el secuestro y desaparición de 43 estudiantes en 2014.[30]

A pesar de la promesa de su gobierno, el uso de Pegasus no cesó bajo AMLO.[31] En 2022, Citizen Lab, un laboratorio interdisciplinario con sede en la Universidad de Toronto, y R3D, una organización mexicana centrada en la defensa de los derechos humanos en el espacio digital, informaron que Pegasus se utilizó con éxito contra periodistas, defensores de los derechos humanos y al menos un político de la oposición.[32] En 2023, SocialTIC, colaboró con R3D y otros socios internacionales para confirmar las infecciones de Pegasus en los teléfonos de dos miembros del personal de la organización mexicana de derechos humanos Centro Prodh.[33]

Para muchos miembros de la sociedad civil mexicana, Pegasus se siente como "lo de siempre". Aunque el periodismo y el activismo siempre han sido ocupaciones peligrosas en México, el uso generalizado de spyware por parte de las autoridades gubernamentales ha normalizado tales amenazas digitales.

Sin embargo, el informe del *New York Times* de mayo de 2023 que reveló el uso del spyware de Pegasus en el teléfono de Alejandro Encinas no se sintió como lo de siempre para muchas personas en el país.[34] En ese momento, Alejandro era el Subsecretario de Derechos Humanos de AMLO y había sido un aliado de AMLO durante mucho tiempo, sirviendo bajo AMLO durante su mandato de AMLO como alcalde de la Ciudad de México dos décadas antes. Es importante destacar que Encinas fue una de las pocas personas dentro del gobierno dispuestas a criticar a los militares, que han seguido ganando poder bajo AMLO. En particular, acusó a los militares de estar implicados en la desaparición de los 43 estudiantes en 2014.[35]

Más que en cualquier otro lugar del mundo, las herramientas de spyware como Pegasus se han convertido en la herramienta favorita de los militares y el gobierno para atacar a los críticos de gobierno, ya sean periodistas, activistas o miembros del propio gobierno.

Otras Lecturas

Como se ve en este informe, las organizaciones de la sociedad civil y los periodistas a menudo enfrentan amenazas únicas y avanzadas, a la vez que carecen de los recursos para detectarlas, analizarlas y prevenirlas. Una comprensión profunda de las amenazas que enfrentan la sociedad civil y los medios permite a los profesionales de la seguridad digital adaptar sus respuestas y apoyar mejor a las organizaciones con las que trabajan, lo que lleva a medidas de mitigación personalizadas que son más efectivas y fáciles de implementar para la sociedad civil y las organizaciones de medios de comunicación. Para obtener más información sobre las amenazas que enfrentan la sociedad civil y los periodistas, Internews y sus socios han escrito el informe "Tendencias Globales en Amenazas Digitales: Sociedad Civil y Medios de Comunicación", así como informes sobre el Panorama de Amenazas Digitales para Armenia, Brasil, Serbia y Ucrania. Estos recursos se pueden encontrar en la página web de Recursos Tecnológicos de Internews.

Historia de México

Los Estados Unidos Mexicanos es una república presidencial federal en América del Norte, que limita con los Estados Unidos al norte y Guatemala y Belice al sur. México está compuesto por 32 entidades federativas. Con una población de más de 128 millones, México es el décimo país más poblado del mundo. México es miembro de las Naciones Unidas[36], del G20[37], de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[38], de la Organización Mundial del Comercio39, del Foro de Cooperación Económica Asia-Pacífico (APEC)[40] y de la Organización de los Estados Americanos (OEA)[41].

México estaba habitado por varios pueblos indígenas antes de que los españoles conquistaran la tierra en el siglo XVI. Después de obtener su independencia en el siglo XIX, México experimentó varios sistemas políticos antes de que el Partido Revolucionario Institucional (PRI) se consolidara en el poder en el período posrevolucionario y comenzara un gobierno de facto de partido único que duró hasta el año 2000. La actual constitución de México fue adoptada en 1917.[42]

Agradecimientos

Desde 2021, Internews ha trabajado con siete Threat Labs (organizaciones locales con la capacidad técnica y las herramientas adecuadas para analizar muestras sospechosas de phishing y malware y luego compartir información con la comunidad sobre tendencias de ataques, amenazas emergentes y contramedidas) para responder a incidentes que afectan la seguridad digital de la sociedad civil y las organizaciones de medios de comunicación de todo el mundo. Los datos recopilados a través del programa de respuesta a incidentes ayudaron a dar forma a las mitigaciones y los enfoques de respuesta para las comunidades en riesgo e informaron este informe.

Internews desea expresar nuestro agradecimiento a la comunidad de Threat Labs que trabajó con nosotros en este proyecto. Están comprometidos a ayudar a los necesitados y garantizar que sus socios de la sociedad civil y las organizaciones de medios puedan completar su importante trabajo de manera segura y efectiva. En total, este proyecto ayudó a Threat Labs a responder a más de 200 incidentes de seguridad digital y a publicar más de 60 recursos educativos a través de sus sitios web y plataformas de redes sociales.

Un agradecimiento especial a SocialTIC por proporcionar la información para documentar y compartir estos estudios de casos y por revisar y aportar valiosos comentarios a este informe. El informe no habría sido posible sin Paul Aguilar y Diego Morabito.

Notas Finales

[1] "México." Reporteros sin Fronteras. Consultado en septiembre de 2023. https://rsf.org/en/country/mexico.

[2] Hoosten, Jan-Albert. "Las periodistas que cubren las protestas feministas mexicanas se enfrentan a una dura respuesta policial". Comité para la Protección de los Periodistas. 10 de noviembre de 2020. https://cpj.org/2020/11/female-journalists-covering-mexican-feminist-protests-face-harsh-police-response/.

[3] Sandin, Linnea and Sarah Baumunk. "Sociedad Civil Mexicana". Centro de Estudios Estratégicos e Internacionales. Diciembre de 2018. https://www.csis.org/analysis/mexican-civil-society.

[4] "México: proyecto de ley regresivo de Shelve para frenar a los grupos de la sociedad civil". Amnistía Internacional. 11 de marzo de 2022. https://www.amnesty.org/en/latest/news/2022/03/mexico-shelve-regressive-bill-to-curb-civil-society-groups/.

[5] "México: Proyecto de ley regresivo de Shelve para frenar a los grupos de la sociedad civil", Amnistía Internacional.

[6] "La libertad en el mundo en 2023: México". Freedom House. Consultado en julio de 2023. https://freedomhouse.org/country/mexico/freedom-world/2023

[7] "La libertad en el mundo en 2023: México," Freedom House.

[8] "La libertad en el mundo en 2023: México," Freedom House.

[9] "La libertad en el mundo en 2023: México," Freedom House.

[10] Fistonich, Matt. "Paradoja del progreso para la comunidad LGBTQ+ en México". Gay Nation. 18 de mayo de 2023. https://gaynation.co/progress-parodox-for-the-lgbtq-community-in-mexico/.

[11] Fistonich, "Paradoja del progreso para la comunidad LGBTQ+ en México".

[12] Osborne, Charlie. "El proveedor de petróleo mexicano Pemex dice que el intento de hackeo está 'neutralizado'". *ZDNET*. 12 de noviembre de 2019. https://www.zdnet.com/article/mexicos-pemex-oil-provider-says-attempted-ransomware-hack-neutralized/#ftag=RSSbaffb68.; Greig, Jonathan. "Foxconn: las operaciones de la fábrica de México 'vuelven gradualmente a la normalidad' después del ataque de ransomware." *The Record*. 1 de junio de 2022. https://therecord.media/foxconn-mexico-factory-operations-gradually-returning-to-normal-after-ransomware-attack.

[13] Ta, Van, Jake Nicastro, Rufus Brown, and Nick Richard. "FIN13: un actor de amenazas cibernéticas centrado en México." Mandiant. Última modificación el 8 de agosto de 2022. https://www.mandiant.com/resources/blog/fin13-cybercriminal-mexico.

[14] Thill, Pol. "Neo_Net: El Kingpin del eCrime Español." SentinelOne. 3 de julio de 2023. https://www.sentinelone.com/blog/neo net-the-kingpin-of-spanish-ecrime/.

[15] "Informe: Un Grupo de Skimmers de Cajeros Automáticos Recibía Protección de la Fiscalía General Mexicana." KrebsonSecurity. 26 de mayo de 2020. https://krebsonsecurity.com/2020/05/report-atm-skimmer-gang-had-protection-from-mexican-attorney-generals-office/.

[16] Rivera, Santiago Fuentes. "Ley de Ciberseguridad en México: Conoce la nueva Ley." Delta Project. 18 de enero de 2023. https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico.

[17] "La Iniciativa de Ley de Ciberseguridad amenaza los derechos humanos y promueve la militarización". Article 19. 27 de abril de 2023. https://articulo19.org/iniciativa-de-ley-de-ciberseguridad-amenaza-los-derechos-humanos-y-promueve-la-militarizacion/.

[18] Segundo, Luis Pablo. "México: Acusan de incoherente a Ley de Ciberseguridad." DPL News. 27 de julio de 2023. https://dplnews.com/mexico-acusan-de-incoherente-a-ley-de-ciberseguridad/.

[19] Op cit.

[20] Greig, Jonathan. "El presidente mexicano confirma el hackeo de 'Guacamaya' dirigido a los militares regionales". *The Record*. 29 de septiembre de 2022. https://therecord.media/mexican-president-confirms-guacamaya-hack- targeting-regional-militaries.

[21] Marczak, Bill and John Scott-Railton. "El disidente del millón de dólares: los días cero del iPhone de NSO Group utilizados contra un defensor de los derechos humanos de los Emiratos Árabes Unidos." The Citizen Lab. 24 de agosto de 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[22] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. "Reckless IV: Abogados de las familias de mujeres mexicanas asesinadas atacadas con spyware de NSO." The Citizen Lab. 2 de agosto de 2017. https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/.

[23] Scott-Railton, John, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. "Reckless VI: Periodistas mexicanos investigan a cárteles atacados con spyware de NSO tras asesinato de colega." The Citizen Lab. 27 de noviembre de 2018. https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/.

[24] Scott-Railton, John, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. "Reckless VII: La esposa del periodista asesinado en un asesinato vinculado a un cártel fue atacada con el spyware de NSO Group." The Citizen Lab. 20 de marzo de 2019. https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/.

[25] “México: las revelaciones de Pegasus provocan nuevos llamados a la verdad.” Article 19. 20 de julio de 2021. https://www.article19.org/resources/mexico-pegasus-revelations-prompt-fresh-calls-for-truth/.

[26] Perez, David Marcial. "Las filtraciones revelan los contratos de espionaje del gobierno mexicano con la empresa de ciberseguridad". *El País*. Última modificación el 7 de julio de 2015. https://english.elpais.com/elpais/2015/07/07/inenglish/1436275149 259998.html.

[27] Carrieri, Matthew. "Cyber Stewards Network y activistas locales investigan a FinFisher en México". The Citizen Lab. 8 de noviembre de 2013. https://citizenlab.ca/2013/11/cyber-steward-network-local-activists- investigate-surveillance-mexico/.

[28] Marczak, Bill, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, and Ron Deibert. “Sweet QuaDreams: Un primer vistazo a las vulnerabilidades, las víctimas y los clientes del proveedor de spyware QuaDream.” The Citizen Lab. 11 de abril de 2023. https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

[29] Kitroeff, Natalie and Ronen Bergman. "Cómo México se convirtió en el mayor usuario de la herramienta de espionaje más notoria del mundo". The New York Times. 18 de abril de 2023. https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html.

[30] "Secuestro masivo en Iguala". Wikipedia. Consultado en julio de 2023. https://en.wikipedia.org/wiki/Iguala mass kidnapping.

[31] Solomon, Daina Beth. "Los ataques con spyware Pegasus en México continuaron bajo Lopez Obrador, según un informe". Reuters, 2 de octubre de 2022. https://www.reuters.com/world/americas/pegasus-spyware-attacks-mexico-continued-under-lopez-obrador-report-2022-10-03/.

[32] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Paolo Nigro Herrero, and Ron Deibert. "Identifican nuevos abusos de spyware Pegasus en México". The Citizen Lab. 2 de octubre de 2022. https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/.

[33] "Una vez más, el Centro Prodh es atacado con Pegasus". Centro Prodh. 18 de abril de 2023. https://centroprodh.org.mx/2023/04/18/nuevamente-centro-prodh-es-atacado-con-pegasus/.

[34] Kitroeff, Natalie and Ronen Bergman. "Estaba investigando a las fuerzas armadas de México. Entonces comenzó el espionaje". *The New York Times*. 22 de mayo de 2023. https://www.nytimes.com/2023/05/22/world/americas/mexico-spying-pegasus-israel.html.

[35] Kitroeff, "Estaba investigando a las fuerzas armadas de México. Entonces comenzó el espionaje".

[36] "Estados miembros". United Nations. Consultado en julio de 2023. https://www.un.org/en/about-us/member-states.

[37] "Sobre el G20". Group of Twenty. Consultado en julio de 2023. https://www.g20.org/en/about-g20/.

[38] "Contribuciones presupuestarias de los Países Miembros". OCDE. Consultado en julio de 2023. https://www.oecd.org/about/budget/member-countries-budget-contributions.htm.

[39] "Miembros y observadores". Organización Mundial del Comercio. Consultado en julio de 2023. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.

[40] "Economías Miembros". Foro de Cooperación Económica Asia-Pacífico. Consultado en julio de 2023. https://www.apec.org/about-us/about-apec/member-economies.

[41] "Estados miembros". OEA. Consultado en julio de 2023. https://www.oas.org/en/member states/default.asp.

[42] "Perfil de país de México". *BBC*. Última modificación el 4 de abril de 2023. https://www.bbc.com/news/world-latin-america-18095241.